



Guide de l'utilisateur

AWS Transfer Family



AWS Transfer Family: Guide de l'utilisateur

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Qu'est-ce que c'est AWS Transfer Family ?	1
Comment AWS Transfer Family fonctionne	3
Articles de blog pertinents pour Transfer Family	4
Prérequis	7
Régions, points de terminaison et quotas	7
Inscrivez-vous pour AWS	7
Configurer le stockage	8
Configuration d'un compartiment Amazon S3	9
Configuration d'un système de EFS fichiers Amazon	13
Création d'un IAM rôle et d'une politique	17
Créer un rôle d'utilisateur	18
Comment fonctionnent les politiques de session	21
Exemple de politique d'accès en lecture/écriture	25
Tutoriels Transfer Family	28
Commencez avec les points de terminaison de serveur	29
Prérequis	29
Connectez-vous à la console	30
Création d'un SFTP serveur activé	30
Ajouter un utilisateur géré par le service	31
Transférer un fichier à l'aide d'un client	33
Création d'un flux de travail de déchiffrement	35
Étape 1 : Configuration d'un rôle d'exécution	36
Étape 2 : créer un flux de travail géré	37
Étape 3 : ajouter le flux de travail à un serveur et créer un utilisateur	39
Étape 4 : Création d'une paire de PGP clés	40
Étape 5 : Stockez la clé PGP privée dans AWS Secrets Manager	41
Étape 6 : Chiffrer un fichier	42
Étape 7 : Exécuter le flux de travail et afficher les résultats	43
Création et utilisation de SFTP connecteurs	44
Étape 1 : créer les ressources de soutien nécessaires	45
Étape 2 : Création et test d'un SFTP connecteur	50
Étape 3 : envoyer et récupérer des fichiers à l'aide du SFTP connecteur	54
Procédures de création d'un serveur Transfer Family à utiliser comme SFTP serveur distant	58

Utiliser un fournisseur d'identité personnalisé	60
Prérequis	61
Étape 1 : créer une CloudFormation pile	61
Étape 2 : Vérifiez la configuration de la méthode API Gateway pour votre serveur	62
Étape 3 : Afficher les détails du serveur Transfer Family	63
Étape 4 : vérifiez que votre utilisateur peut se connecter au serveur	65
Étape 5 : tester la SFTP connexion et le transfert de fichiers	65
Étape 6 : Limiter l'accès au bucket	66
Mettez à jour Lambda si vous utilisez Amazon EFS	68
Configurez une AS2 configuration	69
Étape 1 : créer des certificats pour AS2	71
Étape 2 : Création d'un serveur Transfer Family utilisant le AS2 protocole	75
Étape 3 : Importer des certificats en tant que ressources de certificats Transfer Family	79
Étape 4 : Créez des profils pour vous et votre partenaire commercial	80
Étape 5 : Créez un accord entre vous et votre partenaire	80
Étape 6 : Créez un lien entre vous et votre partenaire	81
Étape 7 : Testez l'échange de fichiers à AS2 l'aide de Transfer Family	83
Transfer Family pourSFTP,FTPS, FTP	86
Options du fournisseur d'identité	86
AWS Transfer Family matrice des types de terminaux	88
Configuration d'un point de terminaison du serveur Transfer Family	92
Création d'un SFTP serveur activé	94
Création d'un FTPS serveur activé	106
Création d'un FTP serveur activé	118
Créez un serveur dans un VPC	129
Utilisation de noms d'hôtes personnalisés	151
Transférer des fichiers via le terminal du serveur	155
SFTP/FTPS/FTPCommandes disponibles	158
Trouvez votre point de VPC terminaison Amazon	159
Évitez les setstat erreurs	161
Utiliser Open SSH	34
Utilisez Win SCP	163
Utilisez Cyberduck	34
Utiliser FileZilla	167
Utiliser un client Perl	168
Traitement après le téléchargement	168

Gestion des utilisateurs	170
Utilisateurs gérés par le service	171
Utilisateurs des services d'annuaire	182
Utilisateurs du fournisseur d'identité personnalisé	199
Utiliser des répertoires logiques	229
Règles d'utilisation des répertoires logiques	231
Implémentation de répertoires logiques et chroot	232
Exemple de configuration de répertoires logiques	235
Configuration de répertoires logiques pour Amazon EFS	236
AWS Lambda Réponse personnalisée	236
SFTPconnecteurs	238
Configuration des SFTP connecteurs	238
Création d'un SFTP connecteur	239
SFTPalgorithmes de connexion	247
Stockez un secret à utiliser avec un SFTP connecteur	248
Génération et SFTP formatage de la clé privée du connecteur	249
Tester un SFTP connecteur	253
Transférez des fichiers avec des SFTP connecteurs	255
Gérer les SFTP connecteurs	257
Mettre à jour les SFTP connecteurs	257
Afficher les détails SFTP du connecteur	257
Quotas pour les SFTP connecteurs	259
Transfer Family pour AS2	261
AS2cas d'utilisation	262
Configurez AS2	267
Création d'un AS2 serveur à l'aide de la console Transfer Family	268
Création d'un AS2 serveur à l'aide d'un modèle	272
AS2configurations	275
AS2fonctionnalités et capacités	281
Configuration des AS2 connecteurs	283
Création d'un AS2 connecteur	284
AS2algorithmes de connexion	287
Authentification de base pour les AS2 connecteurs	288
Activer l'authentification de base pour les AS2 connecteurs	290
Afficher les détails du connecteur	294
Gérer les AS2 partenaires	295

AS2Certificats d'importation	295
AS2rotation des certificats	297
Création de AS2 profils	299
Créez des AS2 accords	299
Transférer AS2 des messages	301
Envoyer AS2 des messages	301
Recevoir des AS2 messages	302
Configurer HTTPS pour AS2	303
Transférez des fichiers avec des AS2 connecteurs	307
Noms et emplacements des fichiers	308
Codes d'état	311
JSONFichiers d'exemple	312
Moniteur AS2	314
Codes d'état AS2	315
Codes d'erreur AS2	316
Gestion des flux de travail de traitement de fichiers	330
Création d'un flux de travail	332
Configuration et exécution d'un flux de travail	333
Afficher les détails du flux de travail	336
Utiliser des étapes prédéfinies	339
Copier le fichier	339
Déchiffrer le fichier	344
Fichier de balises	350
Supprimer le fichier	351
Variables nommées pour les flux de travail	352
Exemple de balise et de flux de travail de suppression	352
Utiliser des étapes de traitement de fichiers personnalisées	357
Utilisation consécutive de plusieurs fonctions Lambda	359
Accès à un fichier après un traitement personnalisé	359
Exemples d'événements envoyés à une adresse AWS Lambda lors du chargement d'un fichier	360
Exemple de fonction Lambda pour une étape de flux de travail personnalisée	362
IAMautorisations pour une étape personnalisée	362
IAMpolitiques relatives aux flux de travail	363
Relations de confiance en matière de flux	365
Exemple de rôle d'exécution : déchiffrer, copier et étiqueter	365

Exemple de rôle d'exécution : Exécuter la fonction et supprimer	367
Gestion des exceptions pour un flux de travail	368
Surveiller l'exécution du flux de	369
CloudWatch journalisation pour un flux de travail	369
CloudWatch métriques pour les flux de travail	372
Créer un flux de travail à partir du modèle	372
Supprimer un flux de travail d'un serveur Transfer Family	376
Restrictions et limites	377
Gestion des serveurs	380
Afficher la liste des serveurs	380
Supprimer un serveur	381
Afficher les détails SFTP du serveur	382
Afficher les détails AS2 du serveur	384
Modifier les détails du serveur	385
Modifier les protocoles de transfert de fichiers	388
Modifier les paramètres du fournisseur d'identité personnalisé	391
Modifier le point de terminaison du serveur	393
Modifier la journalisation	395
Modifier la politique de sécurité	395
Modifier le flux de travail géré	397
Modifier les bannières d'affichage de votre serveur	398
Mettez votre serveur en ligne ou hors ligne	399
Gérer les clés d'hôte du serveur	400
Ajouter une clé d'hôte de serveur supplémentaire	401
Supprimer la clé d'hôte d'un serveur	403
Faites pivoter les clés de l'hôte du serveur	404
Informations supplémentaires sur la clé de l'hôte du serveur	405
Surveiller l'utilisation dans la console	405
Gestion des contrôles d'accès	410
Création d'une politique d'accès au compartiment S3	411
Création d'une politique de session	412
Empêcher les utilisateurs de s'exécuter <code>mkdir</code> dans un compartiment S3	416
Journalisation	417
CloudTrail journalisation	417
Activer la CloudTrail journalisation	419
Exemple d'entrée de journal pour la création d'un serveur	419

CloudWatch journalisation	421
Création d'une journalisation pour les serveurs	422
Gestion de la journalisation des flux de travail	431
Configuration d'un rôle pour CloudWatch	434
Afficher les flux de log de Transfer Family	436
Création d' CloudWatch alarmes Amazon	440
Enregistrement des API appels S3 dans les journaux d'accès S3	440
Exemples pour limiter le problème de confusion des adjoints	441
CloudWatch structure du journal pour Transfer Family	443
Exemples d'entrées de CloudWatch journal	448
Utilisation de CloudWatch métriques	452
Notifications utilisateur	455
Gestion des événements à l'aide de EventBridge	456
Transfer Family événements	457
SFTPFTPS, et événements FTP du serveur	457
SFTPévénements liés aux connecteurs	458
Événements A2S	458
Envoi d' Transfer Family événements	459
Création de modèles d'événements	460
Tester les modèles d'événements pour les Transfer Family événements	461
Autorisations	462
Ressources supplémentaires	462
Référence détaillée des événements	462
Événements liés au serveur	463
Événements relatifs au connecteur	467
AS2événements	472
Sécurité	478
Utilisation des politiques de sécurité	480
Algorithmes cryptographiques	481
TransferSecurityPolicy-2024-01	490
TransferSecurityPolicy-2023-05	491
TransferSecurityPolicy-03	492
TransferSecurityPolicy-2020-06	493
TransferSecurityPolicy-2018-11	494
TransferSecurityPolicy- FIPS -2024-01	495
TransferSecurityPolicy- FIPS -2023-05	497

TransferSecurityPolicy- FIPS -2020-06	498
Politiques de sécurité post-Quantum	499
Politiques de sécurité post-quantique	504
À propos de l'échange de clés hybrides post-quantiques dans SSH	505
Comment l'utiliser	506
Comment le tester	507
Protection des données	511
Chiffrement des données	512
Gestion des clés	514
Gestion des identités et des accès	530
Public ciblé	531
Authentification par des identités	532
Gestion des accès à l'aide de politiques	536
Comment AWS Transfer Family fonctionne avec IAM	538
Exemples de politiques basées sur l'identité	543
Exemples de politique basée sur des balises	546
Résolution des problèmes d'identité et d'accès avec	550
Validation de conformité	552
Résilience	553
Sécurité de l'infrastructure	554
Pare-feu pour applications Web	555
Prévention du problème de l'adjoint confus entre services	556
Rôles des utilisateurs de Transfer Family	558
Rôles du flux de travail Transfer Family	560
Rôles de journalisation et d'invocation Transfer Family	561
AWS politiques gérées	562
AWSTransferConsoleFullAccess	563
AWSTransferFullAccess	565
AWSTransferLoggingAccess	566
AWSTransferReadOnlyAccess	567
Mises à jour des politiques	568
Résolution des problèmes liés à Transfer Family	570
Résoudre les problèmes des utilisateurs gérés par des services	570
Résoudre les problèmes des utilisateurs gérés par le EFS service Amazon	571
Résoudre les problèmes liés à un corps de clé publique trop long	571
Résolution des problèmes : échec de l'ajout de la clé SSH publique	572

Résoudre les problèmes liés à Amazon API Gateway	572
Trop d'échecs d'authentification	572
Connexion fermée	574
Résoudre les problèmes liés aux compartiments Amazon S3 chiffrés	574
Résoudre les problèmes d'authentification	575
Défaillances d'authentification—SSH/SFTP	575
Problème de domaines incompatibles avec Managed AD	576
Problèmes d'authentification divers	576
Résoudre les problèmes liés aux flux de travail gérés	577
Résoudre les erreurs liées au flux de travail à l'aide d'Amazon CloudWatch	577
Résoudre les erreurs de copie du flux de travail	579
Résoudre les problèmes de déchiffrement du flux de travail	579
Résoudre les problèmes liés à Amazon EFS	582
Résoudre les problèmes liés au profil manquant POSIX	582
Résoudre les problèmes liés aux annuaires logiques avec Amazon EFS	583
Résoudre les problèmes liés au test de votre fournisseur d'identité	583
Résoudre les problèmes liés à l'ajout de clés d'hôte fiables pour votre connecteur SFTP	584
Résoudre les problèmes de téléchargement de fichiers	585
Résoudre les erreurs de chargement de fichiers Amazon S3	585
Résoudre les problèmes liés aux noms de fichiers illisibles	585
Résolution des problèmes d'exception ResourceNotFound	586
Résoudre les problèmes liés au SFTP connecteur	587
Échec d'une négociation clé	587
Problèmes de SFTP connexion divers	587
Résolution des problèmes AS2	588
API référence	589
Bienvenue	589
Actions	592
CreateAccess	595
CreateAgreement	603
CreateConnector	609
CreateProfile	617
CreateServer	622
CreateUser	636
CreateWorkflow	645
DeleteAccess	654

DeleteAgreement	657
DeleteCertificate	660
DeleteConnector	662
DeleteHostKey	664
DeleteProfile	667
DeleteServer	669
DeleteSshPublicKey	672
DeleteUser	675
DeleteWorkflow	678
DescribeAccess	681
DescribeAgreement	685
DescribeCertificate	688
DescribeConnector	691
DescribeExecution	694
DescribeHostKey	699
DescribeProfile	702
DescribeSecurityPolicy	705
DescribeServer	709
DescribeUser	714
DescribeWorkflow	719
ImportCertificate	724
ImportHostKey	729
ImportSshPublicKey	733
ListAccesses	738
ListAgreements	742
ListCertificates	746
ListConnectors	750
ListExecutions	754
ListHostKeys	759
ListProfiles	763
ListSecurityPolicies	767
ListServers	771
ListTagsForResource	775
ListUsers	780
ListWorkflows	785
SendWorkflowStepState	788

StartFileTransfer	792
StartServer	799
StopServer	802
TagResource	805
TestConnection	809
TestIdentityProvider	813
UntagResource	820
UpdateAccess	823
UpdateAgreement	831
UpdateCertificate	837
UpdateConnector	841
UpdateHostKey	846
UpdateProfile	850
UpdateServer	853
UpdateUser	866
Types de données	873
As2ConnectorConfig	876
CopyStepDetails	880
CustomStepDetails	883
DecryptStepDetails	885
DeleteStepDetails	888
DescribedAccess	890
DescribedAgreement	894
DescribedCertificate	898
DescribedConnector	902
DescribedExecution	906
DescribedHostKey	909
DescribedProfile	912
DescribedSecurityPolicy	915
DescribedServer	917
DescribedUser	926
DescribedWorkflow	931
EfsFileLocation	933
EndpointDetails	935
ExecutionError	939
ExecutionResults	941

ExecutionStepResult	942
FileLocation	944
HomeDirectoryMapEntry	945
IdentityProviderDetails	947
InputFileLocation	950
ListedAccess	951
ListedAgreement	954
ListedCertificate	957
ListedConnector	960
ListedExecution	962
ListedHostKey	964
ListedProfile	966
ListedServer	968
ListedUser	971
ListedWorkflow	974
LoggingConfiguration	976
PosixProfile	978
ProtocolDetails	980
S3FileLocation	984
S3InputFileLocation	986
S3StorageOptions	988
S3Tag	989
ServiceMetadata	990
SftpConnectorConfig	991
SshPublicKey	993
Tag	995
TagStepDetails	996
UserDetails	998
WorkflowDetail	1000
WorkflowDetails	1002
WorkflowStep	1004
Faire des demandes d'API	1006
Transfer Family a requis les en-têtes de demande	1006
Transfer Family : saisie et signature des demandes	1008
Réponses d'erreur	1009
Bibliothèques disponibles	1011

Paramètres communs	1011
Erreurs courantes	1014
Historique de la documentation	1016
Glossaire AWS	1032
.....	mxxxiii

Qu'est-ce que c'est AWS Transfer Family ?

AWS Transfer Family est un service de transfert sécurisé qui vous permet de transférer des fichiers vers et depuis les services de AWS stockage. Transfer Family fait partie de la AWS Cloud plateforme. AWS Transfer Family offre un support entièrement géré pour le transfert de fichiers SFTP via AS2FTPS,, et FTP directement vers et depuis Amazon S3 ou AmazonEFS. Vous pouvez facilement migrer, automatiser et surveiller vos flux de transfert de fichiers en conservant les configurations existantes côté client pour l'authentification, l'accès et les pare-feux, afin que rien ne change pour vos clients, partenaires et équipes internes, ni pour leurs applications.

Consultez [Getting started with AWS](#) pour en savoir plus et pour commencer à créer des applications cloud avec Amazon Web Services.

AWS Transfer Family prend en charge le transfert de données depuis ou vers les services AWS de stockage suivants.

- Stockage Amazon Simple Storage Service (Amazon S3). Pour plus d'informations sur Amazon S3, consultez [Getting started with Amazon Simple Storage Service](#).
- Systèmes de fichiers Amazon Elastic File System (AmazonEFS) Network File System (NFS). Pour plus d'informations sur AmazonEFS, consultez [Qu'est-ce qu'Amazon Elastic File System ?](#)

AWS Transfer Family prend en charge le transfert de données via les protocoles suivants :

- Protocole de transfert de fichiers Secure Shell (SSHSFTP) : version 3
- Protocole de transfert de fichiers sécurisé (FTPS)
- Protocole de transfert de fichiers (FTP)
- Déclaration d'applicabilité (2) AS2

Note

Pour les connexions de FTPS données FTP et de données, la plage de ports utilisée par Transfer Family pour établir le canal de données est comprise entre 8192 et 8200.

Les protocoles de transfert de fichiers sont utilisés dans les flux de travail d'échange de données dans différents secteurs tels que les services financiers, les soins de santé, la publicité et le

commerce de détail, entre autres. Transfer Family simplifie la migration des flux de transfert de fichiers vers AWS.

Voici quelques exemples d'utilisation courants liés à l'utilisation de Transfer Family avec Amazon S3 :

- Les données proviennent de AWS fuites de données provenant de tiers tels que des fournisseurs et des partenaires.
- Distribution de données à vos clients sur la base d'un abonnement.
- Transferts interne au sein de votre organisation.

Voici quelques exemples d'utilisation courants de Transfer Family avec Amazon EFS :

- Distribution de données
- Chaîne d'approvisionnement
- Gestion de contenu
- Applications de service Web

Voici quelques exemples d'utilisation courants d'utilisation de Transfer Family avec AS2 :

- Des flux de travail avec des exigences de conformité qui reposent sur l'intégration de fonctionnalités de protection et de sécurité des données dans le protocole
- Logistique de la chaîne d'approvisionnement
- Flux de travail des paiements
- Business-to-business transactions (B2B)
- Intégrations avec les systèmes de planification des ressources d'entreprise (ERP) et de gestion de la relation client (CRM)

Avec Transfer Family, vous avez accès à un serveur compatible avec le protocole de transfert de fichiers AWS sans avoir à exécuter d'infrastructure de serveur. Vous pouvez utiliser ce service pour migrer vos flux de travail basés sur le transfert de fichiers AWS tout en conservant les clients et les configurations de vos utilisateurs finaux tels quels. Vous associez d'abord votre nom d'hôte au point de terminaison du serveur, puis vous ajoutez vos utilisateurs et vous leur attribuez le niveau d'accès approprié. Ensuite, les demandes de transfert de vos utilisateurs sont traitées directement depuis le point de terminaison de votre serveur Transfer Family.

Transfer Family offre les avantages suivants :

- Service entièrement géré qui se met à l'échelle en temps réel pour répondre à vos besoins.
- Vous n'avez pas besoin de modifier vos applications ni d'exécuter une infrastructure de protocole de transfert de fichiers.
- Vos données étant stockées dans un espace de stockage durable sur Amazon S3, vous pouvez utiliser le mode natif Services AWS pour les fonctions de traitement, d'analyse, de reporting, d'audit et d'archivage.
- Avec Amazon EFS comme magasin de données, vous bénéficiez d'un système de fichiers élastique entièrement géré à utiliser avec les AWS Cloud services et les ressources sur site. Amazon EFS est conçu pour atteindre des pétaoctets à la demande sans perturber les applications, en augmentant et en diminuant automatiquement au fur et à mesure que vous ajoutez et supprimez des fichiers. Cela permet d'éliminer le besoin de provisionner et de gérer la capacité pour faire face à la croissance.
- Un service de flux de transfert de fichiers entièrement géré et sans serveur qui facilite la configuration, l'exécution, l'automatisation et le suivi du traitement des fichiers téléchargés à l'aide AWS Transfer Family de.
- Vous n'avez pas de coûts initiaux à supporter, et vous payez uniquement en fonction de l'utilisation du service.

Dans les sections suivantes, vous trouverez une description des différentes fonctionnalités de Transfer Family, un didacticiel de démarrage, des instructions détaillées sur la configuration des différents serveurs compatibles avec le protocole, l'utilisation des différents types de fournisseurs d'identité et les API références du service.

Pour commencer à utiliser Transfer Family, consultez ce qui suit :

- [Comment AWS Transfer Family fonctionne](#)
- [Prérequis](#)
- [Commencer à utiliser les points de terminaison AWS Transfer Family de serveur](#)

Comment AWS Transfer Family fonctionne

AWS Transfer Family est un AWS service entièrement géré que vous pouvez utiliser pour transférer des fichiers vers et depuis le stockage Amazon Simple Storage Service (Amazon S3) ou les systèmes de fichiers Amazon Elastic File System (EFSAmazon) via les protocoles suivants :

- Protocole de transfert de fichiers Secure Shell (SSHSFTP) : version 3

- Protocole de transfert de fichiers sécurisé (FTPS)
- Protocole de transfert de fichiers (FTP)
- Déclaration d'applicabilité (2) AS2

AWS Transfer Family prend en charge jusqu'à 3 zones de disponibilité et s'appuie sur un parc redondant à évolutivité automatique pour vos demandes de connexion et de transfert. Pour un exemple sur la manière de renforcer la redondance et de minimiser la latence du réseau en utilisant le routage basé sur la latence, consultez le billet de blog [Minimisez la latence du réseau avec](#) votre transfert pour les serveurs. AWS SFTP

Transfer Family Managed File Transfer Workflows (MFTW) est un service de flux de travail de transfert de fichiers entièrement géré et sans serveur qui facilite la configuration, l'exécution, l'automatisation et le suivi du traitement des fichiers téléchargés à l'aide AWS Transfer Family de. Les clients peuvent MFTW automatiser diverses étapes de traitement telles que la copie, le balisage, la numérisation, le filtrage des données transférées à compressing/decompressing, and encrypting/decrypting l'aide de Transfer Family. Cela fournit une visibilité de bout en bout pour le suivi et l'auditabilité. Pour en savoir plus, consultez [AWS Transfer Family flux de travail gérés](#).

AWS Transfer Family prend en charge n'importe quel client de protocole de transfert de fichiers standard. Certains clients couramment utilisés sont les suivants :

- [Open SSH](#) — Un utilitaire de ligne de commande pour Macintosh et Linux.
- [Win SCP](#) — Un client graphique uniquement pour Windows.
- [Cyberduck](#) — Un client graphique pour Linux, Macintosh et Microsoft Windows.
- [FileZilla](#) — Un client graphique pour Linux, Macintosh et Windows.

Articles de blog pertinents pour Transfer Family

Le tableau suivant répertorie les articles de blog contenant des informations utiles pour les clients de Transfer Family. Le tableau est trié dans l'ordre chronologique inverse, de sorte que les publications les plus récentes figurent au début du tableau.

Titre et lien de l'article de blog	Date
Comment Transfer Family peut vous aider à créer une solution de transfert de fichiers gérée sécurisée et conforme	3 janvier 2024
Déterminez les menaces de logiciels malveillants en utilisant AWS Transfer Family	20 juillet 2023
Élargir SAP les charges de travail avec AWS Transfer Family	13 juillet 2023
Chiffrer et déchiffrer des fichiers avec et PGP AWS Transfer Family	21 juin 2023
Authentification AWS Transfer Family auprès d'Azure Active Directory et AWS Lambda	15 décembre 2022
Personnalisez les notifications de livraison de fichiers à l'aide de workflows AWS Transfer Family gérés	14 octobre 2022
Création d'une plateforme de transfert de fichiers native pour le cloud à l'aide AWS Transfer Family de flux de travail	5 janvier 2022
Permettre la gestion des clés en libre-service aux utilisateurs avec A AWS Transfer Family et AWS Lambda.	17 décembre 2021
Améliorez le contrôle d'accès aux données avec AWS Transfer Family Amazon S3	5 octobre 2021
Améliorez le débit pour les transferts de fichiers via Internet, l'utilisation AWS Global Accelerator et les services AWS Transfer Family	7 juin 2021

Titre et lien de l'article de blog	Date
Sécurisation AWS Transfer Family avec AWS le Web Application Firewall et Amazon API Gateway	5 mai 2021
Sécurisation AWS Transfer Family avec AWS le Web Application Firewall et Amazon API Gateway	15 janvier 2021
AWS Transfer Family support pour Amazon Elastic File System	7 janvier 2021
Activer l'authentification par mot de passe pour AWS Transfer Family l'utilisation AWS Secrets Manager	5 novembre 2020
Centralisez l'accès aux données à l'aide AWS Transfer Family et AWS Storage Gateway	22 juin 2020
Utilisation d'Amazon EFS pour AWS Lambda vos applications sans serveur	18 juin 2020
Utilisez la liste d'adresses IP autorisées pour sécuriser vos AWS Transfer Family serveurs	8 avril 2020
Minimisez la latence du réseau grâce à votre AWS transfert vers les SFTP serveurs	19 février 2020
Migration Lift and Shift des SFTP serveurs vers AWS	12 février 2020
Simplifiez votre AWS SFTP structure avec un chroot et des répertoires logiques	26 septembre 2019
Utiliser Okta en tant que fournisseur d'identité avec AWS Transfer Family	30 mai 2019

Prérequis

Les sections suivantes décrivent les conditions requises pour utiliser le AWS Transfer Family service. Au minimum, vous devez créer un compartiment Amazon Simple Storage Service (Amazon S3) et fournir un accès à ce compartiment via AWS Identity and Access Management un rôle IAM (). Votre rôle doit également établir une relation d'approbation. Cette relation de confiance permet à Transfer Family d'IAM accéder à votre bucket afin de répondre aux demandes de transfert de fichiers de vos utilisateurs.

Rubriques

- [AWS Régions, terminaux et quotas pris en charge](#)
- [Inscrivez-vous pour AWS](#)
- [Configurer le stockage à utiliser avec AWS Transfer Family](#)
- [Création d'un IAM rôle et d'une politique](#)

AWS Régions, terminaux et quotas pris en charge

Pour vous connecter par programmation à un AWS service, vous utilisez un point de terminaison. Par exemple, le point de terminaison pour les clients de la région USA Est (Ohio-east-2) () est `esttransfer.us-east-2.amazonaws.com`. Les quotas de service, également appelés limites, sont le nombre maximal de ressources ou d'opérations de service pour vous Compte AWS. Dans ce guide, vous trouverez les quotas dans [AS2quotas](#) et [Quotas pour les SFTP connecteurs](#).

Pour plus d'informations sur AWS les régions, les points de terminaison et les quotas de service pris en charge, consultez la section [AWS Transfer Family Points de terminaison et quotas](#) dans le. Référence générale d'Amazon Web Services

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez à Amazon Web Services (AWS), votre AWS compte est automatiquement inscrit à tous les services AWS, y compris AWS Transfer Family. Seuls les services que vous utilisez vous sont facturés.

Si vous avez déjà un AWS compte, passez à la tâche suivante. Si vous n'avez pas de compte AWS , observez la procédure suivante pour en créer un.

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 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 AWS est 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 administratif](#), et à utiliser uniquement l'utilisateur racine pour effectuer les [tâches nécessitant un accès utilisateur racine](#).

Pour plus d'informations sur les tarifs et Calculateur de tarification AWS pour obtenir une estimation du coût d'utilisation de Transfer Family, consultez [AWS Transfer Family les tarifs](#).

Pour plus d'informations sur AWS la disponibilité des régions, consultez les [AWS Transfer Family points de terminaison et les quotas](#) dans le Références générales AWS.

Configurer le stockage à utiliser avec AWS Transfer Family

Cette rubrique décrit les options de stockage que vous pouvez utiliser avec AWS Transfer Family. Vous pouvez utiliser Amazon S3 ou Amazon EFS comme espace de stockage pour vos serveurs Transfer Family.

Table des matières

- [Configuration d'un compartiment Amazon S3](#)
 - [Points d'accès Amazon S3](#)
 - [HeadObject Comportement d'Amazon S3](#)
 - [Autoriser uniquement l'écriture et la liste des fichiers](#)
 - [Grand nombre d'objets de zéro octet provoquant des problèmes de latence](#)
- [Configuration d'un système de EFS fichiers Amazon](#)
 - [Propriété des EFS fichiers Amazon](#)
 - [Configurer les EFS utilisateurs Amazon pour Transfer Family](#)

- [Configurer les utilisateurs de Transfer Family sur Amazon EFS](#)
- [Création d'un utilisateur EFS root Amazon](#)
- [EFSCommandes Amazon prises en charge](#)

Configuration d'un compartiment Amazon S3

AWS Transfer Family accède à votre compartiment Amazon S3 pour répondre aux demandes de transfert de vos utilisateurs. Vous devez donc fournir un compartiment Amazon S3 dans le cadre de la configuration de votre serveur compatible avec le protocole de transfert de fichiers. Vous pouvez utiliser un compartiment existant ou en créer un nouveau.

Note

Vous n'êtes pas obligé d'utiliser un serveur et un compartiment Amazon S3 situés dans la même AWS région, mais nous vous recommandons de le faire en tant que bonne pratique.

Lorsque vous configurez vos utilisateurs, vous leur attribuez un IAM rôle à chacun. Ce rôle détermine le niveau d'accès dont ils disposent à votre compartiment Amazon S3.

Pour plus d'informations sur la création d'un nouveau compartiment, consultez [Comment créer un compartiment S3 ?](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Note

Vous pouvez utiliser Amazon S3 Object Lock pour empêcher le remplacement d'objets pendant une durée déterminée ou indéfiniment. Cela fonctionne de la même manière avec Transfer Family qu'avec les autres services. Si un objet existe et est protégé, il est interdit d'écrire dans ce fichier ou de le supprimer. Pour plus de détails sur Amazon S3 Object Lock, consultez la section [Utilisation d'Amazon S3 Object Lock](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Points d'accès Amazon S3

AWS Transfer Family prend en charge les [points d'accès Amazon S3](#), une fonctionnalité d'Amazon S3 qui vous permet de gérer facilement l'accès granulaire aux ensembles de données partagés. Vous

pouvez utiliser des alias de point d'accès S3 partout où vous utilisez un nom de compartiment S3. Vous pouvez créer des centaines de points d'accès dans Amazon S3 pour les utilisateurs disposant d'autorisations différentes pour accéder aux données partagées dans un compartiment Amazon S3.

Par exemple, vous pouvez utiliser des points d'accès pour permettre à trois équipes différentes d'avoir accès au même ensemble de données partagé dans lequel une équipe peut lire les données de S3, une deuxième équipe peut écrire des données dans S3 et la troisième équipe peut lire, écrire et supprimer des données de S3. Pour mettre en œuvre un contrôle d'accès granulaire tel que mentionné ci-dessus, vous pouvez créer un point d'accès S3 contenant une politique qui donne un accès asymétrique aux différentes équipes. Vous pouvez utiliser les points d'accès S3 avec votre serveur Transfer Family pour obtenir un contrôle d'accès précis, sans créer de politique de compartiment S3 complexe couvrant des centaines de cas d'utilisation. Pour en savoir plus sur l'utilisation des points d'accès S3 avec un serveur Transfer Family, consultez le billet de blog [Enhance data access control with AWS Transfer Family et Amazon S3](#).

Note

AWS Transfer Family ne prend actuellement pas en charge les points d'accès multirégionaux Amazon S3.

HeadObject Comportement d'Amazon S3

Note

Lorsque vous créez ou mettez à jour un serveur Transfer Family, vous pouvez optimiser les performances de vos annuaires Amazon S3, ce qui élimine les HeadObject appels.

Dans Amazon S3, les compartiments et les objets sont les ressources principales, et les objets sont stockés dans des compartiments. Amazon S3 peut imiter un système de fichiers hiérarchique, mais peut parfois se comporter différemment d'un système de fichiers classique. Par exemple, les annuaires ne constituent pas un concept de premier ordre dans Amazon S3, mais sont basés sur des clés d'objet. AWS Transfer Family déduit un chemin de répertoire en divisant la clé d'un objet par la barre oblique (/), en traitant le dernier élément comme nom de fichier, puis en regroupant les noms de fichiers portant le même préfixe sous le même chemin. Les objets de zéro octet sont créés pour représenter le chemin d'un dossier lorsque vous créez un répertoire vide à l'aide `mkdir` ou à l'aide de la console Amazon S3. La touche correspondant à ces objets se termine par une barre oblique. Ces

objets de zéro octet sont décrits dans la section [Organisation des objets dans la console Amazon S3 à l'aide de dossiers](#) du guide de l'utilisateur Amazon S3.

Lorsque vous exécutez une `ls` commande et que certains résultats correspondent à des objets Amazon S3 sans octet (les touches de ces objets se terminent par une barre oblique), Transfer Family émet une `HeadObject` demande pour chacun de ces objets (voir [HeadObject](#) le manuel Amazon Simple Storage Service API Reference pour plus de détails). Cela peut entraîner les problèmes suivants lorsque vous utilisez Amazon S3 comme espace de stockage avec Transfer Family.

Autoriser uniquement l'écriture et la liste des fichiers

Dans certains cas, vous souhaitez peut-être n'offrir qu'un accès en écriture à vos objets Amazon S3. Par exemple, vous pouvez autoriser l'accès pour écrire (ou télécharger) et répertorier des objets dans un bucket, mais pas pour lire (télécharger) des objets. Pour exécuter `ls` des `mkdir` commandes à l'aide de clients de transfert de fichiers, vous devez disposer de l'Amazon S3 `ListObjects` et `PutObject` des autorisations. Toutefois, lorsque Transfer Family doit effectuer un `HeadObject` appel pour écrire ou répertorier des fichiers, l'appel échoue avec le message d'erreur « Accès refusé », car cet appel nécessite une `GetObject` autorisation.

Note

Lorsque vous créez ou mettez à jour un serveur Transfer Family, vous pouvez optimiser les performances de vos annuaires Amazon S3, ce qui élimine les `HeadObject` appels.

Dans ce cas, vous pouvez accorder l'accès en ajoutant une condition de politique AWS Identity and Access Management (IAM) qui ajoute l'`GetObject` autorisation uniquement pour les objets se terminant par une barre oblique (/). Cette condition empêche les `GetObject` appels sur des fichiers (afin qu'ils ne puissent pas être lus), mais permet à l'utilisateur de répertorier et de parcourir des dossiers. L'exemple de politique suivant offre uniquement un accès en écriture et en liste à vos compartiments Amazon S3. Pour utiliser cette politique, *DOC-EXAMPLE-BUCKET* remplacez-la par le nom de votre compartiment.

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

```

    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
  },
  {
    "Sid": "AllowReadWrite",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": [
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ]
  },
  {
    "Sid": "DenyIfNotFolder",
    "Effect": "Deny",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "NotResource": [
      "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/"
    ]
  }
]
}

```

Note

Cette règle n'autorise pas les utilisateurs à ajouter des fichiers. En d'autres termes, un utilisateur auquel cette politique est affectée ne peut pas ouvrir de fichiers pour y ajouter du contenu ou pour les modifier. De plus, si votre cas d'utilisation nécessite un `HeadObject` appel avant de télécharger un fichier, cette politique ne fonctionnera pas pour vous.

Grand nombre d'objets de zéro octet provoquant des problèmes de latence

Si vos compartiments Amazon S3 contiennent un grand nombre de ces objets de zéro octet, Transfer Family émet de nombreux `HeadObject` appels, ce qui peut entraîner des retards de traitement.

L'une des solutions possibles à ce problème consiste à supprimer tous vos objets de zéro octet.

Notez ce qui suit :

- Les répertoires vides n'existeront plus. Les répertoires n'existent que parce que leurs noms figurent dans la clé d'un objet.
- Cela n'empêche pas quelqu'un d'appeler `mkdir` et de tout casser à nouveau. Vous pouvez atténuer ce problème en élaborant une politique qui empêche la création de répertoires.
- Certains scénarios utilisent ces objets de 0 octet. Par exemple, vous avez une structure telle que `/inboxes/customer1000` et le répertoire de la boîte de réception est nettoyé tous les jours.

Une autre solution possible consiste à limiter le nombre d'objets visibles par le biais d'une condition de politique afin de réduire le nombre d'`HeadObject` appels. Pour que cette solution soit viable, vous devez accepter le fait que vous ne pourrez peut-être afficher qu'un ensemble limité de tous vos sous-répertoires.

Configuration d'un système de EFS fichiers Amazon

AWS Transfer Family accède à Amazon Elastic File System (AmazonEFS) pour traiter les demandes de transfert de vos utilisateurs. Vous devez donc fournir un système de EFS fichiers Amazon dans le cadre de la configuration de votre serveur compatible avec le protocole de transfert de fichiers. Vous pouvez utiliser un système de fichiers existant ou en créer un nouveau.

Notez ce qui suit :

- Lorsque vous utilisez un serveur Transfer Family et un système de EFS fichiers Amazon, le serveur et le système de fichiers doivent se trouver dans le même emplacement Région AWS.
- Il n'est pas nécessaire que le serveur et le système de fichiers soient sur le même compte. Si le serveur et le système de fichiers ne sont pas dans le même compte, la politique du système de fichiers doit accorder une autorisation explicite au rôle d'utilisateur.

Pour plus d'informations sur la configuration de plusieurs comptes, consultez la section [Gestion des AWS comptes de votre organisation](#) dans le Guide de AWS Organizations l'utilisateur.

- Lorsque vous configurez vos utilisateurs, vous leur attribuez un IAM rôle à chacun. Ce rôle détermine le niveau d'accès dont ils disposent à votre système de EFS fichiers Amazon.
- Pour plus de détails sur le montage d'un système de EFS fichiers Amazon, consultez [Montage de systèmes de EFS fichiers Amazon](#).

Pour en savoir plus sur la manière dont AWS Transfer Family Amazon EFS travaille ensemble, consultez la section [Utiliser AWS Transfer Family pour accéder aux fichiers de votre système de EFS fichiers Amazon](#) dans le guide de l'utilisateur d'Amazon Elastic File System.

Propriété des EFS fichiers Amazon

Amazon EFS utilise le modèle d'autorisation de fichier Portable Operating System Interface (POSIX) pour représenter la propriété des fichiers.

Dans POSIX, les utilisateurs du système sont classés en trois classes d'autorisations distinctes : lorsque vous autorisez un utilisateur à accéder à des fichiers stockés dans un système de EFS fichiers Amazon en utilisant AWS Transfer Family, vous devez lui attribuer un « POSIX profil ». Ce profil est utilisé pour déterminer leur accès aux fichiers et aux répertoires du système de EFS fichiers Amazon.

- Utilisateur (u) : propriétaire du fichier ou du répertoire. Généralement, le créateur d'un fichier ou d'un répertoire en est également le propriétaire.
- Groupe (g) : ensemble d'utilisateurs qui ont besoin d'un accès identique aux fichiers et aux répertoires qu'ils partagent.
- Autres (o) : tous les autres utilisateurs ayant accès au système, à l'exception du propriétaire et des membres du groupe. Cette classe d'autorisation est également appelée « publique ».

Dans le modèle d'POSIX autorisation, chaque objet du système de fichiers (fichiers, répertoires, liens symboliques, canaux nommés et sockets) est associé aux trois ensembles d'autorisations mentionnés précédemment. Un mode de style Unix est associé aux EFS objets Amazon. La valeur de ce mode définit les autorisations permettant d'effectuer des actions au niveau de cet objet.

En outre, sur les systèmes de type Unix, les utilisateurs et les groupes sont mappés à des identifiants numériques, qu'EFS Amazon utilise pour représenter la propriété des fichiers. Pour Amazon EFS, les objets appartiennent à un seul propriétaire et à un seul groupe. Amazon EFS utilise le chiffre mappé IDs pour vérifier les autorisations lorsqu'un utilisateur tente d'accéder à un objet du système de fichiers.

Configurer les EFS utilisateurs Amazon pour Transfer Family

Avant de configurer vos EFS utilisateurs Amazon, vous pouvez effectuer l'une des opérations suivantes :

- Vous pouvez créer des utilisateurs et configurer leurs dossiers personnels sur AmazonEFS. Consultez [Configurer les utilisateurs de Transfer Family sur Amazon EFS](#) pour plus de détails.
- Si vous êtes à l'aise avec l'ajout d'un utilisateur root, vous pouvez le faire [Création d'un utilisateur EFS root Amazon](#).

 Note

Les serveurs Transfer Family ne prennent pas en charge les points EFS d'accès Amazon pour définir POSIX des autorisations. POSIX Les profils des utilisateurs de Transfer Family (décrits dans la section précédente) offrent la possibilité de définir POSIX des autorisations. Ces autorisations sont définies au niveau de l'utilisateur, pour un accès granulaire, basé sur UIDGID, et secondaireGIDs.

Configurer les utilisateurs de Transfer Family sur Amazon EFS

Transfer Family associe les utilisateurs à ceux qui n'UID/GID and directories you specify. If the UID/GID/directories existent pas déjà. Vous devez alors les créer avant de les attribuer dans Transfer à un utilisateur. EFS Les détails relatifs à la création d'EFS utilisateurs Amazon sont décrits dans la section [Travailler avec les utilisateurs, les groupes et les autorisations au niveau du système de fichiers réseau \(NFS\)](#) du guide de l'utilisateur Amazon Elastic File System.

Étapes pour configurer EFS les utilisateurs Amazon dans Transfer Family

1. Mappez le EFS UID et GID pour votre utilisateur dans Transfer Family à l'aide [PosixProfile](#) des champs.
2. Si vous souhaitez que l'utilisateur démarre dans un dossier spécifique lors de la connexion, vous pouvez spécifier le EFS répertoire sous le [HomeDirectory](#) champ.

Vous pouvez automatiser le processus à l'aide d'une CloudWatch règle et d'une fonction Lambda. Pour un exemple de fonction Lambda qui interagit avec EFS, consultez Utiliser [Amazon EFS pour vos applications sans AWS Lambda serveur](#).

En outre, vous pouvez configurer des répertoires logiques pour vos utilisateurs de Transfer Family. Pour plus de détails, consultez la [Configuration de répertoires logiques pour Amazon EFS](#) section de cette [Utilisation de répertoires logiques pour simplifier vos structures de répertoires Transfer Family](#) rubrique.

Création d'un utilisateur EFS root Amazon

Si votre organisation accepte que vous autorisiez l'accès des utilisateurs root via SFTP/FTP pour la configuration de vos utilisateurs, vous pouvez créer un utilisateur qui est UID 0 (utilisateur root), puis utiliser cet utilisateur root pour créer des dossiers et attribuer des propriétaires d'POSIXID aux autres utilisateurs. L'avantage de cette option est qu'il n'est pas nécessaire de monter le système de fichiers Amazon EFS.

Suivez les étapes décrites dans [Ajouter des utilisateurs gérés par le EFS service Amazon](#), et entrez 0 (zéro) pour l'ID utilisateur et l'ID de groupe.

Commandes Amazon EFS prises en charge

Les commandes suivantes sont prises en charge par Amazon EFS pour AWS Transfer Family.

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`: Seul le root (c'est-à-dire les utilisateurs avec uid=0) peut modifier la propriété et les autorisations des fichiers et des répertoires.
- `chmod`: Seul le superutilisateur peut modifier la propriété et les autorisations des fichiers et des répertoires.
- `chgrp`: Pris en charge soit pour le root, soit pour le propriétaire du fichier, qui ne peut modifier le groupe d'un fichier que pour en faire l'un de ses groupes secondaires.
- `ln -s/symlink`
- `mkdir`
- `rm/delete`
- `rmdir`
- `chmtime`

Création d'un IAM rôle et d'une politique

Cette rubrique décrit les types de politiques et de rôles qui peuvent être utilisés et décrit le processus de création d'un rôle utilisateur. AWS Transfer Family II décrit également le fonctionnement des politiques de session et fournit un exemple de rôle utilisateur.

AWS Transfer Family utilise les types de rôles suivants :

- Rôle utilisateur — Permet aux utilisateurs gérés par le service d'accéder aux ressources Transfer Family nécessaires. AWS Transfer Family assume ce rôle dans le contexte d'un utilisateur de Transfer FamilyARN.
- Rôle d'accès — Permet d'accéder uniquement aux fichiers Amazon S3 en cours de transfert. Pour les AS2 transferts entrants, le rôle d'accès utilise le nom de ressource Amazon (ARN) pour l'accord. Pour les AS2 transferts sortants, le rôle d'accès utilise le ARN pour le connecteur.
- Rôle d'invocation : à utiliser avec Amazon API Gateway en tant que fournisseur d'identité personnalisé du serveur. Transfer Family assume ce rôle dans le contexte d'un serveur Transfer FamilyARN.
- Rôle de journalisation : utilisé pour enregistrer les entrées sur Amazon CloudWatch. Transfer Family utilise ce rôle pour enregistrer les informations relatives aux réussites et aux échecs ainsi que les informations relatives aux transferts de fichiers. Transfer Family assume ce rôle dans le contexte d'un serveur Transfer FamilyARN. Pour les AS2 transferts sortants, le rôle de journalisation utilise le connecteurARN.
- Rôle d'exécution — Permet à un utilisateur de Transfer Family d'appeler et de lancer des flux de travail. Transfer Family assume ce rôle dans le contexte d'un flux de travail Transfer FamilyARN.

Outre ces rôles, vous pouvez également utiliser des politiques de session. Une politique de session est utilisée pour limiter l'accès lorsque cela est nécessaire. Notez que ces politiques sont autonomes, c'est-à-dire que vous ne les ajoutez pas à un rôle. Vous ajoutez plutôt une politique de session directement à un utilisateur de Transfer Family.

Note

Lorsque vous créez un utilisateur Transfer Family géré par un service, vous pouvez sélectionner Générer automatiquement une politique en fonction du dossier de base. Il s'agit d'un raccourci utile si vous souhaitez limiter l'accès des utilisateurs à leurs propres dossiers. Vous pouvez également consulter des détails sur les politiques de session et un exemple dans [Comment fonctionnent les politiques de session](#). Vous trouverez également

plus d'informations sur les politiques de session dans la section [Politiques de session](#) du Guide de IAM l'utilisateur.

Rubriques

- [Créer un rôle d'utilisateur](#)
- [Comment fonctionnent les politiques de session](#)
- [Exemple de politique d'accès en lecture/écriture](#)

Créer un rôle d'utilisateur

Lorsque vous créez un utilisateur, vous prenez un certain nombre de décisions concernant son accès. Ces décisions incluent les compartiments Amazon S3 ou les systèmes de EFS fichiers Amazon auxquels l'utilisateur peut accéder, les parties de chaque compartiment Amazon S3 et les fichiers du système de fichiers accessibles, ainsi que les autorisations dont dispose l'utilisateur (par exemple, PUT ou GET).

Pour définir l'accès, vous créez une politique et un rôle basés sur l'identité AWS Identity and Access Management (IAM) qui fournissent ces informations d'accès. Dans le cadre de ce processus, vous permettez à votre utilisateur d'accéder au compartiment Amazon S3 ou au système de EFS fichiers Amazon qui est la cible ou la source des opérations sur les fichiers. Pour ce faire, effectuez les étapes générales suivantes, décrites plus loin en détail :

Créer un rôle d'utilisateur

1. Créez une IAM politique pour AWS Transfer Family. Ceci est décrit dans [Pour créer une IAM politique pour AWS Transfer Family](#).
2. Créez un IAM rôle et associez la nouvelle IAM politique. Pour obtenir un exemple, consultez [Exemple de politique d'accès en lecture/écriture](#).
3. Établissez une relation de confiance entre AWS Transfer Family et le IAM rôle. Ceci est décrit dans [Étape 1 : Établir une relation d'approbation](#).

Les procédures suivantes décrivent comment créer une IAM politique et un rôle.

Pour créer une IAM politique pour AWS Transfer Family

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

2. Dans le volet de navigation, sélectionnez Politiques, puis Créer une politique.
3. Sur la page Créer une politique, choisissez l'JSONonglet.
4. Dans l'éditeur qui apparaît, remplacez le contenu de l'éditeur par la IAM politique que vous souhaitez associer au IAM rôle.

Vous pouvez accorder un accès en lecture/écriture ou restreindre l'accès des utilisateurs à leur répertoire personnel. Pour de plus amples informations, veuillez consulter [Exemple de politique d'accès en lecture/écriture](#).

5. Choisissez Réviser la politique et fournissez un nom et une description pour votre politique, puis choisissez Créer une politique.

Ensuite, vous créez un IAM rôle et vous y associez la nouvelle IAM politique.

Pour créer un IAM rôle pour AWS Transfer Family

1. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.

Sur la page Créer un rôle, assurez-vous que le AWS service est sélectionné.
2. Choisissez Transfer (Transférer) dans la liste des services, puis Next: Permissions (Suivant : Autorisations). Cela établit une relation de confiance entre AWS Transfer Family et AWS.
3. Dans la section Joindre des politiques d'autorisation, recherchez et choisissez la politique que vous venez de créer, puis choisissez Next : Tags.
4. (Facultatif) Entrez une clé et une valeur pour une balise, puis choisissez Next: Review (Suivant : Vérifier).
5. Sur la page Review (Vérifier), entrez un nom et une description pour votre nouveau rôle, puis choisissez Create role (Créer un rôle).

Ensuite, vous établissez une relation de confiance entre AWS Transfer Family et AWS.

Étape 1 : Établir une relation d'approbation

Note

Dans nos exemples, nous utilisons à la fois `ArnLike` et `ArnEquals`. Ils sont fonctionnellement identiques et vous pouvez donc utiliser l'un ou l'autre lorsque vous élaborer vos politiques. La documentation Transfer Family `ArnLike` est utilisée lorsque

la condition contient un caractère générique et `ArnEquals` pour indiquer une condition de correspondance exacte.

1. Dans la IAM console, choisissez le rôle que vous venez de créer.
2. Sur la page Récapitulatif, choisissez Relations d'approbation, puis choisissez Modifier la relation d'approbation.
3. Dans l'éditeur Modifier une relation de confiance, assurez-vous que le service est `transfer.amazonaws.com`. La politique d'accès est illustrée ci-dessous.

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

Nous vous recommandons d'utiliser les clés de condition `aws:SourceAccount` et `aws:SourceArn` pour vous protéger contre le problème de l'adjoint confus. Le compte source est le propriétaire du serveur et la source ARN est celle ARN de l'utilisateur. Par exemple :

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "account_id"
  },
  "ArnLike": {
    "aws:SourceArn": "arn:aws:transfer:region:account_id:user/*"
  }
}
```

Vous pouvez également utiliser `ArnLike` cette condition si vous souhaitez vous limiter à un serveur en particulier plutôt qu'à n'importe quel serveur du compte utilisateur. Par exemple :

```
"Condition": {
  "ArnLike": {
    "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/*"
  }
}
```

Note

Dans les exemples ci-dessus, remplacez chaque *user input placeholder* avec vos propres informations.

Pour plus de détails sur le problème des députés confus et d'autres exemples, voir [Prévention du problème de l'adjoint confus entre services](#).

4. Choisissez Mettre à jour la politique de confiance pour mettre à jour la politique d'accès.

Vous avez maintenant créé un IAM rôle qui permet d' AWS Transfer Family appeler AWS les services en votre nom. Vous avez associé au rôle la IAM politique que vous avez créée pour donner accès à votre utilisateur. Dans la [Commencer à utiliser les points de terminaison AWS Transfer Family de serveur](#) section, ce rôle et cette politique sont attribués à votre ou vos utilisateurs.

Voir aussi

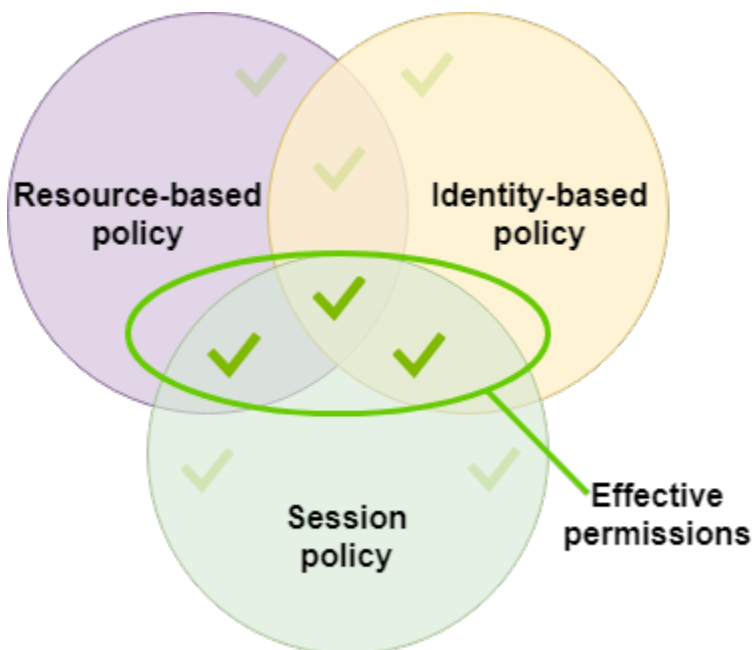
- Pour des informations plus générales sur IAM les rôles, voir [Création d'un rôle pour déléguer des autorisations à un AWS service](#) dans le Guide de IAM l'utilisateur.
- Pour en savoir plus sur les politiques basées sur l'identité pour les ressources Amazon S3, consultez la section [Gestion des identités et des accès dans Amazon S3](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.
- Pour en savoir plus sur les politiques basées sur l'identité applicables aux EFS ressources Amazon, consultez la section [Utiliser IAM pour contrôler l'accès aux données du système de fichiers](#) dans le manuel Amazon Elastic File System User Guide.

Comment fonctionnent les politiques de session

Lorsqu'un administrateur crée un rôle, celui-ci inclut souvent des autorisations étendues pour couvrir plusieurs cas d'utilisation ou plusieurs membres de l'équipe. Si un administrateur configure une

[console URL](#), il peut réduire les autorisations pour la session qui en résulte en utilisant une politique de session. Par exemple, si vous créez un rôle avec un [accès en lecture/écriture](#), vous pouvez en configurer un URL qui limite l'accès des utilisateurs à leurs seuls répertoires personnels.

Les politiques de session sont des politiques avancées que vous transmettez en paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur. Les politiques de session sont utiles pour verrouiller les utilisateurs afin qu'ils n'aient accès qu'aux parties de votre compartiment où les préfixes d'objets contiennent leur nom d'utilisateur. Le schéma suivant montre que les autorisations de la politique de session sont l'intersection des politiques de session et des politiques basées sur les ressources, ainsi que l'intersection des politiques de session et des politiques basées sur l'identité.



Pour plus de détails, consultez les [politiques de session](#) dans le guide de IAM l'utilisateur.

Dans AWS Transfer Family, une politique de session n'est prise en charge que lorsque vous effectuez un transfert vers ou depuis Amazon S3. L'exemple de politique suivant est une stratégie de session qui limite l'accès des utilisateurs à leurs home annuaires uniquement. Notez ce qui suit :

- Les PutObjectACL relèvent GetObjectACL et ne sont nécessaires que si vous devez activer l'accès multicompte. En d'autres termes, votre serveur Transfer Family doit accéder à un bucket d'un autre compte.
- La longueur maximale d'une politique de session est de 2 048 caractères. Pour plus de détails, consultez le [paramètre de demande de politique](#) pour l>CreateUseraction dans la APIréférence.

- Si votre compartiment Amazon S3 est chiffré à l'aide de AWS Key Management Service (AWS KMS), vous devez spécifier des autorisations supplémentaires dans votre politique. Pour plus de détails, consultez [Chiffrement des données dans Amazon S3](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::${transfer:HomeBucket}"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "${transfer:HomeFolder}/*",
            "${transfer:HomeFolder}"
          ]
        }
      }
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
    }
  ]
}
```

 Note

L'exemple de politique précédent suppose que le répertoire personnel des utilisateurs est configuré pour inclure une barre oblique finale, pour indiquer qu'il s'agit d'un répertoire. Si, par contre, vous définissez le nom d'un utilisateur `HomeDirectory` sans la barre oblique finale, vous devez l'inclure dans votre politique.

Dans l'exemple de stratégie précédent, notez l'utilisation des paramètres de `transfer:HomeDirectory` stratégie `transfer:HomeFolder` `transfer:HomeBucket`, et. Ces paramètres sont définis pour `HomeDirectory` ce qui est configuré pour l'utilisateur, comme décrit dans [HomeDirectory](#) et [Implémentation de votre méthode API Gateway](#). Ces paramètres ont les définitions suivantes :

- Le `transfer:HomeBucket` paramètre est remplacé par le premier composant de `HomeDirectory`.
- Le `transfer:HomeFolder` paramètre est remplacé par les parties restantes du `HomeDirectory` paramètre.
- La barre oblique (/) initiale du `transfer:HomeDirectory` paramètre a été supprimée afin de pouvoir être utilisé dans le cadre d'un nom de ressource Amazon S3 (ARN) dans une `Resource` instruction.

 Note

Si vous utilisez des répertoires logiques, c'est-à-dire ceux de l'utilisateur, `LOGICAL` ces paramètres de `homeDirectoryType` stratégie (`HomeBucketHomeDirectory`, et `HomeFolder`) ne sont pas pris en charge.

Supposons, par exemple, que le `HomeDirectory` paramètre configuré pour l'utilisateur `Transfer Family` soit `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` est réglé sur `home`.
- `transfer:HomeFolder` est réglé sur `/bob/amazon/stuff/`.
- `transfer:HomeDirectory` devient `home/bob/amazon/stuff/`.

Le premier "Sid" permet à l'utilisateur de répertorier tous les répertoires à partir de `/home/bob/amazon/stuff/`.

La seconde "Sid" limite l'utilisateur put et l'get accès à ce même chemin, `/home/bob/amazon/stuff/`.

Exemple de politique d'accès en lecture/écriture

Accorder un accès en lecture/écriture au compartiment Amazon S3

L'exemple de politique suivant AWS Transfer Family accorde un accès en lecture/écriture aux objets de votre compartiment Amazon S3.

Notez ce qui suit :

- Remplacez ***DOC-EXAMPLE-BUCKET*** avec le nom de votre compartiment Amazon S3.
- Les PutObjectACL relevés GetObjectACL et ne sont nécessaires que si vous devez activer l'accès multicompte. En d'autres termes, votre serveur Transfer Family doit accéder à un bucket d'un autre compte.
- Les DeleteObjectVersion instructions GetObjectVersion and ne sont requises que si le versionnement est activé sur le compartiment Amazon S3 auquel on accède.

Note

Si vous avez déjà activé la gestion des versions pour votre compartiment, vous avez besoin de ces autorisations, car vous ne pouvez suspendre la gestion des versions que dans Amazon S3, et non la désactiver complètement. Pour plus de détails, consultez les sections Buckets [non versionnés, activés pour le versionnement et Suspendus](#) des versions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],

```

```

        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ],
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    }
]
}

```

Autoriser le système de fichiers à accéder aux fichiers EFS du système de fichiers Amazon

Note

Outre la politique, vous devez également vous assurer que les autorisations relatives à vos POSIX fichiers accordent l'accès approprié. Pour plus d'informations, consultez la section [Travailler avec les utilisateurs, les groupes et les autorisations au niveau du système de fichiers réseau \(NFS\)](#) dans le guide de l'utilisateur d'Amazon Elastic File System.

L'exemple de politique suivant accorde au système de fichiers racine l'accès aux fichiers de votre système de EFS fichiers Amazon.

Note

Dans les exemples suivants, remplacez *region* avec votre région, *account-id* avec le compte dans lequel se trouve le fichier, et *file-system-id* avec l'ID de votre Amazon Elastic File System (AmazonEFS).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RootFileSystemAccess",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id"
    }
  ]
}
```

L'exemple de politique suivant accorde à l'utilisateur l'accès au système de fichiers aux fichiers de votre système de EFS fichiers Amazon.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UserFileSystemAccess",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource": "arn:aws:elasticfilesystem:region:account-id:file-system/file-system-id"
    }
  ]
}
```

Tutoriels Transfer Family

Le guide de AWS Transfer Family l'utilisateur fournit des instructions détaillées pour plusieurs cas d'utilisation.

- [Commencer à utiliser les points de terminaison AWS Transfer Family de serveur](#): ce didacticiel explique comment créer un serveur SFTP Transfer Family et un utilisateur géré par des services, puis explique comment transférer un fichier à l'aide d'un client.
- [Configuration et utilisation des SFTP connecteurs](#): ce didacticiel explique comment configurer un SFTP connecteur, puis transférer des fichiers entre le stockage Amazon S3 et un SFTP serveur.
- [Configuration d'une méthode Amazon API Gateway en tant que fournisseur d'identité personnalisé](#) : ce didacticiel explique comment configurer une méthode Amazon API Gateway et comment l'utiliser en tant que fournisseur d'identité personnalisé pour télécharger des fichiers sur un AWS Transfer Family serveur.
- [Configuration d'un flux de travail géré pour le déchiffrement d'un fichier](#): ce didacticiel explique comment configurer un flux de travail géré contenant une étape de déchiffrement, et comment télécharger un fichier chiffré dans un compartiment Amazon S3, puis afficher le fichier déchiffré.
- [Configuration d'une AS2 configuration](#): ce didacticiel décrit les étapes nécessaires à la configuration d'un serveur AS2 Transfer Family. Il existe des instructions pour importer des certificats, créer des profils et des accords, éventuellement créer un AS2 connecteur, puis tester la configuration.

Rubriques

- [Commencer à utiliser les points de terminaison AWS Transfer Family de serveur](#)
- [Configuration d'un flux de travail géré pour le déchiffrement d'un fichier](#)
- [Configuration et utilisation des SFTP connecteurs](#)
- [Configuration d'une méthode Amazon API Gateway en tant que fournisseur d'identité personnalisé](#)
- [Configuration d'une AS2 configuration](#)

Commencer à utiliser les points de terminaison AWS Transfer Family de serveur

Utilisez ce tutoriel pour démarrer avec AWS Transfer Family (Transfer Family). Vous apprendrez à créer un serveur SFTP compatible avec un point de terminaison accessible au public à l'aide du stockage Amazon S3, à ajouter un utilisateur avec une authentification gérée par le service et à transférer un fichier avec Cyberduck.

Rubriques

- [Prérequis](#)
- [Étape 1 : Se connecter à la console AWS Transfer Family](#)
- [Étape 2 : Création d'un SFTP serveur compatible](#)
- [Étape 3 : Ajouter un utilisateur géré par le service](#)
- [Étape 4 : Transférer un fichier à l'aide d'un client](#)

Prérequis

Avant de commencer, assurez-vous de remplir les conditions requises dans [Prérequis](#). Dans le cadre de cette configuration, vous créez un bucket Amazon Simple Storage Service (Amazon S3) et AWS Identity and Access Management un rôle utilisateur IAM ().

Des autorisations sont requises pour utiliser la AWS Transfer Family console et des autorisations sont requises pour configurer d'autres AWS services utilisés par Transfer Family, tels qu'Amazon Simple Storage Service AWS Certificate Manager, Amazon Elastic File System et Amazon Route 53. Par exemple, pour les utilisateurs qui transfèrent des fichiers depuis et vers Transfer Family à AWS l'aide de Transfer Family, AmazonS3 FullAccess accorde les autorisations nécessaires pour configurer et utiliser un compartiment Amazon S3. Certaines des autorisations définies dans cette politique sont nécessaires pour créer des compartiments Amazon S3.

Pour utiliser la console Transfer Family, vous avez besoin des éléments suivants :

- AWSTransferConsoleFullAccess autorise votre SFTP utilisateur à créer des ressources Transfer Family.
- IAMFullAccess(ou plus précisément une politique autorisant la création de IAM rôles) n'est nécessaire que si vous souhaitez que Transfer Family crée automatiquement un rôle de

journalisation pour votre serveur dans Amazon CloudWatch Logs ou un rôle d'utilisateur pour un utilisateur se connectant à un serveur.

- Pour créer et supprimer des types de VPC serveurs, vous devez ajouter les actions `ec2 : CreateVpcEndpoint` et `ec2 : DeleteVpcEndpoints` à votre politique.

Note

L'AmazonS3 FullAccess et IAMFullAccess politiques ne sont en eux-mêmes pas nécessaires pour une utilisation générale de. AWS Transfer Family Elles sont présentées ici comme un moyen simple de s'assurer que toutes les autorisations dont vous avez besoin sont couvertes. En outre, il s'agit de politiques AWS gérées, qui sont des politiques standard disponibles pour tous les AWS clients. Vous pouvez consulter les autorisations individuelles dans ces politiques et déterminer l'ensemble minimal dont vous avez besoin pour vos besoins.

Étape 1 : Se connecter à la console AWS Transfer Family

Pour vous connecter à Transfer Family

1. Connectez-vous à la AWS Transfer Family console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le champ ID de compte ou alias, entrez l'ID de votre Compte AWS.
3. Pour le nom IAM d'utilisateur, entrez le nom du rôle utilisateur que vous avez créé pour Transfer Family.
4. Dans Mot de passe, saisissez le mot de passe de votre AWS compte.
5. Choisissez Sign in (Connexion).

Étape 2 : Création d'un SFTP serveur compatible

Le protocole de transfert de fichiers Secure Shell (SSH/SFTP) est un protocole réseau utilisé pour le transfert sécurisé de données sur Internet. Le protocole prend en charge toutes les fonctionnalités de sécurité et d'authentification de SSH. Il est largement utilisé pour échanger des données, y compris des informations sensibles entre des partenaires commerciaux de divers secteurs tels que les services financiers, les soins de santé, le commerce de détail et la publicité.

Pour créer un SFTP serveur activé

1. Sélectionnez Serveurs dans le volet de navigation, puis choisissez Créer un serveur.
2. Dans Choisir les protocoles, sélectionnez SFTP, puis cliquez sur Suivant.
3. Dans Choose an identity provider, choisissez Service managed pour stocker les identités et les clés des utilisateurs dans Transfer Family, puis choisissez Next.
4. Dans Choisir un point de terminaison, procédez comme suit :
 - a. Pour le type de point de terminaison, choisissez le type de point de terminaison accessible au public.
 - b. Pour Nom d'hôte personnalisé, choisissez Aucun.
 - c. Choisissez Suivant.
5. Dans Choisissez un domaine, sélectionnez Amazon S3.
6. Dans Configurer les détails supplémentaires, procédez comme suit :
 - a. Pour la CloudWatch journalisation, choisissez Create a new role pour permettre à Transfer Family de créer automatiquement le IAM rôle, à condition que vous disposiez des autorisations nécessaires pour créer un nouveau rôle. Le IAM rôle créé est appelé `AWSTransferLoggingAccess`.
 - b. Pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur. La politique de sécurité par défaut est `TransferSecurityPolicy-2020-06`.
 - c. Choisissez Suivant.
7. Dans Réviser et créer, choisissez Créer un serveur. Vous êtes redirigé vers la page Serveurs.

Quelques minutes peuvent s'écouler avant que le statut de votre nouveau serveur passe à En ligne. À ce stade, votre serveur peut effectuer des opérations sur les fichiers, mais vous devez d'abord créer un utilisateur.

Étape 3 : Ajouter un utilisateur géré par le service

Pour ajouter un utilisateur au SFTP serveur activé

1. Sur la page Serveurs, cochez la case du serveur auquel vous souhaitez ajouter un utilisateur.
2. Sélectionnez Ajouter un utilisateur.

3. Dans la section Configuration utilisateur, pour Nom d'utilisateur, entrez le nom d'utilisateur. Ce nom d'utilisateur doit comporter au minimum 3 et au maximum 100 caractères. Vous pouvez utiliser les caractères suivants dans le nom d'utilisateur : a—z, A-Z, 0—9, trait de soulignement « _ », tiret « - », point ' . ', et au panneau « @ ». Le nom d'utilisateur ne peut pas commencer par un tiret, un point ou un signe arobase.
4. Pour Access, choisissez le IAM rôle que vous avez créé précédemment et qui donne accès à votre compartiment Amazon S3.

Vous avez créé ce IAM rôle à l'aide de la procédure décrite dans [Création d'un IAM rôle et d'une politique](#). Ce IAM rôle inclut une IAM politique qui fournit l'accès à votre compartiment Amazon S3. Cela inclut également une relation de confiance avec le AWS Transfer Family service, définie dans une autre IAM politique.

 Note

Le IAM rôle de l'utilisateur géré par le service doit contenir les autorisations nécessaires pour accéder au compartiment souhaité. Les autorisations d'accès au compartiment souhaité sont couvertes par S3 FullAccess, qui accorde des autorisations de niveau administrateur aux ressources S3.

5. Pour Politique, choisissez Aucune.
6. Pour le répertoire personnel, choisissez le compartiment Amazon S3 dans lequel stocker les données à transférer AWS Transfer Family. Entrez le chemin d'accès au home répertoire dans lequel votre utilisateur atterrit lorsqu'il se connecte à l'aide de son client.

Si vous laissez ce paramètre vide, le root répertoire de votre compartiment Amazon S3 est utilisé. Dans ce cas, assurez-vous que votre IAM rôle donne accès à ce root répertoire.

 Note

Nous vous recommandons de choisir un chemin de répertoire contenant le nom d'utilisateur de l'utilisateur, afin d'utiliser efficacement une politique de session. La politique de session limite l'accès des utilisateurs dans le compartiment Amazon S3 au home répertoire de cet utilisateur.

7. Pour Restreint, cochez la case afin que vos utilisateurs ne puissent accéder à rien en dehors de ce dossier et ne puissent pas voir le nom du compartiment ou du dossier Amazon S3.

 Note

Lorsque vous attribuez un répertoire personnel à l'utilisateur et que vous le limitez à ce répertoire personnel, cela devrait être suffisant pour verrouiller l'accès de l'utilisateur au dossier désigné. Utilisez une politique de session lorsque vous devez appliquer des contrôles supplémentaires.

8. Pour clé SSH publique, entrez la partie SSH clé publique de la paire de SSH clés.

Votre clé est validée par le service avant que vous puissiez ajouter votre nouvel utilisateur.

 Important

Le format de la clé SSH publique est `ssh-rsa <string>`. Pour obtenir des instructions sur la façon de générer une paire de SSH clés, consultez [Génération de SSH clés pour les utilisateurs gérés par des services](#).

9. (Facultatif) Pour Clé et Valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
10. Choisissez Add (Ajouter) pour ajouter votre nouvel utilisateur au serveur que vous avez choisi.

Le nouvel utilisateur apparaît dans la section Utilisateurs de la page de détails du serveur.

Étape 4 : Transférer un fichier à l'aide d'un client

Vous transférez des fichiers via le AWS Transfer Family service en spécifiant l'opération de transfert dans un client. AWS Transfer Family prend en charge plusieurs clients. Pour plus d'informations, consultez [Transfert de fichiers via un point de terminaison serveur à l'aide d'un client](#).

Cette section contient les procédures d'utilisation de Cyberduck et OpenSSH.

Rubriques

- [Utilisez Cyberduck](#)
- [Utiliser Open SSH](#)

Utilisez Cyberduck

Pour transférer des fichiers à AWS Transfer Family l'aide de Cyberduck

1. Ouvrez le client [Cyberduck](#).
2. Choisissez Open Connection.
3. Dans la boîte de dialogue Ouvrir une connexion, choisissez SFTP(SSHFile Transfer Protocol).
4. Pour Serveur, entrez le point de terminaison de votre serveur. Le point de terminaison du serveur se trouve sur la page des détails du serveur, voir [Afficher SFTP FTPS et détails FTP du serveur](#).
5. Dans le champ Numéro de port, entrez **22** pour SFTP.
6. Dans Nom d'utilisateur, entrez le nom de l'utilisateur que vous avez créé dans [Gestion des utilisateurs pour les points de terminaison du serveur](#).
7. Pour Clé SSH privée, choisissez ou entrez la clé SSH privée.
8. Choisissez Se connecter.
9. Effectuez le transfert de vos fichiers.

Selon l'emplacement de vos fichiers, effectuez l'une des actions suivantes :

- Dans votre répertoire local (la source), choisissez les fichiers que vous souhaitez transférer, puis faites-les glisser dans le répertoire Amazon S3 (la cible).
- Dans le répertoire Amazon S3 (la source), choisissez les fichiers que vous souhaitez transférer, puis faites-les glisser dans votre répertoire local (la cible).

Utiliser Open SSH

Suivez les instructions ci-dessous pour transférer des fichiers depuis la ligne de commande à l'aide d'OpenSSH.

Note

Ce client fonctionne uniquement avec un SFTP serveur activé.

Pour transférer des fichiers à l' AWS Transfer Family aide de l'utilitaire de ligne de SSH commande Open

1. Sur Linux ou Macintosh, ouvrez un terminal de commande.

2. À l'invite, entrez la commande suivante : `% sftp -i transfer-key sftp_user@service_endpoint`

Dans la commande précédente, `sftp_user` il s'agit du nom d'utilisateur et `transfer-key` de la clé SSH privée. `service_endpoint` Voici le point de terminaison du serveur tel qu'indiqué dans la AWS Transfer Family console du serveur sélectionné.

Une invite `sftp` doit s'afficher.

3. (Facultatif) Pour afficher le répertoire personnel de l'utilisateur, entrez la commande suivante à l'`sftp` invite : `sftp> pwd`
4. Sur la ligne suivante, entrez le texte suivant : `sftp> cd /mybucket/home/sftp_user`

Dans cet exercice de démarrage, ce compartiment Amazon S3 est la cible du transfert de fichiers.

5. Sur la ligne suivante, entrez la commande suivante : `sftp> put filename.txt`

La `put` commande transfère le fichier dans le compartiment Amazon S3.

Un message comparable au suivant s'affiche à l'écran, ce qui indique que le transfert du fichier est en cours ou terminé.

```
Uploading filename.txt to /my-bucket/home/sftp_user/filename.txt
```

```
some-file.txt 100% 127 0.1KB/s 00:00
```

Configuration d'un flux de travail géré pour le déchiffrement d'un fichier

Ce didacticiel explique comment configurer un flux de travail géré contenant une étape de déchiffrement. Le didacticiel explique également comment télécharger un fichier chiffré dans un compartiment Amazon S3, puis afficher le fichier déchiffré dans ce même compartiment.

Note

Le blog sur le AWS stockage contient un article qui décrit comment crypter et déchiffrer des fichiers, crypter et [déchiffrer des fichiers avec et](#). PGP AWS Transfer Family

Rubriques

- [Étape 1 : Configuration d'un rôle d'exécution](#)
- [Étape 2 : créer un flux de travail géré](#)
- [Étape 3 : ajouter le flux de travail à un serveur et créer un utilisateur](#)
- [Étape 4 : Création d'une paire de PGP clés](#)
- [Étape 5 : Stockez la clé PGP privée dans AWS Secrets Manager](#)
- [Étape 6 : Chiffrer un fichier](#)
- [Étape 7 : Exécuter le flux de travail et afficher les résultats](#)

Étape 1 : Configuration d'un rôle d'exécution

Créez un rôle d'exécution AWS Identity and Access Management (IAM) que Transfer Family peut utiliser pour lancer un flux de travail. Le processus de création d'un rôle d'exécution est décrit dans [IAM politiques relatives aux flux de travail](#).

Note

Dans le cadre de la création d'un rôle d'exécution, veillez à établir une relation de confiance entre le rôle d'exécution et Transfer Family, comme décrit dans [Étape 1 : Établir une relation d'approbation](#).

La politique de rôle d'exécution suivante contient toutes les autorisations requises pour exécuter correctement le flux de travail que vous allez créer dans ce didacticiel. Pour utiliser cet exemple de politique, remplacez *user input placeholders* par vos propres informations. **DOC-EXAMPLE-BUCKET** Remplacez-le par le nom du compartiment Amazon S3 dans lequel vous téléchargerez vos fichiers chiffrés.

Note

Tous les flux de travail ne nécessitent pas toutes les autorisations répertoriées dans cet exemple. Vous pouvez limiter les autorisations en fonction des types d'étapes de votre flux de travail spécifique. Les autorisations nécessaires pour chaque type d'étape prédéfini sont décrites dans [Utiliser des étapes prédéfinies](#). Les autorisations nécessaires pour une étape personnalisée sont décrites dans [IAM autorisations pour une étape personnalisée](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkflowsS3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:ListBucket",
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"],
      "Condition": {
        "StringEquals": {
          "s3:RequestObjectTag/Archive": "yes"
        }
      }
    },
    {
      "Sid": "DecryptSecret",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
    }
  ]
}

```

Étape 2 : créer un flux de travail géré

Vous devez maintenant créer un flux de travail contenant une étape de déchiffrement.

Pour créer un flux de travail contenant une étape de déchiffrement

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Workflows, puis Create Workflow.
3. Entrez les informations suivantes :
 - Entrez une description, par exemple **Decrypt workflow example**.
 - Dans la section Étapes nominales, choisissez Ajouter une étape.
4. Pour Choisir le type d'étape, choisissez Déchiffrer le fichier, puis Suivant.
5. Dans la boîte de dialogue Configurer les paramètres, spécifiez les éléments suivants :
 - Entrez un nom d'étape descriptif, par exemple, **decrypt-step**. Les espaces ne sont pas autorisés dans les noms des étapes.
 - Pour la destination des fichiers déchiffrés, choisissez Amazon S3.
 - Pour le nom du compartiment de destination, choisissez le même compartiment Amazon S3 que celui que vous avez spécifié **DOC-EXAMPLE-BUCKET** dans la IAM politique que vous avez créée à l'étape 1.
 - Pour le préfixe de clé de destination, entrez le nom du préfixe (dossier) dans lequel vous souhaitez stocker vos fichiers déchiffrés dans votre compartiment de destination, par exemple, **decrypted-files/**

Note

Assurez-vous d'ajouter une barre oblique (/) à votre préfixe.

- Pour ce didacticiel, laissez la case Overwrite existing désactivée. Lorsque ce paramètre est désactivé, si vous essayez de déchiffrer un fichier portant le même nom qu'un fichier existant, le traitement du flux de travail s'arrête et le nouveau fichier n'est pas traité.

Choisissez Suivant pour passer à l'écran de révision.

6. Passez en revue les détails de l'étape. Si tout est correct, choisissez Create step.
7. Votre flux de travail ne nécessite qu'une seule étape de déchiffrement, il n'y a donc aucune étape supplémentaire à configurer. Choisissez Créer un flux de travail pour créer le nouveau flux de travail.

Notez l'ID de flux de travail de votre nouveau flux de travail. Vous aurez besoin de cet identifiant pour l'étape suivante. Ce didacticiel utilise *w-1234abcd5678efghi* comme exemple d'ID de flux de travail.

Étape 3 : ajouter le flux de travail à un serveur et créer un utilisateur

Maintenant que vous disposez d'un flux de travail comportant une étape de déchiffrement, vous devez l'associer à un serveur Transfer Family. Ce didacticiel explique comment associer le flux de travail à un serveur Transfer Family existant. Vous pouvez également créer un nouveau serveur à utiliser avec votre flux de travail.

Après avoir attaché le flux de travail à un serveur, vous devez créer un utilisateur qui peut accéder SFTP au serveur et déclencher l'exécution du flux de travail.

Pour configurer un serveur Transfer Family afin d'exécuter un flux de travail

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers, puis choisissez un serveur dans la liste. Assurez-vous que ce serveur prend en charge le SFTP protocole.
3. Sur la page de détails du serveur, faites défiler la page jusqu'à la section Détails supplémentaires, puis choisissez Modifier.
4. Sur la page Modifier les détails supplémentaires, dans la section Flux de travail gérés, choisissez votre flux de travail et choisissez le rôle d'exécution correspondant.
 - Pour Workflow pour les téléchargements complets de fichiers, choisissez le flux de travail que vous avez créé dans [Étape 2 : créer un flux de travail géré](#), par exemple, *w-1234abcd5678efghi*.
 - Pour le rôle d'exécution des flux de travail gérés, choisissez le IAM rôle que vous avez créé dans [Étape 1 : Configuration d'un rôle d'exécution](#).
5. Faites défiler la page vers le bas, puis choisissez Enregistrer pour enregistrer vos modifications.

Notez l'ID du serveur que vous utilisez. Le nom du AWS Secrets Manager secret que vous utilisez pour stocker vos PGP clés est en partie basé sur l'ID du serveur.

Pour ajouter un utilisateur capable de déclencher le flux de travail

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.

2. Dans le volet de navigation de gauche, choisissez Servers, puis choisissez le serveur que vous utilisez pour le flux de travail de déchiffrement.
3. Sur la page de détails du serveur, faites défiler la page jusqu'à la section Utilisateurs, puis choisissez Ajouter un utilisateur.
4. Pour votre nouvel utilisateur, entrez les informations suivantes :
 - Pour Username (Nom d'utilisateur), saisissez **decrypt-user**.
 - Pour Rôle, choisissez un rôle d'utilisateur qui peut accéder à votre serveur.
 - Pour le répertoire personnel, choisissez le compartiment Amazon S3 que vous avez utilisé précédemment, par exemple **DOC-EXAMPLE-BUCKET**.
 - Pour les clés SSH publiques, collez une clé publique correspondant à une clé privée que vous possédez. Pour plus de détails, consultez [Génération de SSH clés pour les utilisateurs gérés par des services](#).
5. Choisissez Ajouter pour enregistrer votre nouvel utilisateur.

Notez le nom de votre utilisateur Transfer Family pour ce serveur. Le secret est partiellement basé sur le nom de l'utilisateur. Pour des raisons de simplicité, ce didacticiel utilise un secret par défaut qui peut être utilisé par n'importe quel utilisateur du serveur.

Étape 4 : Création d'une paire de PGP clés

Utilisez l'un des [PGPclients pris en charge](#) pour générer une paire de PGP clés. Ce processus est décrit en détail dans [Générer des PGP clés](#).

Pour générer une paire de PGP clés

1. Pour ce didacticiel, vous pouvez utiliser le client gpg (GnuPG) version 2.0.22 pour générer une paire de PGP clés qui sera utilisée RSA comme algorithme de chiffrement. Pour ce client, exécutez la commande suivante et fournissez une adresse e-mail et un mot de passe. Vous pouvez utiliser le nom ou l'adresse e-mail de votre choix. Assurez-vous de vous souvenir des valeurs que vous utilisez, car vous devrez les saisir ultérieurement dans le didacticiel.

```
gpg --gen-key
```

Note

Si vous utilisez la GnuPG version 2.3.0 ou une version plus récente, vous devez exécuter `gpg --full-gen-key`. Lorsque vous êtes invité à saisir le type de clé à créer, choisissez RSA ou ECC. Toutefois, si vous le souhaitez ECC, assurez-vous de choisir l'un des deux NIST or BrainPool pour la courbe elliptique. Ne choisissez pas Curve 25519.

2. Exportez la clé privée en exécutant la commande suivante. Remplacez `user@example.com` par l'adresse e-mail que vous avez utilisée lors de la génération de la clé.

```
gpg --output workflow-tutorial-key.pgp --armor --export-secret-key user@example.com
```

Cette commande exporte la clé privée vers le **workflow-tutorial-key.pgp** fichier. Vous pouvez nommer le fichier de sortie comme bon vous semble. Vous pouvez également supprimer le fichier de clé privée une fois que vous l'avez ajouté AWS Secrets Manager.

Étape 5 : Stockez la clé PGP privée dans AWS Secrets Manager

Vous devez stocker la clé privée dans Secrets Manager, de manière très spécifique, afin que le flux de travail puisse trouver la clé privée lorsque le flux de travail exécute une étape de déchiffrement sur un fichier téléchargé.

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](#).

Pour stocker une clé PGP privée dans Secrets Manager

1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Dans le volet de navigation de gauche, choisissez Secrets.
3. Sur la page Secrets, choisissez Enregistrer un nouveau secret.
4. Sur la page Choisir un type de secret, pour Type de secret, choisissez Autre type de secret.

5. Dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.
 - Clé — Entrée **PGPPrivateKey**.
 - valeur — Collez le texte de votre clé privée dans le champ de valeur.
 6. Choisissez Ajouter une ligne, puis dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.
 - Clé — Entrée **PGPPassphrase**.
 - valeur — Entrez le mot de passe que vous avez utilisé lorsque vous avez généré votre paire de PGP clés. [Étape 4 : Création d'une paire de PGP clés](#)
 7. Choisissez Suivant.
 8. Sur la page Configurer le secret, entrez le nom et la description de votre secret. Pour ce didacticiel, vous pouvez créer un secret par défaut que tous les utilisateurs peuvent utiliser. En supposant que l'ID du serveur est **s-11112222333344445**, nommez le secret **aws/transfer/s-11112222333344445/pggp-default**. **s-11112222333344445** Remplacez-le par l'ID de votre serveur Transfer Family. Entrez une description de votre secret.
- 
- Note**
- Pour créer un secret uniquement pour l'utilisateur que vous avez créé précédemment, nommez-le **aws/transfer/s-11112222333344445/decrypt-user**.
9. Choisissez Next, puis acceptez les valeurs par défaut sur la page Configurer la rotation. Ensuite, sélectionnez Suivant.
 10. Sur la page Révision, choisissez Store pour créer et stocker le secret.

Pour plus d'informations sur l'ajout de votre clé PGP privée à Secrets Manager, consultez la section [Utiliser AWS Secrets Manager pour stocker votre PGP clé](#).

Étape 6 : Chiffrer un fichier

Utilisez le gpg programme pour chiffrer un fichier à utiliser dans votre flux de travail. Exécutez la commande suivante pour chiffrer un fichier :

```
gpg -e -r marymajor@example.com --openpgp testfile.txt
```

Avant d'exécuter cette commande, notez ce qui suit :

- Pour l'-rargument, remplacez-le *marymajor@example.com* par l'adresse e-mail que vous avez utilisée lors de la création de la paire de PGP clés.
- Le --openpgp drapeau est facultatif. Cet indicateur rend le fichier crypté conforme à la norme [Open PGP RFC488 0](#).
- Cette commande crée un fichier nommé **testfile.txt.gpg** au même emplacement que **testfile.txt**.

Étape 7 : Exécuter le flux de travail et afficher les résultats

Pour exécuter le flux de travail, vous devez vous connecter au serveur Transfer Family avec l'utilisateur que vous avez créé à l'étape 3. Vous pouvez ensuite consulter le compartiment Amazon S3 que vous avez spécifié à l'[étape 2.5, configurer les paramètres de destination](#) pour voir le fichier déchiffré.

Pour exécuter le flux de travail de déchiffrement

1. Ouvrez un terminal de commande.
2. Exécutez la commande suivante, en la *your-endpoint* remplaçant par votre point de terminaison actuel et *transfer-key* par la clé SSH privée de votre utilisateur :

```
sftp -i transfer-key decrypt-user@your-endpoint
```

Par exemple, si la clé privée est stockée dans `~/.ssh/decrypt-user`, et que votre point de terminaison l'est `s-11112222333344445.server.transfer.us-east-2.amazonaws.com`, la commande est la suivante :

```
sftp -i ~/.ssh/decrypt-user decrypt-user@s-11112222333344445.server.transfer.us-east-2.amazonaws.com
```

3. Exécutez la commande `pwd`. En cas de succès, cette commande renverra ce qui suit :

```
Remote working directory: /DOC-EXAMPLE-BUCKET/decrypt-user
```

Votre répertoire reflète le nom de votre compartiment Amazon S3.

4. Exécutez la commande suivante pour télécharger le fichier et déclencher l'exécution du flux de travail :

```
put testfile.txt.gpg
```

5. Pour la destination des fichiers déchiffrés, vous avez indiqué le `decrypted-files/` dossier lors de la création du flux de travail. Vous pouvez maintenant accéder à ce dossier et en répertorier le contenu.

```
cd ../decrypted-files/  
ls
```

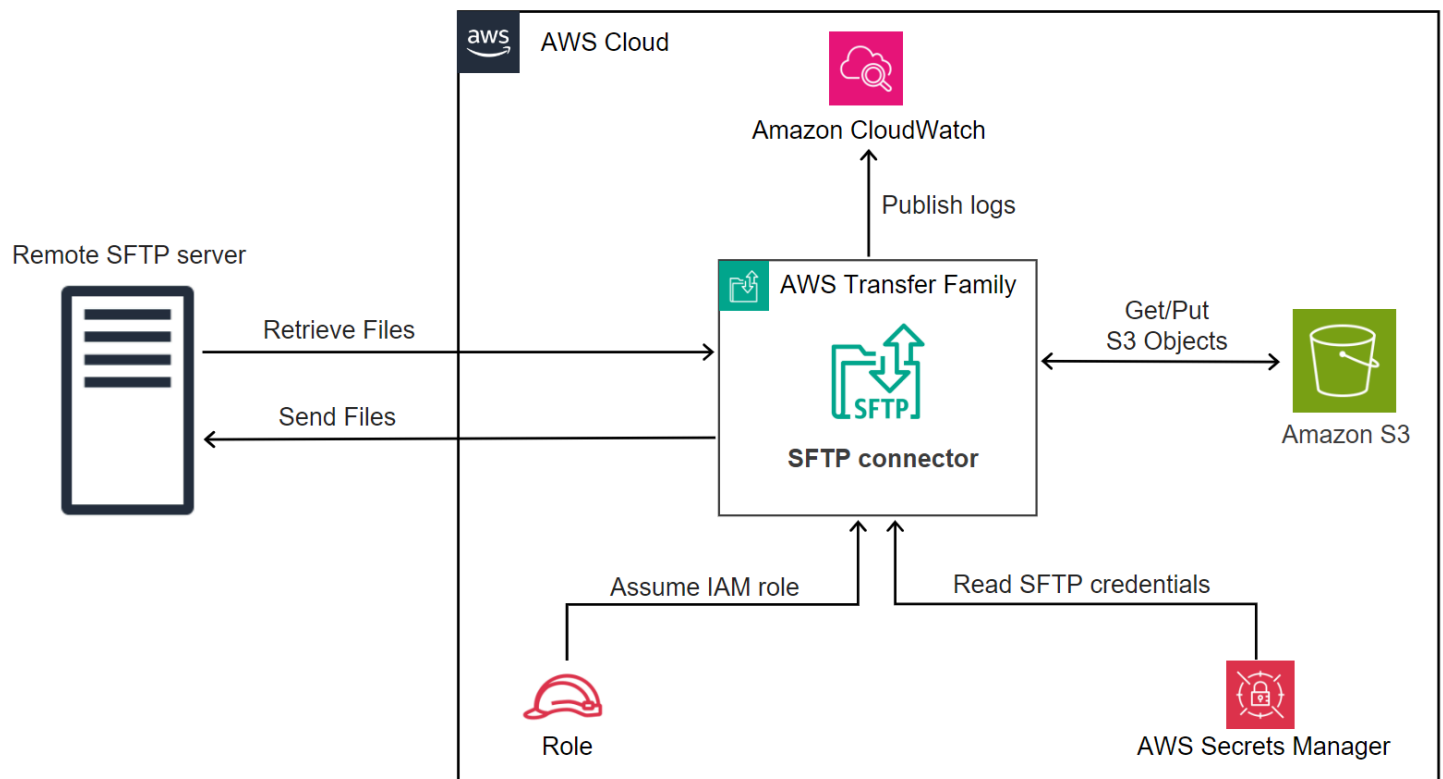
En cas de succès, la `ls` commande répertorie le `testfile.txt` fichier. Vous pouvez télécharger ce fichier et vérifier qu'il est identique au fichier d'origine que vous avez chiffré précédemment.

Configuration et utilisation des SFTP connecteurs

L'objectif d'un connecteur est d'établir une relation entre votre système AWS de stockage et le SFTP serveur d'un partenaire. Vous pouvez envoyer des fichiers depuis Amazon S3 vers une destination externe appartenant à un partenaire. Vous pouvez également utiliser un SFTP connecteur pour récupérer des fichiers depuis le SFTP serveur d'un partenaire.

Ce didacticiel explique comment configurer un SFTP connecteur, puis transférer des fichiers entre le stockage Amazon S3 et un SFTP serveur.

Un SFTP connecteur récupère les SFTP informations d'identification AWS Secrets Manager pour s'authentifier auprès d'un SFTP serveur distant et établir une connexion. Le connecteur envoie des fichiers au serveur distant ou en extrait des fichiers, puis les stocke dans Amazon S3. Un IAM rôle est utilisé pour autoriser l'accès au compartiment Amazon S3 et aux informations d'identification stockées dans Secrets Manager. Et vous pouvez vous connecter à Amazon CloudWatch.



Rubriques

- [Étape 1 : créer les ressources de soutien nécessaires](#)
- [Étape 2 : Création et test d'un SFTP connecteur](#)
- [Étape 3 : envoyer et récupérer des fichiers à l'aide du SFTP connecteur](#)
- [Procédures de création d'un serveur Transfer Family à utiliser comme SFTP serveur distant](#)

Étape 1 : créer les ressources de soutien nécessaires

Vous pouvez utiliser des SFTP connecteurs pour copier des fichiers entre Amazon S3 et n'importe quel SFTP serveur distant. Pour ce didacticiel, nous utilisons un AWS Transfer Family serveur comme SFTP serveur distant. Nous devons créer et configurer les ressources suivantes :

- Créez des compartiments Amazon S3 pour stocker des fichiers dans votre AWS environnement, et pour envoyer et récupérer des fichiers depuis le SFTP serveur distant : [Création de compartiments Amazon S3](#).
- Créez un AWS Identity and Access Management rôle pour accéder au stockage Amazon S3 et à notre secret dans Secrets Manager : [Créez un IAM rôle avec les autorisations nécessaires](#).

- Créez un serveur Transfer Family qui utilise le SFTP protocole et un utilisateur géré par le service qui utilise le SFTP connecteur pour transférer des fichiers vers ou depuis le SFTP serveur :.

[Création d'un SFTP serveur Transfer Family et d'un utilisateur](#)

- Créez un AWS Secrets Manager secret qui stocke les informations d'identification utilisées par le SFTP connecteur pour se connecter au SFTP serveur distant : [Créez et stockez un secret dans AWS Secrets Manager](#).

Création de compartiments Amazon S3

Pour créer un compartiment Amazon S3

1. Connectez-vous à la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez une région et entrez un nom.

Pour ce didacticiel, notre bucket est dedans **US East (N. Virginia) us-east-1**, et son nom l'est **sftp-server-storage-east**.

3. Acceptez les valeurs par défaut et choisissez Create bucket.

Pour en savoir plus sur la création de compartiments Amazon S3, consultez [Comment créer un compartiment S3](#) ? dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Créez un IAM rôle avec les autorisations nécessaires

Pour le rôle d'accès, créez une politique avec les autorisations suivantes.

L'exemple suivant accorde les autorisations nécessaires pour accéder au **DOC-EXAMPLE-BUCKET** dans Amazon S3, et le secret spécifié est stocké dans Secrets Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
    }
  ],
}
```



```

    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    ],
  },
  {
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
  },
  {
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

Remplacez les éléments comme suit :

- Dans *DOC-EXAMPLE-BUCKET*, le didacticiel utilise **s3-storage-east**.
- Dans *region*, le didacticiel utilise **us-east-1**.
- Dans *account-id*, utilisez votre Compte AWS identifiant.
- Dans *SecretName-6RandomCharacters*, nous sommes **using sftp-connector1** là pour le nom (vous aurez vos propres six caractères aléatoires pour votre secret).

Vous devez également vous assurer que ce rôle contient une relation de confiance qui permet au connecteur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos

utilisateurs. Pour plus de détails sur l'établissement d'une relation de confiance, voir [Étape 1 : Établir une relation d'approbation](#).

 Note

Pour en savoir plus sur le rôle que nous utilisons dans le didacticiel, consultez [Utilisateur et rôle d'accès combinés](#).

Créez et stockez un secret dans AWS Secrets Manager

Nous devons enregistrer un secret dans Secrets Manager afin de stocker les informations d'identification utilisateur de votre SFTP connecteur. Vous pouvez utiliser un mot de passe, une clé SSH privée ou les deux. Pour le didacticiel, nous utilisons une clé privée.

 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](#).

Avant de commencer la procédure de stockage du secret, récupérez et formatez votre clé privée. La clé privée doit correspondre à la clé publique configurée pour l'utilisateur sur le SFTP serveur distant. Pour notre tutoriel, la clé privée doit correspondre à la clé publique qui est stockée pour notre utilisateur de test sur le SFTP serveur Transfer Family que nous utilisons comme serveur distant.

Pour ce faire, exécutez la commande suivante :

```
jq -sR . path-to-private-key-file
```

Par exemple, si votre fichier de clé privée se trouve dans `~/ .ssh/sftp-testuser-privatekey`, la commande est la suivante.

```
jq -sR . ~/ .ssh/sftp-testuser-privatekey
```

Cela affiche la clé dans le format correct (avec des caractères de nouvelle ligne intégrés) sur la sortie standard. Copiez ce texte quelque part, car vous devez le coller dans la procédure suivante (étape 6).

Pour stocker les informations d'identification utilisateur dans le Gestionnaire des Secrets Manager d'un SFTP connecteur

1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Dans le volet de navigation de gauche, choisissez Secrets.
3. Sur la page Secrets, choisissez Enregistrer un nouveau secret.
4. Sur la page Choisir un type de secret, pour Type de secret, choisissez Autre type de secret.
5. Dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.
 - Clé — Entrez **Username**.
 - valeur — Entrez le nom de notre utilisateur, **sftp-testuser**.
6. Pour saisir la clé, nous vous recommandons d'utiliser l'onglet Texte en clair.
 - a. Choisissez Ajouter une ligne, puis entrez **PrivateKey**.
 - b. Choisissez l'onglet Plaintext. Le champ contient désormais le texte suivant :

```
{"Username":"sftp-testuser","PrivateKey":""}
```

- c. Collez le texte de votre clé privée (enregistré précédemment) entre guillemets vides (« »).

Votre écran doit se présenter comme suit (les données clés sont grisées).



7. Choisissez Suivant.
8. Sur la page Configurer le secret, entrez le nom de votre secret. Pour ce didacticiel, nous nommons le secret **aws/transfer/sftp-connector1**.
9. Choisissez Next, puis acceptez les valeurs par défaut sur la page Configurer la rotation. Ensuite, sélectionnez Suivant.
10. Sur la page Révision, choisissez Store pour créer et stocker le secret.

Étape 2 : Création et test d'un SFTP connecteur

Dans cette section, nous créons un SFTP connecteur qui utilise toutes les ressources que nous avons créées précédemment. Pour en savoir plus, consultez [Configuration des SFTP connecteurs](#).

Pour créer un SFTP connecteur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Connectors, puis Create connector.
3. Choisissez SFTPLe type de connecteur pour créer un SFTP connecteur, puis choisissez Next.

Transfer Family > Connectors > Create connector

Create connector [Info](#)

Create a connector that will be used to connect to your trading partner's server

Choose the connector type

Choose the protocol of the remote server to create a connector

☒ **SFTP**
Create a connector to connect to remote SFTP server

☐ **AS2**
Create a connector to connect to your trading partner's AS2 server

Cancel **Next**

4. Dans la section Configuration du connecteur, fournissez les informations suivantes :
 - Pour le URL, entrez le URL du SFTP serveur distant. Pour le didacticiel, nous saisissons le serveur Transfer Family que nous utilisons comme SFTP serveur distant. URL

```
sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
```

Remplacez **1111aaaa2222bbbb3** avec votre identifiant de serveur Transfer Family.

- Pour le rôle Access, entrez le rôle que nous avons créé précédemment, **sftp-connector-role**.
- Pour le rôle Logging, choisissez **AWSTransferLoggingAccess**.

 Note

AWSTransferLoggingAccess est une politique AWS gérée. Cette politique est décrite en détail dans [AWS politique gérée : AWSTransferLoggingAccess](#).

Connector configuration

URL

Specify the URL of remote server

sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com

Access role

IAM Role for Amazon S3 access and AWS Secrets Manager access

sftp-connector-role

Logging role - optional [Info](#)

IAM role for the connector to push events to your CloudWatch logs

AWSTransferLoggingAccess

5. Dans la section SFTPConfiguration, fournissez les informations suivantes :

- Pour les informations d'identification du Connector, choisissez le nom de votre ressource Secrets Manager qui contient les SFTP informations d'identification. Pour le didacticiel, choisissez **aws/transfer/sftp-connector1**.
- Pour les clés d'hôte fiables, collez la partie publique de la clé d'hôte. Vous pouvez récupérer cette clé en exécutant la `ssh-keyscan` commande pour votre SFTP serveur. Pour plus de détails sur le formatage et le stockage de la clé d'hôte approuvée, consultez le [SftpConnectorConfig](#) documentation sur les types de données.

SFTP configuration [Info](#)

Connector credentials
Select the username and password / SSH private key that will be used to connect to the remote server from AWS Secret Manager

aws/transfer/sftp-connector1

Trusted host keys
Connector connects to the remote server only if the SSH public key matches one of the below

ssh-rsa AAA...

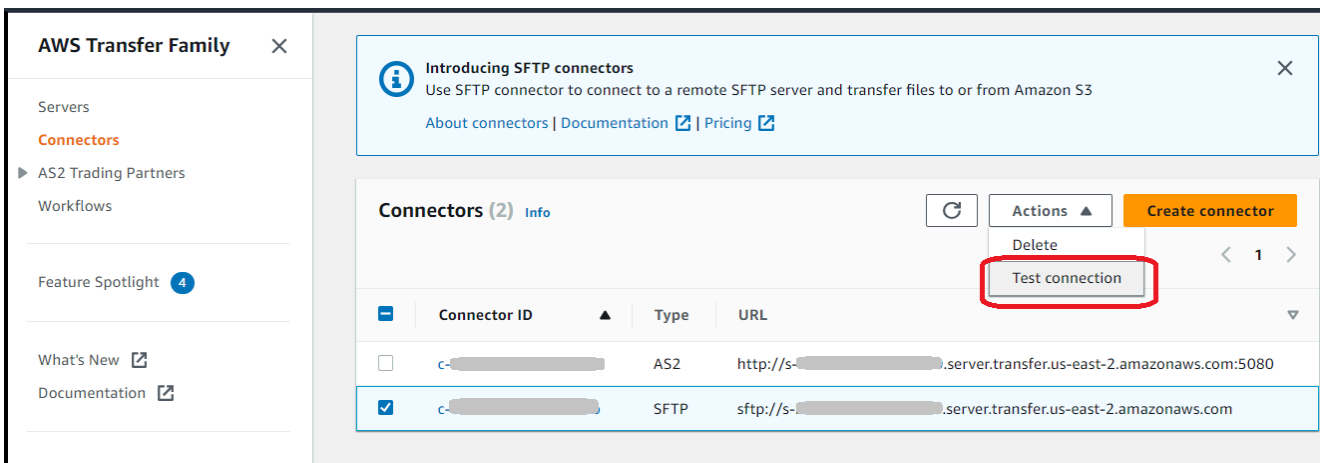
6. Après avoir confirmé tous vos paramètres, choisissez **Create connector** pour créer le SFTP connecteur.

Après avoir créé un SFTP connecteur, nous vous recommandons de le tester avant de tenter de transférer des fichiers à l'aide de votre nouveau connecteur.

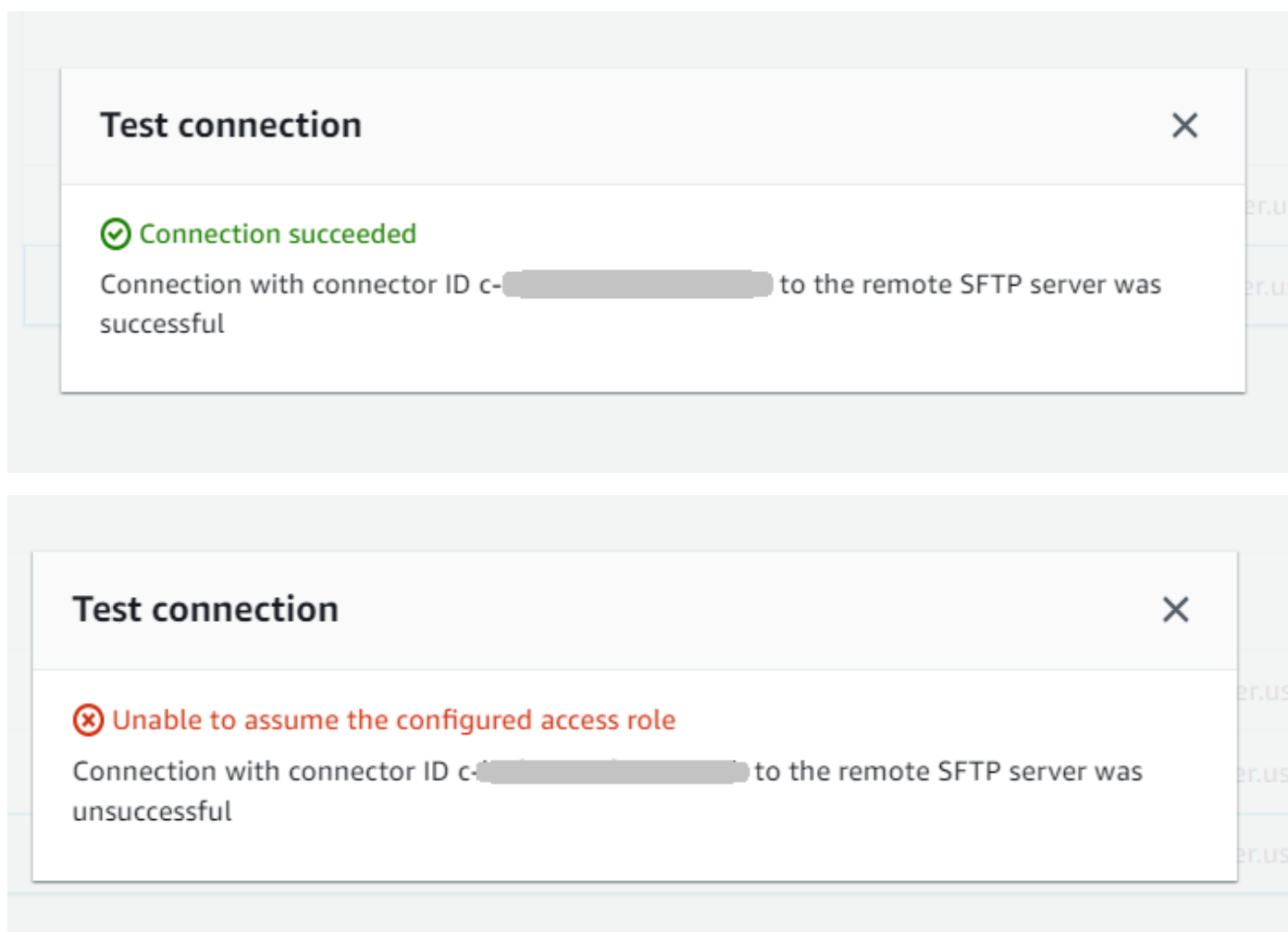
Test a connector using the console

Pour tester un SFTP connecteur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez **Connectors**, puis sélectionnez un connecteur.
3. Dans le menu **Actions**, choisissez **Tester la connexion**.



Le système renvoie un message indiquant si le test est réussi ou non. Si le test échoue, le système affiche un message d'erreur basé sur la raison de l'échec du test.



Test a connector using the CLI

Pour tester un connecteur à l'aide du AWS Command Line Interface, exécutez la commande suivante à l'invite de commande (remplacez *connector-id* (avec votre identifiant de connecteur actuel) :

```
aws transfer test-connection --connector-id c-connector-id
```

Si le test est réussi, les lignes suivantes sont renvoyées :

```
{
  "Status": "OK",
  "StatusMessage": "Connection succeeded"
}
```

Si le test échoue, vous recevez un message d'erreur descriptif, par exemple :

```
{
  "Status": "ERROR",
  "StatusMessage": "Unable to assume the configured access role"
}
```

Étape 3 : envoyer et récupérer des fichiers à l'aide du SFTP connecteur

Pour des raisons de simplicité, nous partons du principe que vous avez déjà des fichiers dans votre compartiment Amazon S3.

Note

Le didacticiel utilise des compartiments Amazon S3 pour les emplacements de stockage source et de destination. Si votre SFTP serveur n'utilise pas le stockage Amazon S3, `sftp-server-storage-east` dans les commandes suivantes, vous pouvez remplacer le chemin par un chemin vers les emplacements de fichiers accessibles depuis votre SFTP serveur.

- Nous envoyons un fichier nommé `SEND-to-SERVER.txt` depuis le stockage Amazon S3 au SFTP serveur.

- Nous récupérons un fichier nommé `RETRIEVE-to-S3.txt` depuis le SFTP serveur vers le stockage Amazon S3.

Note

Dans les commandes suivantes, remplacez *connector-id* avec votre identifiant de connecteur.

Tout d'abord, nous envoyons un fichier depuis notre compartiment Amazon S3 vers le SFTP serveur distant. À partir d'une invite de commande, exécutez la commande suivante :

```
aws transfer start-file-transfer --connector-id c-connector-id --send-file-paths "/s3-storage-east/SEND-to-SERVER.txt" /  
--remote-directory-path "/sftp-server-storage-east/incoming"
```

Votre `sftp-server-storage-east` seau devrait maintenant ressembler à ceci.

The screenshot shows the Amazon S3 console interface. The breadcrumb navigation at the top reads: [Amazon S3](#) > [Buckets](#) > [sftp-server-storage-east](#) > [incoming/](#). The main heading is 'incoming/' with a 'Copy S3 URI' button. Below this, there are tabs for 'Objects' (selected) and 'Properties'. The 'Objects' section shows 'Objects (1) Info' with a description and a 'Learn more' link. Below the description are buttons for 'Refresh', 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', and 'Create folder'. There is also an 'Upload' button. A search bar labeled 'Find objects by prefix' is present. At the bottom, a table lists the objects:

☐	Name	Type	Last modified	Size	Storage class
☐	SEND-to-SERVER.txt	txt	December 18, 2023, 10:36:40 (UTC-05:00)	4.1 KB	Standard

Si le fichier ne s'affiche pas comme prévu, consultez vos CloudWatch journaux.

Pour consulter vos CloudWatch journaux

1. Ouvrez la CloudWatch console Amazon à l'adresse <https://console.aws.amazon.com/cloudwatch/>
2. Sélectionnez Groupes de journaux dans le menu de navigation de gauche.
3. Entrez votre identifiant de connecteur dans la barre de recherche pour trouver vos journaux.
4. Sélectionnez le flux de journal renvoyé par la recherche.
5. Développez l'entrée de journal la plus récente.

En cas de succès, l'entrée dans le journal ressemble à ce qui suit :

```
{
  "operation": "SEND",
  "timestamp": "2023-12-18T15:26:57.346283Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/s3-storage-east/SEND-to-SERVER.txt",
  "status-code": "COMPLETED",
  "start-time": "2023-12-18T15:26:56.915864Z",
  "end-time": "2023-12-18T15:26:57.298122Z",
  "account-id": "500655546075",
  "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/connector-id",
  "remote-directory-path": "/sftp-server-storage-east/incoming"
}
```

Si le transfert de fichier a échoué, l'entrée du journal contient un message d'erreur qui précise le problème. Les causes courantes d'erreurs sont les problèmes d'IAM autorisations et les chemins de fichiers incorrects.

Ensuite, nous récupérons un fichier du SFTP serveur dans un compartiment Amazon S3. À partir d'une invite de commande, exécutez la commande suivante :

```
aws transfer start-file-transfer --connector-id c-connector-id --retrieve-file-paths "/sftp-server-storage-east/RETRIEVE-to-S3.txt" --local-directory-path "/s3-storage-east/incoming"
```

Si le transfert réussit, votre compartiment Amazon S3 contient le fichier transféré, comme indiqué ici.

Amazon S3 > Buckets > s3-storage-east > incoming/

incoming/

 Copy S3 URI

Objects | Properties

Objects (1) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)


 Copy S3 URI
  Copy URL
  Download
  Open
 Delete
 Actions ▼
 Create folder

 Upload

Find objects by prefix

☐	Name	Type	Last modified	Size	Storage class
☐	 RETRIEVE-to-S3.txt	txt	December 18, 2023, 10:26:58 (UTC-05:00)	4.1 KB	Standard

En cas de succès, l'entrée dans le journal ressemble à ce qui suit :

```
{
  "operation": "RETRIEVE",
  "timestamp": "2023-12-18T15:36:40.017800Z",
  "connector-id": "c-connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://s-server-id.server.transfer.us-east-1.amazonaws.com",
  "file-path": "/sftp-server-storage-east/RETRIEVE-to-S3.txt",
  "status-code": "COMPLETED",
  "start-time": "2023-12-18T15:36:39.727626Z",
  "end-time": "2023-12-18T15:36:39.895726Z",
  "account-id": "500655546075",
  "connector-arn": "arn:aws:transfer:us-east-1:500655546075:connector/c-connector-id",
  "local-directory-path": "/s3-storage-east/incoming"
}
```

Procédures de création d'un serveur Transfer Family à utiliser comme SFTP serveur distant

Nous décrivons ci-dessous les étapes à suivre pour créer un serveur Transfer Family qui vous servira de SFTP serveur distant pour ce didacticiel. Notez ce qui suit :

- Nous utilisons un serveur Transfer Family pour représenter un SFTP serveur distant. Les utilisateurs habituels SFTP du connecteur disposent de leur propre SFTP serveur distant. Consultez [Création d'un SFTP serveur Transfer Family et d'un utilisateur](#).
- Comme nous utilisons un serveur Transfer Family, nous utilisons également un utilisateur géré par le serviceSFTP. Et, par souci de simplicité, nous avons combiné les autorisations dont cet utilisateur a besoin pour accéder au serveur Transfer Family avec les autorisations dont il a besoin pour utiliser notre connecteur. Encore une fois, la plupart des cas d'utilisation du SFTP connecteur ont un SFTP utilisateur distinct qui n'est pas associé à un serveur Transfer Family. Consultez [Création d'un SFTP serveur Transfer Family et d'un utilisateur](#).
- Dans le cadre du didacticiel, étant donné que nous utilisons le stockage Amazon S3 pour notre SFTP serveur distant, nous devons créer un deuxième compartiment afin de pouvoir transférer des fichiers d'un compartiment à un autre. **s3-storage-east**

Création d'un SFTP serveur Transfer Family et d'un utilisateur

La plupart des utilisateurs n'auront pas besoin de créer un SFTP serveur Transfer Family ni un utilisateur, car vous avez déjà un SFTP serveur avec des utilisateurs, et vous pouvez utiliser ce serveur pour transférer des fichiers depuis et vers. Cependant, pour ce didacticiel, pour des raisons de simplicité, nous utilisons un serveur Transfer Family qui fonctionne en tant que SFTP serveur distant.

Suivez la procédure décrite dans [Création d'un SFTP serveur activé](#) pour créer un serveur et [Étape 3 : Ajouter un utilisateur géré par le service](#) ajouter un utilisateur. Voici les informations utilisateur que nous utilisons pour le didacticiel :

- Créez votre utilisateur géré par le service,. `sftp-testuser`
 - Définissez le répertoire de base sur `/sftp-server-storage-east/sftp-testuser`
 - Lorsque vous créez l'utilisateur, vous stockez une clé publique. Plus tard, lorsque vous créerez le secret dans Secrets Manager, vous devrez fournir la clé privée correspondante.

- Rôle `sftp-connector-role`. Pour le didacticiel, nous utilisons le même IAM rôle pour notre SFTP utilisateur et pour accéder au SFTP connecteur. Lorsque vous créez des connecteurs pour votre organisation, vous pouvez avoir des rôles d'utilisateur et d'accès distincts.
- Clé d'hôte du serveur : vous devez utiliser la clé d'hôte du serveur lorsque vous créez le connecteur. Vous pouvez récupérer cette clé en exécutant la `ssh-keyscan` commande pour votre serveur. Par exemple, si l'ID de votre serveur est présent `s-1111aaaa2222bbbb3` et que son point de terminaison se trouve `us-east-1`, la commande suivante permet de récupérer la clé d'hôte du serveur :

```
ssh-keyscan s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
```

Copiez ce texte quelque part, car vous devez le coller dans la [Étape 2 : Création et test d'un SFTP connecteur](#) procédure.

Utilisateur et rôle d'accès combinés

Pour le didacticiel, nous utilisons un seul rôle combiné. Nous utilisons ce rôle à la fois pour notre SFTP utilisateur et pour accéder au connecteur. L'exemple suivant contient les détails de ce rôle, au cas où vous souhaiteriez effectuer les tâches du didacticiel.

L'exemple suivant accorde les autorisations nécessaires pour accéder à nos deux compartiments dans Amazon S3 et au secret nommé `aws/transfer/sftp-connector1` stocké dans Secrets Manager. Pour le didacticiel, ce rôle est nommé `sftp-connector-role`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::sftp-server-storage-east",
        "arn:aws:s3:::s3-storage-east"
      ]
    }
  ],
}
```

```

{
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObjectVersion",
    "s3:GetObjectACL",
    "s3:PutObjectACL"
  ],
  "Resource": [
    "arn:aws:s3:::sftp-server-storage-east/*",
    "arn:aws:s3:::s3-storage-east/*"
  ]
},
{
  "Sid": "GetConnectorSecretValue",
  "Effect": "Allow",
  "Action": [
    "secretsmanager:GetSecretValue"
  ],
  "Resource": "arn:aws:secretsmanager:us-east-1:500655546075:secret:aws/transfer/sftp-connector1-6RandomCharacters"
}
]
}

```

Pour plus de détails sur la création de rôles pour Transfer Family, suivez la procédure décrite dans [Créer un rôle d'utilisateur](#) pour créer un rôle.

Configuration d'une méthode Amazon API Gateway en tant que fournisseur d'identité personnalisé

Ce didacticiel explique comment configurer une méthode Amazon API Gateway et comment l'utiliser en tant que fournisseur d'identité personnalisé pour télécharger des fichiers sur un AWS Transfer Family serveur. Ce didacticiel utilise le [modèle de pile de base](#) et d'autres fonctionnalités de base uniquement à titre d'exemple.

Rubriques

- [Prérequis](#)
- [Étape 1 : créer une CloudFormation pile](#)
- [Étape 2 : Vérifiez la configuration de la méthode API Gateway pour votre serveur](#)
- [Étape 3 : Afficher les détails du serveur Transfer Family](#)
- [Étape 4 : vérifiez que votre utilisateur peut se connecter au serveur](#)
- [Étape 5 : tester la SFTP connexion et le transfert de fichiers](#)
- [Étape 6 : Limiter l'accès au bucket](#)
- [Mettez à jour Lambda si vous utilisez Amazon EFS](#)

Prérequis

Avant de créer les ressources Transfer Family dans AWS CloudFormation, créez votre espace de stockage et votre rôle d'utilisateur.

Pour spécifier le stockage et créer un rôle d'utilisateur

1. En fonction du stockage que vous utilisez, consultez la documentation suivante :
 - Pour créer un compartiment Amazon S3, consultez [Comment créer un compartiment S3 ?](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.
 - Pour créer un système de EFS fichiers Amazon, consultez [Configuration d'un système de EFS fichiers Amazon](#).
2. Pour créer un rôle d'utilisateur, voir [Création d'un IAM rôle et d'une politique](#)

Vous entrez les détails de votre espace de stockage et de votre rôle d'utilisateur lorsque vous créez votre AWS CloudFormation stack dans la section suivante.

Étape 1 : créer une CloudFormation pile

Pour créer une AWS CloudFormation pile à partir du modèle fourni

1. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Sélectionnez Créer une pile, puis choisissez Avec de nouvelles ressources (standard).
3. Dans le volet Prérequis - Préparer le modèle, sélectionnez Le modèle est prêt.

4. Copiez ce lien, [modèle de pile de base](#), et collez-le dans le URL champ Amazon S3.
5. Cliquez sur Next (Suivant).
6. Spécifiez les paramètres, y compris le nom de votre pile. Veillez à effectuer les opérations suivantes :
 - Remplacez les valeurs par défaut pour UserName et UserPassword.
 - Pour UserHomeDirectory, entrez les détails du stockage (un compartiment Amazon S3 ou un système de EFS fichiers Amazon) que vous avez créé précédemment.
 - Remplacez le rôle UserRoleArn par défaut par le rôle utilisateur que vous avez créé précédemment. Le rôle AWS Identity and Access Management (IAM) doit disposer des autorisations appropriées. Pour un exemple de politique relative aux IAM rôles et aux compartiments, voir [Étape 6 : Limiter l'accès au bucket](#).
 - Si vous souhaitez vous authentifier à l'aide d'une clé publique plutôt que d'un mot de passe, entrez votre clé publique dans le champ UserPublicKey1. La première fois que vous vous connectez au serveur en utilisant SFTP, vous fournissez la clé privée au lieu d'un mot de passe.
7. Choisissez Next, puis de nouveau Next sur la page Configurer les options de pile.
8. Passez en revue les détails de la pile que vous créez, puis choisissez Create stack.

 Note

Au bas de la page, sous Capacités, vous devez reconnaître que cela AWS CloudFormation peut créer IAM des ressources.

Étape 2 : Vérifiez la configuration de la méthode API Gateway pour votre serveur

 Note

Pour améliorer la sécurité, vous pouvez configurer un pare-feu pour applications Web. AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les HTTPS demandes HTTP et les demandes qui sont transmises à Amazon API Gateway. Pour plus de détails, consultez [Ajouter un pare-feu pour applications Web](#).

Pour vérifier la configuration de la méthode API Gateway pour votre serveur et la déployer

1. Ouvrez la console API Gateway à l'adresse <https://console.aws.amazon.com/apigateway/>.
2. Choisissez le modèle API de base Transfer Custom Identity Provider généré par le AWS CloudFormation modèle.
3. Dans le volet Ressources, choisissez GET, puis Method Request.
4. Pour Actions, sélectionnez Déployer API. Pour l'étape de déploiement, choisissez prod, puis Deploy.

Une fois la méthode API Gateway déployée avec succès, consultez ses performances dans la section Stage Editor.

 Note

Copiez l'URL adresse Invoke qui apparaît en haut de la page. Vous en aurez besoin pour la prochaine étape.

Étape 3 : Afficher les détails du serveur Transfer Family

Lorsque vous utilisez le modèle pour créer une AWS CloudFormation pile, un serveur Transfer Family est automatiquement créé.

Pour consulter les détails de votre serveur Transfer Family

1. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Choisissez la pile que vous avez créée.
3. Sélectionnez l'onglet Ressources.

Resources (18)			
Search resources			
Logical ID	Physical ID	Type	
ApiCloudWatchLogsRole	-ApiCloudWatchLogsRole-	AWS::IAM::Role	
ApiDeployment202008		AWS::ApiGateway::Deployment	
ApiLoggingAccount		AWS::ApiGateway::Account	
ApiStage	prod	AWS::ApiGateway::Stage	
CloudWatchLoggingRole	-CloudWatchLoggingRole-	AWS::IAM::Role	
CustomIdentityProviderApi		AWS::ApiGateway::RestApi	
GetUserConfigLambda	-GetUserConfigLambda-	AWS::Lambda::Function	
GetUserConfigLambdaPermission	GetUserConfigLambdaPermission-	AWS::Lambda::Permission	
GetUserConfigRequest		AWS::ApiGateway::Method	
GetUserConfigResource		AWS::ApiGateway::Resource	
GetUserConfigResponseModel	UserConfigResponseModel	AWS::ApiGateway::Model	
LambdaExecutionRole	-LambdaExecutionRole-	AWS::IAM::Role	
ServerIdResource		AWS::ApiGateway::Resource	
ServersResource		AWS::ApiGateway::Resource	
TransferIdentityProviderRole	-TransferIdentityProviderRole-	AWS::IAM::Role	
TransferServer	arn:aws:transfer:us-east-2:::server/s-	AWS::Transfer::Server	
UserNameResource		AWS::ApiGateway::Resource	
UsersResource		AWS::ApiGateway::Resource	

Le serveur ARN est affiché dans la colonne Physical ID de la TransferServerligne. L'ID du serveur est contenu dans leARN, par exemple, s-11112222333344445.

- Ouvrez la AWS Transfer Family console à <https://console.aws.amazon.com/transfer/>, et sur la page Serveurs, choisissez le nouveau serveur.

L'ID du serveur correspond à l'ID affiché pour la TransferServerressource dans AWS CloudFormation.

Étape 4 : vérifiez que votre utilisateur peut se connecter au serveur

Pour vérifier que votre utilisateur peut se connecter au serveur, à l'aide de la console Transfer Family

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Sur la page Serveurs, choisissez votre nouveau serveur, sélectionnez Actions, puis sélectionnez Test.
3. Entrez le texte de vos informations de connexion dans le champ Nom d'utilisateur et dans le champ Mot de passe. Il s'agit des valeurs que vous avez définies lorsque vous avez déployé la AWS CloudFormation pile.
4. Pour le protocole serveur, sélectionnez SFTP, et pour l'adresse IP source, entrez **127.0.0.1**.
5. Sélectionnez Tester).

Si l'authentification de l'utilisateur réussit, le test renvoie une `StatusCode: 200 HTML` réponse et un JSON objet contenant les détails des rôles et des autorisations de l'utilisateur. Par exemple :

```
{
  "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/my-user-role\",
  \"HomeDirectory\": \"/${transfer:HomeBucket}/\",
  \"StatusCode\": 200,
  \"Message\": \"\",
  \"Url\": \"https://1a2b3c4d5e.execute-api.us-east-2.amazonaws.com/prod/servers/s-1234abcd5678efgh0/users/myuser/config\"
}
```

Si le test échoue, ajoutez l'une des politiques AWS gérées par API Gateway au rôle que vous utilisez pour votre API.

Étape 5 : tester la SFTP connexion et le transfert de fichiers

Pour tester la SFTP connexion

1. Sur un appareil Linux ou macOS, ouvrez un terminal de commande.
2. Entrez l'une des commandes suivantes, selon que vous utilisez un mot de passe ou une paire de clés pour l'authentification.
 - Si vous utilisez un mot de passe, entrez cette commande :

```
sftp -o PubkeyAuthentication=no myuser@server-ID.server.transfer.region-code.amazonaws.com
```

Lorsque vous y êtes invité, saisissez votre mot de passe.

- Si vous utilisez une paire de clés, entrez cette commande :

```
sftp -i private-key-file myuser@server-ID.server.transfer.region-code.amazonaws.com
```

Note

Pour ces sftp commandes, insérez le code indiquant Région AWS où se trouve votre serveur Transfer Family. Par exemple, si votre serveur se trouve dans l'est des États-Unis (Ohio), entrez **us-east-2**.

3. À l'`sftp>invite`, assurez-vous que vous pouvez charger (put), télécharger (get) et afficher les répertoires et les fichiers (`pwd` et `ls`).

Étape 6 : Limiter l'accès au bucket

Vous pouvez limiter les personnes autorisées à accéder à un compartiment Amazon S3 spécifique. L'exemple suivant montre les paramètres à utiliser dans votre CloudFormation pile et dans la politique que vous sélectionnez pour votre utilisateur.

Dans cet exemple, nous avons défini les paramètres suivants pour la AWS CloudFormation pile :

- `CreateServer`: `true`
- `UserHomeDirectory`: `/myuser-bucket`
- `UserName`: `myuser`
- `UserPassword`: `MySuperSecretPassword`

Important

Il s'agit d'un exemple de mot de passe. Lorsque vous configurez votre méthode API Gateway, assurez-vous de saisir un mot de passe fort.

- UserPublicKey1 : *your-public-key*
- UserRoleArn: arn:aws:iam::*role-id*:role/myuser-api-gateway-role

Le UserPublicKey1 est une clé publique que vous avez générée dans le cadre d'une paire de clés publique/privée.

Le *role-id* est propre au rôle d'utilisateur que vous créez. La politique qui y est rattachée myuser-api-gateway-role est la suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::myuser-bucket"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectAcl",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::myuser-bucket/*"
    }
  ]
}
```

Pour vous connecter au serveur en utilisant SFTP, entrez l'une des commandes suivantes à l'invite.

- Si vous utilisez un mot de passe pour vous authentifier, exécutez la commande suivante :

```
sftp -o PubkeyAuthentication=no myuser@transfer-server-  
ID.server.transfer.region-id.amazonaws.com
```

Lorsque vous y êtes invité, saisissez votre mot de passe.

- Si vous utilisez une paire de clés pour vous authentifier, exécutez la commande suivante :

```
sftp -i private-key-file myuser@transfer-server-ID.server.transfer.region-id.amazonaws.com
```

Note

Pour ces sftp commandes, utilisez l'ID correspondant à l' Région AWS emplacement de votre serveur Transfer Family. Par exemple, si votre serveur se trouve dans l'est des États-Unis (Ohio), utilisez `us-east-2`.

À l'invite `sftp`, vous êtes dirigé vers votre répertoire personnel, que vous pouvez consulter en exécutant la `pwd` commande. Par exemple :

```
sftp> pwd
Remote working directory: /myuser-bucket
```

L'utilisateur ne peut afficher aucun répertoire situé au-dessus du répertoire de base. Par exemple :

```
sftp> pwd
Remote working directory: /myuser-bucket
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

Mettez à jour Lambda si vous utilisez Amazon EFS

Si vous avez sélectionné Amazon EFS comme option de stockage pour votre serveur Transfer Family, vous devez modifier la fonction lambda de votre stack.

Pour ajouter un profil posix à votre fonction Lambda

1. Ouvrez la console Lambda à l'adresse. <https://console.aws.amazon.com/lambda/>
2. Sélectionnez la fonction Lambda que vous avez créée précédemment. La fonction Lambda a le format suivant ***stack-name***-GetUserConfigLambda-***lambda-identifiant***, où ***stack-name*** est le nom de la CloudFormation pile et ***lambda-identifiant*** est l'identifiant de la fonction.

3. Dans l'onglet Code, sélectionnez `index.js` pour afficher le code de la fonction.
4. Dans la réponse, ajoutez la ligne suivante entre `Policy` et `HomeDirectory` :

```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

Où le *uid-value* and *gid-value* sont des nombres entiers, supérieurs ou égaux à 0, qui représentent respectivement l'ID utilisateur et l'ID de groupe.

Par exemple, après avoir ajouté le profil Posix, le champ de réponse peut ressembler à ce qui suit :

```
response = {  
  Role: 'arn:aws:iam::123456789012:role/api-gateway-transfer-efs-role', // The  
  user will be authenticated if and only if the Role field is not blank  
  Policy: '', // Optional JSON blob to further restrict this user's permissions  
  PosixProfile: {"Gid": 65534, "Uid": 65534},  
  HomeDirectory: '/fs-fab2c234' // Not required, defaults to '/'  
};
```

Configuration d'une AS2 configuration

Ce didacticiel explique comment configurer une configuration Applicability Statement 2 (AS2) avec AWS Transfer Family. Après avoir effectué les étapes décrites ici, vous disposerez d'un AS2 serveur compatible prêt à accepter les AS2 messages d'un partenaire commercial type. Vous disposerez également d'un connecteur qui pourra être utilisé pour envoyer AS2 des messages au partenaire commercial témoin.

Note

Certaines parties de l'exemple de configuration utilisent le AWS Command Line Interface (AWS CLI). Si vous ne l'avez pas encore installé AWS CLI, consultez la section [Installation ou mise à jour de la AWS CLI dernière version du](#) Guide de l'AWS Command Line Interface utilisateur.

1. Créez des certificats pour vous-même et pour votre partenaire commercial. Si vous disposez de certificats existants que vous pouvez utiliser, vous pouvez ignorer cette section.

Ce processus est décrit dans [Étape 1 : créer des certificats pour AS2](#).

2. Créez un AWS Transfer Family serveur qui utilise le AS2 protocole. Vous pouvez éventuellement ajouter une adresse IP élastique au serveur pour le rendre accessible à Internet.

Ce processus est décrit dans [Étape 2 : Création d'un serveur Transfer Family utilisant le AS2 protocole](#).

 Note

Vous devez créer un serveur Transfer Family pour les transferts entrants uniquement. Si vous effectuez uniquement des transferts sortants, vous n'avez pas besoin d'un serveur Transfer Family.

3. Importez les certificats que vous avez créés à l'étape 1.

Ce processus est décrit dans [Étape 3 : Importer des certificats en tant que ressources de certificats Transfer Family](#).

4. Pour configurer vos partenaires commerciaux, créez un profil local et un profil de partenaire.

Ce processus est décrit dans [Étape 4 : Créez des profils pour vous et votre partenaire commercial](#).

5. Créez un accord entre vous et votre partenaire commercial.

Ce processus est décrit dans [Étape 5 : Créez un accord entre vous et votre partenaire](#).

 Note

Vous devez créer un accord pour les transferts entrants uniquement. Si vous effectuez uniquement des transferts sortants, vous n'avez pas besoin d'accord.

6. Créez un lien entre vous et votre partenaire commercial.

Ce processus est décrit dans [Étape 6 : Créez un lien entre vous et votre partenaire](#).

 Note

Vous devez créer un connecteur pour les transferts sortants uniquement. Si vous effectuez uniquement des transferts entrants, vous n'avez pas besoin de connecteur.

7. Testez un échange de AS2 fichiers.

Ce processus est décrit dans [Étape 7 : Testez l'échange de fichiers à AS2 l'aide de Transfer Family](#).

Après avoir effectué ces étapes, vous pouvez effectuer les opérations suivantes :

- Envoyez des fichiers vers un serveur partenaire AS2 compatible avec la télécommande à l'aide de la commande Transfer Family `start-file-transfer` AWS Command Line Interface (AWS CLI).
- Recevez des fichiers depuis un serveur partenaire AS2 compatible à distance sur le port 5080 via votre point de terminaison de cloud privé virtuel (VPC).

Étape 1 : créer des certificats pour AS2

Les deux parties à un AS2 échange ont besoin de certificats X.509. Vous pouvez créer ces certificats comme bon vous semble. Cette rubrique décrit comment utiliser [Open SSL](#) depuis la ligne de commande pour créer un certificat racine, puis signer des certificats subordonnés. Les deux parties doivent générer leurs propres certificats.

 Note

La longueur de la clé pour les AS2 certificats doit être d'au moins 2 048 bits et d'au plus 4 096 bits.

Pour transférer des fichiers avec un partenaire, prenez note des points suivants :

- Vous pouvez joindre des certificats aux profils. Les certificats contiennent des clés publiques ou privées.
- Votre partenaire commercial vous envoie ses clés publiques, et vous lui envoyez les vôtres.

- Votre partenaire commercial chiffre les messages avec votre clé publique et les signe avec sa clé privée. Inversement, vous cryptez les messages avec la clé publique de votre partenaire et vous les signez avec votre clé privée.

Note

Si vous préférez gérer les clés avec un GUI, [Portecle](#) est une option que vous pouvez utiliser.

Pour générer des exemples de certificats

Important

N'envoyez pas vos clés privées à votre partenaire. Dans cet exemple, vous générez un ensemble de clés publiques et privées auto-signées pour une partie. Si vous comptez agir en tant que deux partenaires commerciaux à des fins de test, vous pouvez répéter ces instructions pour générer deux jeux de clés : un pour chaque partenaire commercial. Dans ce cas, il n'est pas nécessaire de générer deux autorités de certification racine (CAs).

1. Exécutez la commande suivante pour générer une clé RSA privée avec un module de 2 048 bits.

```
/usr/bin/openssl genrsa -out root-ca-key.pem 2048
```

2. Exécutez la commande suivante pour créer un certificat auto-signé avec votre `root-ca-key.pem` fichier.

```
/usr/bin/openssl req \  
-x509 -new -nodes -sha256 \  
-days 1825 \  
-subj "/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=R00TCA" \  
-key root-ca-key.pem \  
-out root-ca.pem
```

L'-subj argument comprend les valeurs suivantes.

	Name (Nom)	Description
C	Code pays	Code à deux lettres pour le pays dans lequel se trouve votre organisation.
ST	État, région ou province	État, région ou province dans lequel se trouve votre organisation. (Dans ce cas, la région ne fait pas référence à votre Région AWS.)
L	Nom de la localité	Ville dans laquelle se trouve votre organisation.
O	Nom de l'organisation	Le nom légal complet de votre organisation, y compris les suffixes LLC, tels que Corp, etc.
OU	Nom de l'unité organisationnelle	Division de votre organisation qui s'occupe de ce certificat.
CN	Nom commun ou nom de domaine complet (FQDN)	Dans ce cas, nous créons un certificat racine, donc la valeur est ROOTCA. Dans ces exemples, nous utilisons CN pour décrire l'objectif du certificat.

3. Créez une clé de signature et une clé de chiffrement pour votre profil local.

```
/usr/bin/openssl genrsa -out signing-key.pem 2048
/usr/bin/openssl genrsa -out encryption-key.pem 2048
```

 Note

Certains serveurs AS2 compatibles, tels qu'OpenAS2, nécessitent que vous utilisiez le même certificat pour la signature et le chiffrement. Dans ce cas, vous pouvez importer la même clé privée et le même certificat dans les deux cas. Pour ce faire, exécutez cette commande au lieu des deux commandes précédentes :

```
/usr/bin/openssl genrsa -out signing-and-encryption-key.pem 2048
```

- Exécutez les commandes suivantes pour créer des demandes de signature de certificat (CSRs) pour la signature de la clé racine.

```
/usr/bin/openssl req -new -key signing-key.pem -subj \  
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Signer" -out signing-  
key-csr.pem
```

```
/usr/bin/openssl req -new -key encryption-key.pem -subj \  
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Encrypter" -out  
encryption-key-csr.pem
```

- Ensuite, vous devez créer un `signing-cert.conf` fichier et un `encryption-cert.conf` fichier.

- Utilisez un éditeur de texte pour créer le `signing-cert.conf` fichier avec le contenu suivant :

```
authorityKeyIdentifier=keyid,issuer  
keyUsage = digitalSignature, nonRepudiation
```

- Utilisez un éditeur de texte pour créer le `encryption-cert.conf` fichier avec le contenu suivant :

```
authorityKeyIdentifier=keyid,issuer  
keyUsage = dataEncipherment
```

- Enfin, vous créez les certificats signés en exécutant les commandes suivantes.

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in signing-key-csr.pem -out signing-cert.pem -CA \
root-ca.pem -CAkey root-ca-key.pem -extfile signing-cert.conf
```

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in encryption-key-csr.pem -out encryption-cert.pem \
-CA root-ca.pem -CAkey root-ca-key.pem -extfile encryption-cert.conf
```

Étape 2 : Création d'un serveur Transfer Family utilisant le AS2 protocole

Cette procédure explique comment créer un serveur AS2 compatible à l'aide du Transfer Family AWS CLI.

Note

De nombreux exemples d'étapes utilisent des commandes qui chargent des paramètres à partir d'un fichier. Pour plus de détails sur l'utilisation de fichiers pour charger des paramètres, consultez [Comment charger des paramètres à partir d'un fichier](#).

Si vous souhaitez plutôt utiliser la console, consultez [Création d'un AS2 serveur à l'aide de la console Transfer Family](#).

De la même manière que vous créez un FTPS AWS Transfer Family serveur SFTP OR, vous créez un AS2 serveur activé en utilisant le `--protocols AS2` paramètre de la `create-server` AWS CLI commande. Actuellement, Transfer Family ne prend en charge que les types de VPC terminaux et le stockage Amazon S3 avec le AS2 protocole.

Lorsque vous créez votre serveur AS2 compatible pour Transfer Family à l'aide de la `create-server` commande, un VPC point de terminaison est automatiquement créé pour vous. Ce point de terminaison expose TCP le port 5080 afin qu'il puisse accepter AS2 des messages.

Si vous souhaitez exposer votre VPC point de terminaison publiquement à Internet, vous pouvez associer des adresses IP élastiques à votre VPC point de terminaison.

Pour utiliser ces instructions, vous devez disposer des éléments suivants :

- L'identifiant de votre VPC (par exemple, `vpc-abcdef01`).

- Les IDs de vos VPC sous-réseaux (par exemple, subnet-abcdef01, 01, subnet-021345ab). subnet-subnet-abcdef
- Un ou plusieurs groupes IDs de sécurité qui autorisent le trafic entrant sur le TCP port 5080 en provenance de vos partenaires commerciaux (par exemple, sg-1234567890abcdef0 et sg-abcdef01234567890).
- (Facultatif) Les adresses IP élastiques que vous souhaitez associer à votre VPC point de terminaison.
- Si votre partenaire commercial n'est pas connecté à vous VPC via unVPN, vous avez besoin d'une passerelle Internet. Pour plus d'informations, consultez [la section Se connecter à Internet à l'aide d'une passerelle Internet](#) dans le guide de VPC l'utilisateur Amazon.

Pour créer un AS2 serveur activé

1. Exécutez la commande suivante. Remplacez chaque *user input placeholder* par vos propres informations.

```
aws transfer create-server --endpoint-type VPC \  
--endpoint-details VpcId=vpc-abcdef01,SubnetIds=subnet-abcdef01,subnet-  
abcdef01,subnet-  
021345ab,SecurityGroupIds=sg-abcdef01234567890,sg-1234567890abcdef0 --protocols AS2 \  
\   
--protocol-details As2Transports=HTTP
```

2. (Facultatif) Vous pouvez rendre le VPC point de terminaison public. Vous ne pouvez associer des adresses IP Elastic à un serveur Transfer Family que par le biais d'une update-server opération. Les commandes suivantes arrêtent le serveur, le mettent à jour avec des adresses IP élastiques, puis le redémarrent.

```
aws transfer stop-server --server-id your-server-id
```

```
aws transfer update-server --server-id your-server-id --endpoint-details \  
AddressAllocationIds=eipalloc-abcdef01234567890,eipalloc-  
1234567890abcdef0,eipalloc-abcd012345cccccc
```

```
aws transfer start-server --server-id your-server-id
```

Cette `start-server` commande crée automatiquement un DNS enregistrement contenant l'adresse IP publique de votre serveur. Pour permettre à votre partenaire commercial d'accéder au serveur, vous lui fournissez les informations suivantes. Dans ce cas, *your-region* fait référence à votre Région AWS.

`s-your-server-id.server.transfer.your-region.amazonaws.com`

Le montant complet URL que vous fournissez à votre partenaire commercial est le suivant :

`http://s-your-server-id.server.transfer.your-region.amazonaws.com:5080`

3. Pour vérifier si votre AS2 serveur activé est accessible, utilisez les commandes suivantes. Assurez-vous que votre serveur est accessible via l'adresse privée de votre VPC point de terminaison ou via votre point de terminaison public (si vous avez associé une adresse IP élastique à votre point de terminaison).

Si votre serveur est correctement configuré, la connexion sera établie. Cependant, vous recevrez une réponse avec HTTP le code d'état 400 (Mauvaise demande) car vous n'envoyez pas un AS2 message valide.

- Pour un point de terminaison public (si vous avez associé une adresse IP élastique à l'étape précédente), exécutez la commande suivante en remplaçant votre ID de serveur et votre région.

```
curl -vv -X POST http://s-your-server-id.transfer.your-region.amazonaws.com:5080
```

- Si vous vous connectez au sein de votre VPC, recherchez le DNS nom privé de votre VPC point de terminaison en exécutant les commandes suivantes.

```
aws transfer describe-server --server-id s-your-server-id
```

Cette `describe-server` commande renvoie votre identifiant de point de VPC terminaison dans le `VpcEndpointId` paramètre. Utilisez cette valeur pour exécuter la commande suivante.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-your-vpc-endpoint-id
```

Cette `describe-vpc-endpoints` commande renvoie un `DNSEntries` tableau contenant plusieurs `DnsName` paramètres. Utilisez le DNS nom régional (celui qui n'inclut pas la zone de disponibilité) dans la commande suivante.

```
curl -vv -X POST http://vpce-your-vpce.vpce-svc-your-vpce-svc.your-region.vpce.amazonaws.com:5080
```

Par exemple, la commande suivante montre des exemples de valeurs pour les espaces réservés de la commande précédente.

```
curl -vv -X POST http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

4. (Facultatif) Configurez un rôle de journalisation. Transfer Family enregistre le statut des messages envoyés et reçus dans un JSON format structuré dans Amazon CloudWatch Logs. Pour permettre à Transfer Family d'accéder aux CloudWatch journaux de votre compte, vous devez configurer un rôle de journalisation sur votre serveur.

Créez un rôle AWS Identity and Access Management (IAM) qui fait confiance `transfer.amazonaws.com` à la politique `AWSTransferLoggingAccess` gérée et associez-y. Pour plus de détails, consultez [Création d'un IAM rôle et d'une politique](#). Notez le nom de ressource Amazon (ARN) du IAM rôle que vous venez de créer et associez-le au serveur en exécutant la `update-server` commande suivante :

```
aws transfer update-server --server-id your-server-id --logging-role  
arn:aws:iam::your-account-id:role/logging-role-name
```

Note

Même si le rôle de journalisation est facultatif, nous vous recommandons vivement de le configurer afin que vous puissiez voir l'état de vos messages et résoudre les problèmes de configuration.

Étape 3 : Importer des certificats en tant que ressources de certificats Transfer Family

Cette procédure explique comment importer des certificats à l'aide du AWS CLI. Si vous souhaitez plutôt utiliser la console Transfer Family, consultez [the section called “AS2Certificats d'importation”](#).

Pour importer les certificats de signature et de chiffrement que vous avez créés à l'étape 1, exécutez les `import-certificate` commandes suivantes. Si vous utilisez le même certificat pour le chiffrement et la signature, importez le même certificat deux fois (une fois avec l'`SIGNING` utilisation et une fois avec l'`ENCRYPTION` utilisation).

```
aws transfer import-certificate --usage SIGNING --certificate file://signing-cert.pem \
    --private-key file://signing-key.pem --certificate-chain file://root-ca.pem
```

Cette commande renvoie votre `signatureCertificateId`. Dans la section suivante, cet ID de certificat est appelé *my-signing-cert-id*.

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://encryption-
cert.pem \
    --private-key file://encryption-key.pem --certificate-chain file://root-
ca.pem
```

Cette commande renvoie votre `chiffrementCertificateId`. Dans la section suivante, cet ID de certificat est appelé *my-encrypt-cert-id*.

Importez ensuite les certificats de chiffrement et de signature de votre partenaire en exécutant les commandes suivantes.

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://partner-
encryption-cert.pem \
    --certificate-chain file://partner-root-ca.pem
```

Cette commande renvoie le chiffrement de votre partenaire `CertificateId`. Dans la section suivante, cet ID de certificat est appelé *partner-encrypt-cert-id*.

```
aws transfer import-certificate --usage SIGNING --certificate file://partner-signing-
cert.pem \
    --certificate-chain file://partner-root-ca.pem
```

Cette commande renvoie la signature de votre partenaire `CertificateId`. Dans la section suivante, cet ID de certificat est appelé *partner-signing-cert-id*.

Étape 4 : Créez des profils pour vous et votre partenaire commercial

Cette procédure explique comment créer des AS2 profils à l'aide de AWS CLI. Si vous souhaitez plutôt utiliser la console Transfer Family, consultez [the section called “Création de AS2 profils”](#).

Créez votre AS2 profil local en exécutant la commande suivante. Cette commande fait référence aux certificats contenant vos clés publiques et privées.

```
aws transfer create-profile --as2-id MYCORP --profile-type LOCAL --certificate-ids \
my-signing-cert-id my-encrypt-cert-id
```

Cette commande renvoie votre identifiant de profil. Dans la section suivante, cet identifiant est appelé *my-profile-id*.

Créez maintenant le profil du partenaire en exécutant la commande suivante. Cette commande utilise uniquement les certificats de clé publique de votre partenaire. Pour utiliser cette commande, remplacez le *user input placeholders* par vos propres informations, par exemple le AS2 nom et le certificat de votre partenaire IDs.

```
aws transfer create-profile --as2-id PARTNER-COMPANY --profile-type PARTNER --
certificate-ids \
partner-signing-cert-id partner-encrypt-cert-id
```

Cette commande renvoie l'identifiant de profil de votre partenaire. Dans la section suivante, cet identifiant est appelé *partner-profile-id*.

Note

Dans les commandes précédentes, remplacez *MYCORP* avec le nom de votre organisation, et *PARTNER-COMPANY* avec le nom de l'organisation de votre partenaire commercial.

Étape 5 : Créez un accord entre vous et votre partenaire

Cette procédure explique comment créer des AS2 accords à l'aide du AWS CLI. Si vous souhaitez plutôt utiliser la console Transfer Family, consultez [the section called “Créez des AS2 accords”](#).

Les accords réunissent les deux profils (local et partenaire), leurs certificats et une configuration de serveur qui permet les AS2 transferts entrants entre deux parties. Vous pouvez répertorier vos articles en exécutant les commandes suivantes.

```
aws transfer list-profiles --profile-type LOCAL
aws transfer list-profiles --profile-type PARTNER
aws transfer list-servers
```

Cette étape nécessite un compartiment et un IAM rôle Amazon S3 avec un accès en lecture/écriture vers et depuis le compartiment. Les instructions pour créer ce rôle sont les mêmes que pour le Transfer Family SFTP et FTP les FTPS protocoles et sont disponibles dans [Création d'un IAM rôle et d'une politique](#).

Pour créer un accord, vous avez besoin des éléments suivants :

- Le nom du compartiment Amazon S3 (et le préfixe de l'objet, s'il est spécifié)
- Le ARN IAM rôle ayant accès au bucket
- L'identifiant de votre serveur Transfer Family
- Votre identifiant de profil et l'identifiant de profil de votre partenaire

Créez l'accord en exécutant la commande suivante.

```
aws transfer create-agreement --description "ExampleAgreementName" --server-id your-server-id \
--local-profile-id your-profile-id --partner-profile-id your-partner-profile-id --base-
directory /DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox \
--access-role arn:aws:iam::111111111111:role/TransferAS2AccessRole
```

En cas de succès, cette commande renvoie l'ID de l'accord. Vous pouvez ensuite consulter les détails de l'accord à l'aide de la commande suivante.

```
aws transfer describe-agreement --agreement-id agreement-id --server-id your-server-id
```

Étape 6 : Créez un lien entre vous et votre partenaire

Cette procédure explique comment créer des AS2 connecteurs à l'aide du AWS CLI. Si vous souhaitez plutôt utiliser la console Transfer Family, consultez [the section called “Configuration des AS2 connecteurs”](#).

Vous pouvez utiliser cette `StartFileTransfer` API opération pour envoyer des fichiers stockés dans Amazon S3 vers le point de AS2 terminaison de votre partenaire commercial à l'aide d'un connecteur. Vous pouvez retrouver les profils que vous avez créés précédemment en exécutant la commande suivante.

```
aws transfer list-profiles
```

Lorsque vous créez le connecteur, vous devez fournir le AS2 serveur de votre partenaireURL. Copiez le texte suivant dans un fichier nommé `testAS2Config.json`.

```
{
  "Compression": "ZLIB",
  "EncryptionAlgorithm": "AES256_CBC",
  "LocalProfileId": "your-profile-id",
  "MdnResponse": "SYNC",
  "MdnSigningAlgorithm": "DEFAULT",
  "MessageSubject": "Your Message Subject",
  "PartnerProfileId": "partner-profile-id",
  "SigningAlgorithm": "SHA256"
}
```

Note

En effet `EncryptionAlgorithm`, ne spécifiez pas l'`DES_EDE3_CBC` algorithme sauf si vous devez prendre en charge un ancien client qui en a besoin, car il s'agit d'un algorithme de chiffrement faible.

Exécutez ensuite la commande suivante pour créer le connecteur.

```
aws transfer create-connector --url "http://partner-as2-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess
\
--as2-config file:///path/to/testAS2Config.json
```

Étape 7 : Testez l'échange de fichiers à AS2 l'aide de Transfer Family

Recevez un fichier de votre partenaire commercial

Si vous avez associé une adresse IP Elastic publique à votre VPC point de terminaison, Transfer Family a automatiquement créé un DNS nom contenant votre adresse IP publique. Le sous-domaine est l'ID de votre AWS Transfer Family serveur (au formats `-1234567890abcdef0`). Fournissez votre serveur URL à votre partenaire commercial dans le format suivant.

```
http://s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com:5080
```

Si vous n'avez pas associé d'adresse IP élastique publique à votre VPC point de terminaison, recherchez le nom d'hôte du point de VPC terminaison qui peut accepter les AS2 messages HTTP POST de vos partenaires commerciaux sur le port 5080. Pour récupérer les détails du VPC point de terminaison, utilisez la commande suivante.

```
aws transfer describe-server --server-id s-1234567890abcdef0
```

Supposons, par exemple, que la commande précédente renvoie un identifiant de point de VPC terminaison `devpce-1234abcd5678efghi`. Ensuite, vous devez utiliser la commande suivante pour récupérer les DNS noms.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1234abcd5678efghi
```

Cette commande renvoie tous les détails du VPC point de terminaison dont vous avez besoin pour exécuter la commande suivante.

Le DNS nom est répertorié dans le `DnsEntries` tableau. Votre partenaire commercial doit se trouver dans votre VPC enceinte pour accéder à votre VPC terminal (par exemple via AWS PrivateLink ou aVPN). Fournissez votre VPC point URL de terminaison à votre partenaire au format suivant.

```
http://vpce-your-vpce-id.vpce-svc-your-vpce-svc-id.your-region.vpce.amazonaws.com:5080
```

Par exemple, vous trouverez ci-dessous URL des exemples de valeurs pour les espaces réservés dans les commandes précédentes.

```
http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

Dans cet exemple, les transferts réussis sont stockés à l'emplacement spécifié dans le `base-directory` paramètre que vous avez spécifié dans [Étape 5 : Créez un accord entre vous et votre partenaire](#). Si nous recevons avec succès les fichiers nommés `myfile1.txt` et `myfile2.txt`, les fichiers sont stockés sous le nom `/path-defined-in-the-agreement/processed/original_filename.messageId.original_extension`. Ici, les fichiers sont stockés sous forme `/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile1.messageId.txt` et `/DOC-EXAMPLE-DESTINATION-BUCKET/AS2-inbox/processed/myfile2.messageId.txt`.

Si vous avez configuré un rôle de journalisation lors de la création de votre serveur Transfer Family, vous pouvez également consulter vos CloudWatch journaux pour connaître l'état des AS2 messages.

Envoyez un fichier à votre partenaire commercial

Vous pouvez utiliser Transfer Family pour envoyer AS2 des messages en faisant référence à l'ID du connecteur et aux chemins d'accès aux fichiers, comme illustré dans la commande suivante `start-file-transfer` AWS Command Line Interface (AWS CLI) :

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-SOURCE-BUCKET/
myfile2.txt"
```

Pour obtenir les détails de vos connecteurs, exécutez la commande suivante :

```
aws transfer list-connectors
```

La `list-connectors` commande renvoie le connecteur IDs et Amazon Resource Names (ARNs) pour vos connecteurs. URLs

Pour renvoyer les propriétés d'un connecteur spécifique, exécutez la commande suivante avec l'ID que vous souhaitez utiliser :

```
aws transfer describe-connector --connector-id your-connector-id
```

La `describe-connector` commande renvoie toutes les propriétés du connecteur, notamment ses rôles, ses profilsURL, ses notifications de disposition des messages (MDNs), ses balises et ses mesures de surveillance.

Vous pouvez vérifier que le partenaire a bien reçu les fichiers en consultant les MDN fichiers JSON et. Ces fichiers sont nommés conformément aux conventions décrites dans [Noms et emplacements](#)

[des fichiers](#). Si vous avez configuré un rôle de journalisation lors de la création du connecteur, vous pouvez également vérifier l'état des AS2 messages dans vos CloudWatch journaux.

Configuration d'un point SFTP de FTPS terminaison ou d'FTPun serveur

Cette rubrique fournit des informations détaillées sur la création et l'utilisation de points de terminaison de AWS Transfer Family serveur utilisant un ou plusieurs des FTP protocoles SFTPFTPS, et.

Rubriques

- [Options du fournisseur d'identité](#)
- [AWS Transfer Family matrice des types de terminaux](#)
- [Configuration d'un point SFTP de FTPS terminaison ou d'FTPun serveur](#)
- [Transfert de fichiers via un point de terminaison serveur à l'aide d'un client](#)
- [Gestion des utilisateurs pour les points de terminaison du serveur](#)
- [Utilisation de répertoires logiques pour simplifier vos structures de répertoires Transfer Family](#)

Options du fournisseur d'identité

AWS Transfer Family propose plusieurs méthodes d'authentification et de gestion des utilisateurs. Le tableau suivant compare les fournisseurs d'identité disponibles que vous pouvez utiliser avec Transfer Family.

Action	AWS Transfer Family service géré	AWS Managed Microsoft AD	APIPasserelle Amazon	AWS Lambda
Protocoles pris en charge	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Authentification basée sur des clés	Oui	Non	Oui	Oui

Action	AWS Transfer Family service géré	AWS Managed Microsoft AD	API Passerelle Amazon	AWS Lambda
Authentification par mot de passe	Non	Oui	Oui	Oui
AWS Identity and Access Management (IAM) et POSIX	Oui	Oui	Oui	Oui
Répertoire de base logique	Oui	Oui	Oui	Oui
Accès paramétré (basé sur le nom d'utilisateur)	Oui	Oui	Oui	Oui
Structure d'accès ad hoc	Oui	Non	Oui	Oui
AWS WAF	Non	Non	Oui	Non

Remarques :

- IAM est utilisé pour contrôler l'accès au stockage de sauvegarde Amazon S3, et POSIX est utilisé pour Amazon EFS.
- Ad hoc fait référence à la possibilité d'envoyer le profil utilisateur lors de l'exécution. Par exemple, vous pouvez rediriger les utilisateurs vers leur répertoire personnel en transmettant le nom d'utilisateur sous forme de variable.
- Pour plus de détails sur AWS WAF, voir [Ajouter un pare-feu pour applications Web](#).
- Un article de blog décrit l'utilisation d'une fonction Lambda intégrée à Microsoft Azure AD en tant que fournisseur d'identité Transfer Family. Pour plus de détails, consultez [Authentification AWS Transfer Family auprès d'Azure Active Directory et AWS Lambda](#).

- Nous proposons plusieurs AWS CloudFormation modèles pour vous aider à déployer rapidement un serveur Transfer Family qui utilise un fournisseur d'identité personnalisé. Pour plus de détails, consultez [Modèles de fonctions Lambda](#).

Dans les procédures suivantes, vous pouvez créer un SFTP serveur activé, un FTPS serveur activé, un FTP serveur activé ou AS2 un serveur activé.

Étape suivante

- [Création d'un SFTP serveur activé](#)
- [Création d'un FTPS serveur activé](#)
- [Création d'un FTP serveur activé](#)
- [Configuration AS2](#)

AWS Transfer Family matrice des types de terminaux

Lorsque vous créez un serveur Transfer Family, vous choisissez le type de point de terminaison à utiliser. Le tableau suivant décrit les caractéristiques de chaque type de point de terminaison.

Matrice des types de terminaux

Caractéristiques	Public	VPC- Internet	VPC- Interne	VPC_Endpoint (obsolète)
Protocoles pris en charge	SFTP	SFTP, FTPS, AS2	SFTP, FTP, FTPS, AS2	SFTP
Accès	Depuis Internet. Ce type de point de terminaison ne nécessite aucune configuration particulière dans votre VPC.	Sur Internet et depuis des environnements internes VPC et VPC connectés, tels qu'un centre de données sur site au-dessus AWS Direct	Depuis des environnements internes VPC et VPC connectés, tels qu'un centre de données sur site au-dessus AWS Direct Connect de ou. VPN	Depuis des environnements internes VPC et VPC connectés, tels qu'un centre de données sur site au-dessus AWS Direct Connect de ou. VPN

Caractéristiques	Public	VPC- Internet	VPC- Interne	VPC_Endpoint (obsolète)
		Connect de ou. VPN		
Adresse IP statique	Vous ne pouvez pas joindre une adresse IP statique. AWS fournit des adresses IP susceptibles d'être modifiées.	Vous pouvez associer des adresses IP élastiques au point de terminaison. Il peut s'agir d'adresses IP que vous AWS possédez ou de vos propres adresses IP (apportez vos propres adresses IP). Les adresses IP élastique s associées au point de terminaison ne changent pas. Les adresses IP privées associées au serveur ne changent pas non plus.	Les adresses IP privées associées au point de terminaison ne changent pas.	Les adresses IP privées associées au point de terminaison ne changent pas.

Caractéristiques	Public	VPC- Internet	VPC- Interne	VPC_Endpoint (obsolète)
Liste d'adresses IP autorisées source	Ce type de point de terminaison ne prend pas en charge les listes d'autorisation par adresse IP source. Le point de terminaison est accessible au public et écoute le trafic sur le port 22.  Note Pour les points de terminaison VPC hébergés, les serveurs SFTP Transfer Family peuvent fonctionner via le port 22 (par défaut)	Pour autoriser l'accès par adresse IP source, vous pouvez utiliser des groupes de sécurité attachés aux points de terminaison du serveur et un réseau ACLs rattaché au sous-réseau dans lequel se trouve le point de terminaison.	Pour autoriser l'accès par adresse IP source, vous pouvez utiliser des groupes de sécurité attachés aux points de terminaison du serveur et des listes de contrôle d'accès réseau (réseauACLs) attachées au sous-réseau dans lequel se trouve le point de terminaison.	Pour autoriser l'accès par adresse IP source, vous pouvez utiliser des groupes de sécurité attachés aux points de terminaison du serveur et un réseau ACLs rattaché au sous-réseau dans lequel se trouve le point de terminaison.

Caractéristiques	Public	VPC- Internet	VPC- Interne	VPC_Endpoint (obsolète)
	ou le port 2222.			
Liste d'autorisations du pare-feu client	Vous devez autoriser le DNS nom du serveur. Les adresses IP étant susceptibles de changer, évitez d'utiliser des adresses IP pour la liste d'autorisation de votre pare-feu client.	Vous pouvez autoriser le DNS nom du serveur ou les adresses IP élastiques associées au serveur.	Vous pouvez autoriser les adresses IP privées ou le DNS nom des points de terminaison.	Vous pouvez autoriser les adresses IP privées ou le DNS nom des points de terminaison.

Note

Le type de VPC_ENDPOINT point de terminaison est désormais obsolète et ne peut pas être utilisé pour créer de nouveaux serveurs. Au lieu de l'utiliser `EndpointType=VPC_ENDPOINT`, utilisez le nouveau type de point de VPC terminaison (`EndpointType=VPC`), que vous pouvez utiliser comme point de terminaison interne ou connecté à Internet, comme décrit dans le tableau précédent. Pour plus de détails, consultez [Cessation de l'utilisation de _ VPC_ENDPOINT](#).

Envisagez les options suivantes pour améliorer le niveau de sécurité de votre AWS Transfer Family serveur :

- Utilisez un VPC point de terminaison doté d'un accès interne, afin que le serveur ne soit accessible qu'aux clients au sein de votre environnement VPC ou d'environnements VPC connectés, tels qu'un centre de données sur site au-dessus AWS Direct Connect de ou. VPN

- Pour permettre aux clients d'accéder au point de terminaison via Internet et de protéger votre serveur, utilisez un VPC point de terminaison doté d'un accès Internet. Modifiez ensuite les groupes VPC de sécurité pour autoriser uniquement le trafic provenant de certaines adresses IP hébergeant les clients de vos utilisateurs.
- Si vous avez besoin d'une authentification par mot de passe et que vous utilisez un fournisseur d'identité personnalisé pour votre serveur, il est recommandé que votre politique en matière de mots de passe empêche les utilisateurs de créer des mots de passe faibles et limite le nombre de tentatives de connexion infructueuses.
- AWS Transfer Family est un service géré et ne fournit donc pas d'accès au shell. Vous ne pouvez pas accéder directement au SFTP serveur sous-jacent pour exécuter des commandes natives du système d'exploitation sur les serveurs Transfer Family.
- Utilisez un Network Load Balancer devant un VPC terminal disposant d'un accès interne. Changez le port d'écoute de l'équilibreur de charge du port 22 à un port différent. Cela peut réduire, mais pas éliminer, le risque que des scanners de ports et des robots explorent votre serveur, car le port 22 est le plus souvent utilisé pour le scan. Pour plus de détails, consultez le billet de blog [Les Network Load Balancers supportent désormais les groupes de sécurité](#).

Note

Si vous utilisez un Network Load Balancer, les AWS Transfer Family CloudWatch journaux indiquent l'adresse IP duNLB, plutôt que l'adresse IP réelle du client.

Configuration d'un point SFTP de FTPS terminaison ou d'FTPun serveur

Vous pouvez créer un serveur de transfert de fichiers à l'aide de ce AWS Transfer Family service. Les protocoles de transfert de fichiers suivants sont disponibles :

- Protocole de transfert de fichiers Secure Shell (SSH) (SFTP) — Transfert de fichiers effectuéSSH. Pour plus de détails, consultez [the section called “Création d'un SFTP serveur activé”](#).

Note

Nous fournissons un AWS CDK exemple de création d'un serveur SFTP Transfer Family. L'exemple utilise TypeScript, et est disponible GitHub [ici](#).

- File Transfer Protocol Secure (FTPS) — Transfert de fichiers avec TLS chiffrement. Pour plus de détails, consultez [the section called “Création d'un FTPS serveur activé”](#).
- Protocole de transfert de fichiers (FTP) — Transfert de fichiers non chiffré. Pour plus de détails, consultez [the section called “Création d'un FTP serveur activé”](#).
- Déclaration d'applicabilité 2 (AS2) — Transfert de fichiers pour le transport de business-to-business données structurées. Pour plus de détails, consultez [the section called “Configurez AS2”](#). En AS2 effet, vous pouvez créer rapidement une AWS CloudFormation pile à des fins de démonstration. Cette procédure est décrite dans [Utilisez un modèle pour créer un AS2 stack Transfer Family de démonstration](#).

Vous pouvez créer un serveur avec plusieurs protocoles.

 Note

Si plusieurs protocoles sont activés pour le même point de terminaison de serveur et que vous souhaitez fournir un accès en utilisant le même nom d'utilisateur sur plusieurs protocoles, vous pouvez le faire à condition que les informations d'identification spécifiques au protocole aient été configurées dans votre fournisseur d'identité. Pour FTP, nous vous recommandons de conserver des informations d'identification distinctes de SFTP et FTPS. Cela est dû au fait que, contrairement à SFTP et FTPS, FTP transmet les informations d'identification en texte clair. En isolant les FTP informations d'identification de vos charges de travail SFTP ou FTPS, si FTP elles sont partagées ou exposées, en utilisant SFTP ou en préservant leur sécurité FTPS.

Lorsque vous créez un serveur, vous choisissez un serveur spécifique Région AWS pour exécuter les demandes d'opérations de fichier des utilisateurs assignés à ce serveur. Outre l'attribution d'un ou de plusieurs protocoles au serveur, vous attribuez également l'un des types de fournisseurs d'identité suivants :

- Service géré à l'aide de SSH clés. Pour plus de détails, consultez [Travailler avec des utilisateurs gérés par des services](#).
- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Cette méthode vous permet d'intégrer vos groupes Microsoft Active Directory afin de fournir un accès à vos serveurs Transfer Family. Pour plus de détails, consultez [Utilisation du fournisseur d'identité du AWS Directory Service](#).

- Une méthode personnalisée. La méthode du fournisseur d'identité personnalisé utilise AWS Lambda Amazon API Gateway et vous permet d'intégrer votre service d'annuaire pour authentifier et autoriser vos utilisateurs. Le service attribue automatiquement un identifiant qui identifie de façon unique votre serveur. Pour plus de détails, consultez [Travailler avec des fournisseurs d'identité personnalisés](#). Transfer Family fournit des AWS CloudFormation modèles que vous pouvez utiliser pour déployer rapidement des serveurs utilisant un fournisseur d'identité personnalisé.
- [Fonctions Lambda pour l'authentification](#) décrit les CloudFormation modèles qui utilisent une fonction Lambda pour l'authentification.
- [Authentification à l'aide d'une méthode API Gateway](#) décrit les CloudFormation modèles qui utilisent une méthode Amazon API Gateway pour l'authentification.

Vous attribuez également au serveur un type de point de terminaison (accessible au public ou VPC hébergé) et un nom d'hôte en utilisant le point de terminaison du serveur par défaut, ou un nom d'hôte personnalisé en utilisant le service Amazon Route 53 ou en utilisant le service Domain Name System (DNS) de votre choix. Le nom d'hôte d'un serveur doit être unique dans l' Région AWS endroit où il a été créé.

En outre, vous pouvez attribuer un rôle de CloudWatch journalisation Amazon pour envoyer des événements à vos CloudWatch journaux, choisir une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur et ajouter des métadonnées au serveur sous la forme de balises qui sont des paires clé-valeur.

Important

Vous engagez des coûts pour les serveurs instanciés et pour le transfert de données. Pour plus d'informations sur les tarifs et Calculateur de tarification AWS pour obtenir une estimation du coût d'utilisation de Transfer Family, consultez [AWS Transfer Family les tarifs](#).

Création d'un SFTP serveur activé

Le protocole de transfert de fichiers Secure Shell (SSH/SFTP) est un protocole réseau utilisé pour le transfert sécurisé de données sur Internet. Le protocole prend en charge toutes les fonctionnalités de sécurité et d'authentification de SSH. Il est largement utilisé pour échanger des données, y compris des informations sensibles entre des partenaires commerciaux de divers secteurs tels que les services financiers, les soins de santé, le commerce de détail et la publicité.

Note

SFTP Les serveurs de Transfer Family fonctionnent via le port 22. Pour les terminaux VPC hébergés, les serveurs SFTP Transfer Family peuvent également fonctionner via le port 2222. Pour plus de détails, consultez [Création d'un serveur dans un cloud privé virtuel](#).

Voir aussi

- Nous fournissons un AWS CDK exemple de création d'un serveur SFTP Transfer Family. L'exemple utilise TypeScript, et est disponible GitHub [ici](#).
- Pour savoir comment déployer un serveur Transfer Family au sein d'un VPC, voir [Utiliser la liste d'adresses IP autorisées pour sécuriser vos AWS Transfer Family serveurs](#).

Pour créer un SFTP serveur activé

1. Ouvrez la AWS Transfer Family console sur <https://console.aws.amazon.com/transfer/> et sélectionnez Servers dans le volet de navigation, puis choisissez Create server.
2. Dans Choisir les protocoles, sélectionnez SFTP, puis cliquez sur Suivant.

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☒ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

Cancel Next

3. Dans Choisir un fournisseur d'identité, choisissez le fournisseur d'identité que vous souhaitez utiliser pour gérer l'accès des utilisateurs. Vous avez les options suivantes :
- Service géré — Vous y stockez les identités et les clés des utilisateurs AWS Transfer Family.

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☒ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

[Cancel](#) [Previous](#) [Next](#)

- **AWS Directory Service for Microsoft Active Directory**— Vous fournissez un AWS Directory Service répertoire pour accéder au point de terminaison. Ce faisant, vous pouvez utiliser les informations d'identification stockées dans votre Active Directory pour authentifier vos utilisateurs. Pour en savoir plus sur la collaboration avec les fournisseurs AWS Managed Microsoft AD d'identité, consultez [Utilisation du fournisseur d'identité du AWS Directory Service](#).

Note

- Les annuaires multicomptes et partagés ne sont pas pris en charge pour AWS Managed Microsoft AD.
- Pour configurer un serveur avec Directory Service comme fournisseur d'identité, vous devez ajouter des AWS Directory Service autorisations. Pour plus de détails, consultez [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#).

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ Service managed
Create and manage users within the service

☒ AWS Directory
[Service Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ Custom Identity Provider
[Provider Info](#)
Manage users by integrating an identity provider of your choice

Directory
TATER3

Cancel Previous Next

- Fournisseur d'identité personnalisé : choisissez l'une des options suivantes :
 - AWS Lambda À utiliser pour connecter votre fournisseur d'identité : vous pouvez utiliser un fournisseur d'identité existant, soutenu par une fonction Lambda. Vous indiquez le nom de la fonction Lambda. Pour de plus amples informations, veuillez consulter [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#).
 - Utilisez Amazon API Gateway pour connecter votre fournisseur d'identité : vous pouvez créer une méthode API Gateway basée sur une fonction Lambda à utiliser en tant que fournisseur d'identité. Vous fournissez un Amazon API Gateway URL et un rôle d'invocation. Pour de plus amples informations, veuillez consulter [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#).

Pour l'une ou l'autre option, vous pouvez également spécifier le mode d'authentification.

- Mot de passe OU clé : les utilisateurs peuvent s'authentifier à l'aide de leur mot de passe ou de leur clé. C'est la valeur par défaut.
- Mot de passe ONLY : les utilisateurs doivent fournir leur mot de passe pour se connecter.
- Clé ONLY : les utilisateurs doivent fournir leur clé privée pour se connecter.
- ANDClé de mot de passe : les utilisateurs doivent fournir leur clé privée et leur mot de passe pour se connecter. Le serveur vérifie d'abord la clé, puis si la clé est valide, le système

demande un mot de passe. Si la clé privée fournie ne correspond pas à la clé publique stockée, l'authentification échoue.

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ Service managed
Create and manage users within the service

☐ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function

Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) Either a valid password or valid private key will be required during user authentication

Cancel Previous Next

4. Choisissez Suivant.
5. Dans Choisir un point de terminaison, procédez comme suit :
 - a. Pour le type de point de terminaison, choisissez le type de point de terminaison accessible au public. Pour un point de terminaison VPChébergé, voir [Création d'un serveur dans un cloud privé virtuel](#).
 - b. (Facultatif) Pour Nom d'hôte personnalisé, choisissez Aucun.

Vous obtenez un nom d'hôte de serveur fourni par AWS Transfer Family. Le nom d'hôte du serveur se présente sous la forme `serverId.server.transfer.regionId.amazonaws.com`.

Pour un nom d'hôte personnalisé, vous devez spécifier un alias personnalisé pour le point de terminaison de votre serveur. Pour en savoir plus sur l'utilisation de noms d'hôtes personnalisés, consultez [Utilisation de noms d'hôtes personnalisés](#).

- c. (Facultatif) Pour FIPSActivé, cochez la case FIPSEnabled endpoint pour vous assurer que le endpoint est conforme aux normes fédérales de traitement de l'information (FIPS).

Note

FIPSLes points de terminaison compatibles ne sont disponibles que dans les régions d'Amérique AWS du Nord. Pour les régions disponibles, consultez les [AWS Transfer Family points de terminaison et les quotas](#) dans le Références générales AWS. Pour plus d'informations surFIPS, voir [Federal Information Processing Standard \(FIPS\) 140-2](#).

- d. Choisissez Suivant.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☒ **Publicly accessible**
Accessible over the internet

☐ **VPC hosted** [Info](#)
Access controlled using Security Groups

Custom hostname
Specify a custom alias for your server endpoint.

None ▼

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ **FIPS Enabled endpoint**

Cancel Previous **Next**

- 6. Sur la page Choisir un domaine, choisissez le service de AWS stockage que vous souhaitez utiliser pour stocker et accéder à vos données via le protocole sélectionné :

- Choisissez Amazon S3 pour stocker et accéder à vos fichiers sous forme d'objets via le protocole sélectionné.
- Choisissez Amazon EFS pour stocker et accéder à vos fichiers dans votre système de EFS fichiers Amazon via le protocole sélectionné.

Choisissez Suivant.

7. Dans Configurer les détails supplémentaires, procédez comme suit :
 - a. Pour la journalisation, spécifiez un groupe de journaux existant ou créez-en un nouveau (option par défaut).

The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. The left sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains two sections: 'Logging' and 'Logging role'. The 'Logging' section has a heading 'Log group' and a description: 'Choose the CloudWatch log group where your events will be delivered in a structured JSON format'. It features two radio buttons: 'Create a new log group' (selected) and 'Choose an existing log group'. Below these is a dropdown menu labeled 'Choose an existing log group' with a refresh icon and a 'Create log group' button with an external link icon. The 'Logging role' section has a heading 'Logging role' and a description: 'Choose the IAM role that will be used to deliver events to your CloudWatch logs'. It features two radio buttons: 'Create a new role' (selected) and 'Choose an existing role'. At the bottom, a blue information box states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Si vous choisissez un groupe de journaux existant, vous devez en sélectionner un qui est associé à votre Compte AWS.

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

/aws/transfer/ [dropdown] [refresh] [Create log group]

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

Logging role is only required when selecting a workflow in the Managed workflows section below.

Si vous choisissez Créer un groupe de journaux, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) s'ouvre sur la page Créer un groupe de journaux. Pour plus de détails, voir [Création d'un groupe de CloudWatch journaux dans Logs](#).

- b. (Facultatif) Pour les flux de travail gérés, choisissez le flux de travail IDs (et le rôle correspondant) que Transfer Family doit assumer lors de l'exécution du flux de travail. Vous pouvez choisir un flux de travail à exécuter lors d'un téléchargement complet et un autre à exécuter lors d'un téléchargement partiel. Pour en savoir plus sur le traitement de vos fichiers à l'aide de flux de travail gérés, consultez [AWS Transfer Family flux de travail gérés](#).

Managed workflows Info

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

[w- [dropdown]] [refresh] [Create a new Workflow]

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

[w- [dropdown]] [refresh] [Create a new Workflow]

Managed workflows execution role Info
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

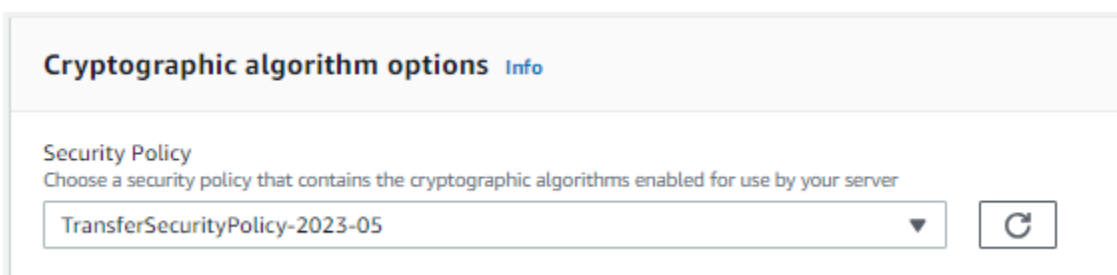
- c. Pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur.

Note

Par défaut :

- Si le point de terminaison FIPS activé n'est pas sélectionné, la politique de TransferSecurityPolicy-2020-06 sécurité est attachée à votre serveur.
- Si FIPSEnabled endpoint est sélectionné, la politique de TransferSecurityPolicy-FIPS-2020-06 sécurité est attachée à votre serveur.

Pour plus d'informations sur les stratégies de sécurité, consultez [Politiques de sécurité pour AWS Transfer Family](#).



Cryptographic algorithm options Info

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05

- d. (Facultatif) Pour la clé d'hôte du serveur RSAED25519, entrez une clé ECDSA privée ou une clé privée qui sera utilisée pour identifier votre serveur lorsque les clients s'y connecteront SFTP. Vous pouvez également ajouter une description pour différencier les différentes clés d'hôte.

Après avoir créé votre serveur, vous pouvez ajouter des clés d'hôte supplémentaires. Il est utile de disposer de plusieurs clés hôtes si vous souhaitez faire pivoter des clés ou si vous souhaitez avoir différents types de clés, comme une RSA clé et une ECDSA clé.

Note

La section Server Host Key est utilisée uniquement pour migrer des utilisateurs depuis un serveur SFTP compatible existant.

Server Host Key [Info](#)

Private key - *optional*

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - *optional*

Add a description to differentiate between multiple private keys

Enter optional description

i You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (Facultatif) Pour les balises, pour la clé et la valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
- f. Choisissez Suivant.

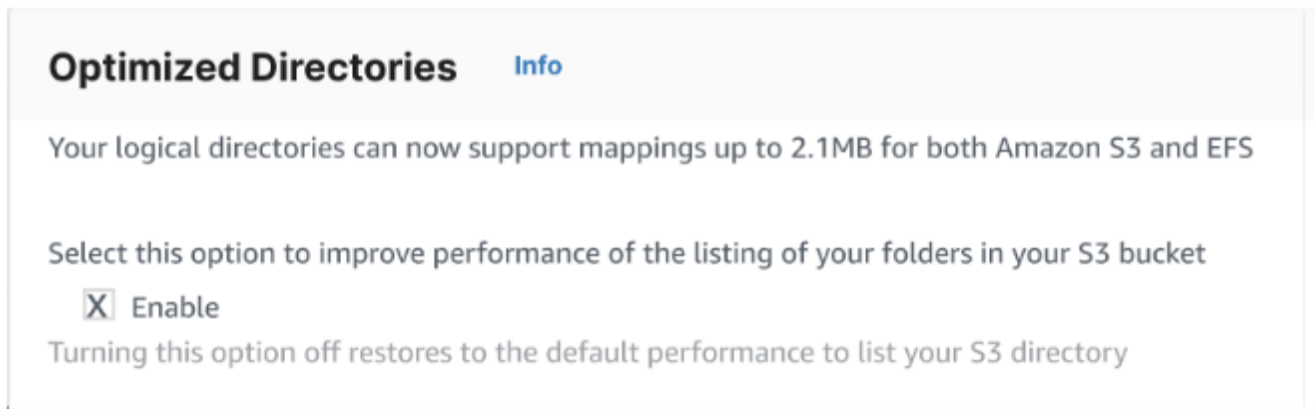
Tags

Key	Value	
Enter key	Enter value	<button>Remove tag</button>

Add tag

Cancel Previous Next

- g. Vous pouvez optimiser les performances de vos annuaires Amazon S3. Supposons, par exemple, que vous vous rendiez dans votre répertoire personnel et que vous disposiez de 10 000 sous-répertoires. En d'autres termes, votre compartiment S3 contient 10 000 dossiers. Dans ce scénario, si vous exécutez la commande `ls` (list), l'opération de liste prend entre six et huit minutes. Toutefois, si vous optimisez vos répertoires, cette opération ne prend que quelques secondes.



Optimized Directories [Info](#)

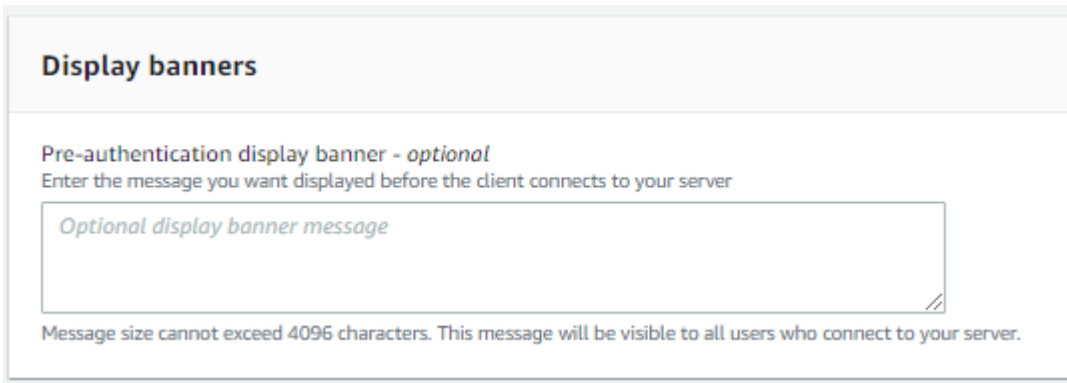
Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

- h. (Facultatif) Configurez AWS Transfer Family les serveurs pour afficher des messages personnalisés tels que les politiques organisationnelles ou les conditions générales à l'intention de vos utilisateurs finaux. Pour Afficher la bannière, dans la zone de texte de la bannière d'affichage préalable à l'authentification, entrez le message texte que vous souhaitez afficher à vos utilisateurs avant qu'ils ne s'authentifient.



Display banners

Pre-authentication display banner - *optional*
Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

- i. (Facultatif) Vous pouvez configurer les options supplémentaires suivantes.
- SetStat option : activez cette option pour ignorer l'erreur générée lorsqu'un client tente de l'utiliser SETSTAT sur un fichier que vous téléchargez dans un compartiment Amazon S3. Pour plus de détails, consultez la SetStatOption documentation dans le [ProtocolDetails](#).
 - TLSreprise de session : cette option n'est disponible que si vous l'avez activée FTPS comme l'un des protocoles pour ce serveur.
 - IP passive : cette option n'est disponible que si vous avez activé FTPS ou FTP en tant que protocole pour ce serveur.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

 To enable TLS session resumption, enable FTPS as one of the protocols selected in Step 1

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

 To enable Passive IP, enable FTP or FTPS as one of the protocols selected in Step 1

8. Dans Réviser et créer, passez en revue vos choix.

- Si vous souhaitez modifier l'un d'entre eux, choisissez Modifier à côté de l'étape.

 Note

Vous devez passer en revue chaque étape après celle que vous avez choisi de modifier.

- Si aucune modification n'est apportée, choisissez Create server pour créer votre serveur. Vous êtes dirigé vers la page Servers (Serveurs), représentée ci-dessous, dans laquelle figure votre nouveau serveur.

Quelques minutes peuvent s'écouler avant que le statut de votre nouveau serveur passe à En ligne. À ce stade, votre serveur peut effectuer des opérations sur fichiers pour vos utilisateurs.

Servers (1)							Actions	Add user	Create server
☐	Hostname	Server ID	State	users	Endpoint type	Domain			
☐	-	s-	Starting	No Users	Public	Amazon S3			

Création d'un FTPS serveur activé

Le protocole de transfert de fichiers over SSL (FTPS) est une extension de FTP. Il utilise les protocoles cryptographiques Transport Layer Security (TLS) et Secure Sockets Layer (SSL) pour chiffrer le trafic. FTPS permet le chiffrement des connexions au canal de commande et au canal de données, simultanément ou indépendamment.

Pour créer un FTPS serveur activé

1. Ouvrez la AWS Transfer Family console sur <https://console.aws.amazon.com/transfer/> et sélectionnez Servers dans le volet de navigation, puis choisissez Create server.
2. Dans Choisir les protocoles, sélectionnez FTPS.

Pour le certificat de serveur, choisissez un certificat stocké dans AWS Certificate Manager (ACM) qui sera utilisé pour identifier votre serveur lorsque les clients s'y connecteront, FTPS puis choisissez Next.

Pour demander un nouveau certificat public, consultez la section [Demander un certificat public](#) dans le guide de AWS Certificate Manager l'utilisateur.

Pour importer un certificat existant dans ACM, consultez la section [Importation de certificats ACM](#) dans le guide de AWS Certificate Manager l'utilisateur.

Pour demander un certificat privé à utiliser FTPS via des adresses IP privées, consultez la section [Demande d'un certificat privé](#) dans le guide de AWS Certificate Manager l'utilisateur.

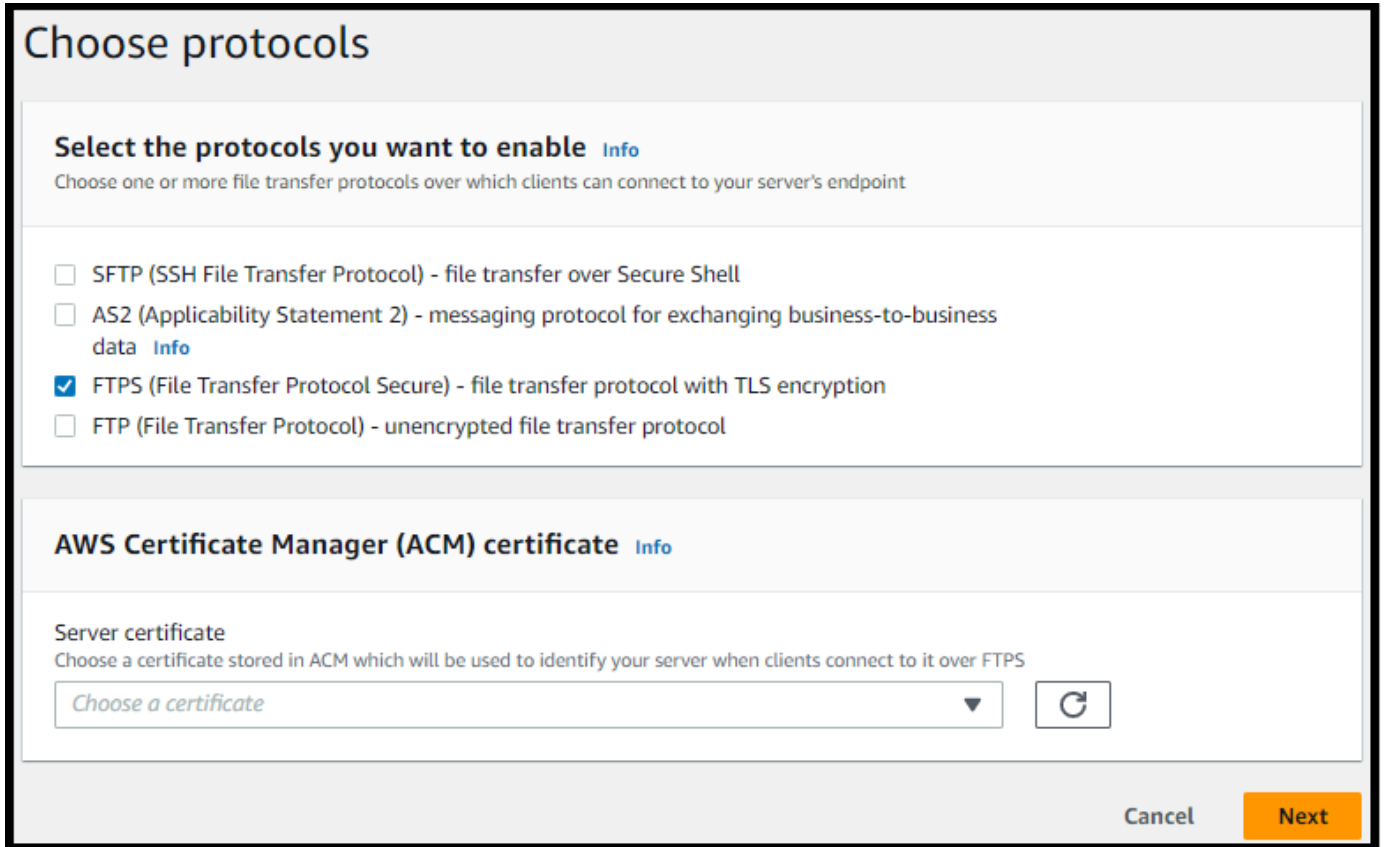
Les certificats avec les algorithmes de chiffrement et les tailles de clés suivants sont pris en charge :

- 2048 bits RSA (_2048) RSA
- 4096 bits (_4096RSA) RSA
- Elliptic Prime Curve 256 octets (EC_prime256v1)
- Elliptic Prime Curve 384 octets (EC_secp384r1)

- Elliptic Prime Curve 521 octets (EC_secp521r1)

 Note

Le certificat doit être un SSL TLS certificat/X.509 version 3 valide avec une FQDN adresse IP spécifiée et des informations sur l'émetteur.



Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☒ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

AWS Certificate Manager (ACM) certificate [Info](#)

Server certificate

Choose a certificate stored in ACM which will be used to identify your server when clients connect to it over FTPS



[Cancel](#) [Next](#)

3. Dans Choisir un fournisseur d'identité, choisissez le fournisseur d'identité que vous souhaitez utiliser pour gérer l'accès des utilisateurs. Vous avez les options suivantes :
- AWS Directory Service for Microsoft Active Directory— Vous fournissez un AWS Directory Service répertoire pour accéder au point de terminaison. Ce faisant, vous pouvez utiliser les informations d'identification stockées dans votre Active Directory pour authentifier vos utilisateurs. Pour en savoir plus sur la collaboration avec les fournisseurs AWS Managed Microsoft AD d'identité, consultez [Utilisation du fournisseur d'identité du AWS Directory Service](#).

Note

- Les annuaires multicomptes et partagés ne sont pas pris en charge pour AWS Managed Microsoft AD.
- Pour configurer un serveur avec Directory Service comme fournisseur d'identité, vous devez ajouter des AWS Directory Service autorisations. Pour plus de détails, consultez [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#).

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ Service managed
Create and manage users within the service

☒ AWS Directory **Service Info**
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ Custom Identity Provider **Provider Info**
Manage users by integrating an identity provider of your choice

Directory
TATER3

Cancel Previous Next

- Fournisseur d'identité personnalisé : choisissez l'une des options suivantes :
 - AWS Lambda À utiliser pour connecter votre fournisseur d'identité : vous pouvez utiliser un fournisseur d'identité existant, soutenu par une fonction Lambda. Vous indiquez le nom de la fonction Lambda. Pour de plus amples informations, veuillez consulter [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#).
 - Utilisez Amazon API Gateway pour connecter votre fournisseur d'identité : vous pouvez créer une méthode API Gateway basée sur une fonction Lambda à utiliser en tant que fournisseur d'identité. Vous fournissez un Amazon API Gateway URL et un rôle d'invocation.

Pour de plus amples informations, veuillez consulter [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory

Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity

Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

[i](#) To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel

Previous

Next

4. Choisissez Suivant.
5. Dans Choisir un point de terminaison, procédez comme suit :

[i](#) Note

FTPSLes serveurs de Transfer Family fonctionnent sur le port 21 (canal de contrôle) et sur la plage de ports 8192 à 8200 (canal de données).

- a. Pour le type de point de terminaison, choisissez le type de point de terminaison VPC hébergé pour héberger le point de terminaison de votre serveur. Pour plus d'informations sur la configuration de votre point de terminaison VPC hébergé, consultez [Création d'un serveur dans un cloud privé virtuel](#).

 Note

Les points de terminaison accessibles au public ne sont pas pris en charge.

- b. (Facultatif) Pour FIPS Activé, cochez la case FIPSEnabled endpoint pour vous assurer que le endpoint est conforme aux normes fédérales de traitement de l'information (FIPS).

 Note

FIPS Les points de terminaison compatibles ne sont disponibles que dans les régions d'Amérique AWS du Nord. Pour les régions disponibles, consultez les [AWS Transfer Family points de terminaison et les quotas](#) dans le Références générales AWS. Pour plus d'informations sur FIPS, voir [Federal Information Processing Standard \(FIPS\) 140-2](#).

- c. Choisissez Suivant.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

6. Sur la page Choisir un domaine, choisissez le service de AWS stockage que vous souhaitez utiliser pour stocker et accéder à vos données via le protocole sélectionné :
- Choisissez Amazon S3 pour stocker et accéder à vos fichiers sous forme d'objets via le protocole sélectionné.
 - Choisissez Amazon EFS pour stocker et accéder à vos fichiers dans votre système de EFS fichiers Amazon via le protocole sélectionné.

Choisissez Suivant.

7. Dans Configurer les détails supplémentaires, procédez comme suit :

- a. Pour la journalisation, spécifiez un groupe de journaux existant ou créez-en un nouveau (option par défaut).

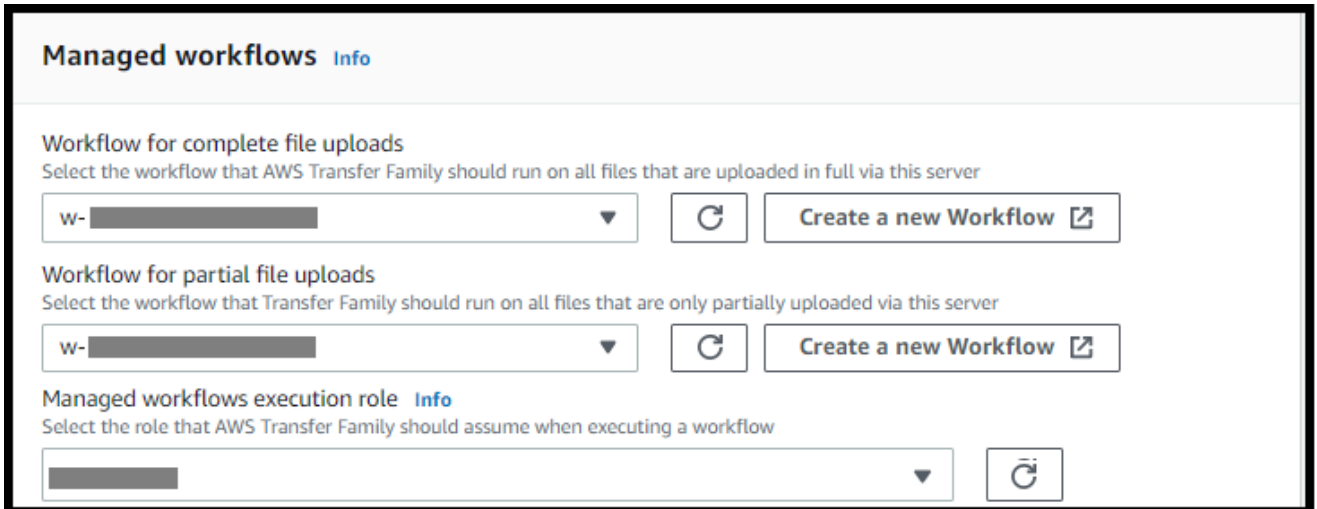
The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details), and Step 6 (Review and create). Step 5 is currently selected. The main content area is titled 'Configure additional details' and contains a 'Logging' section. Under 'Log group', there are two radio buttons: 'Create a new log group' (which is selected) and 'Choose an existing log group'. Below these is a dropdown menu for 'Choose an existing log group' and a 'Create log group' button. Under 'Logging role', there are two radio buttons: 'Create a new role' and 'Choose an existing role'. A blue information box at the bottom states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Si vous choisissez un groupe de journaux existant, vous devez en sélectionner un qui est associé à votre Compte AWS.

This screenshot shows the same 'Configure additional details' step, but with 'Choose an existing log group' selected. The 'Log group' section now shows a dropdown menu with the path '/aws/transfer/' and a 'Create log group' button. The 'Logging role' section remains the same with 'Create a new role' selected. The same blue information box is present at the bottom.

Si vous choisissez Créer un groupe de journaux, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) s'ouvre sur la page Créer un groupe de journaux. Pour plus de détails, voir [Création d'un groupe de CloudWatch journaux dans Logs](#).

- b. (Facultatif) Pour les flux de travail gérés, choisissez le flux de travail IDs (et le rôle correspondant) que Transfer Family doit assumer lors de l'exécution du flux de travail. Vous pouvez choisir un flux de travail à exécuter lors d'un téléchargement complet et un autre à exécuter lors d'un téléchargement partiel. Pour en savoir plus sur le traitement de vos fichiers à l'aide de flux de travail gérés, consultez [AWS Transfer Family flux de travail gérés](#).



The screenshot displays the 'Managed workflows' configuration page in the AWS Transfer Family console. It includes three main sections: 'Workflow for complete file uploads', 'Workflow for partial file uploads', and 'Managed workflows execution role'. Each section has a dropdown menu for selecting a workflow, a refresh button, and a 'Create a new Workflow' button with an external link icon. The 'Managed workflows execution role' section also includes a dropdown menu and a refresh button.

- c. Pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur.

Note

Par défaut :

- Si le point de terminaison FIPS activé n'est pas sélectionné, la politique de TransferSecurityPolicy-2020-06 sécurité est attachée à votre serveur.
- Si FIPSEnabled endpoint est sélectionné, la politique de TransferSecurityPolicy-FIPS-2020-06 sécurité est attachée à votre serveur.

Pour plus d'informations sur les stratégies de sécurité, consultez [Politiques de sécurité pour AWS Transfer Family](#).

Cryptographic algorithm options [Info](#)

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05

↕



- d. Pour la clé d'hôte du serveur, laissez-la vide.

 Note

La section Server Host Key est utilisée uniquement pour migrer des utilisateurs depuis un serveur SFTP compatible existant.

Server Host Key [Info](#)

Private key - optional

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - optional

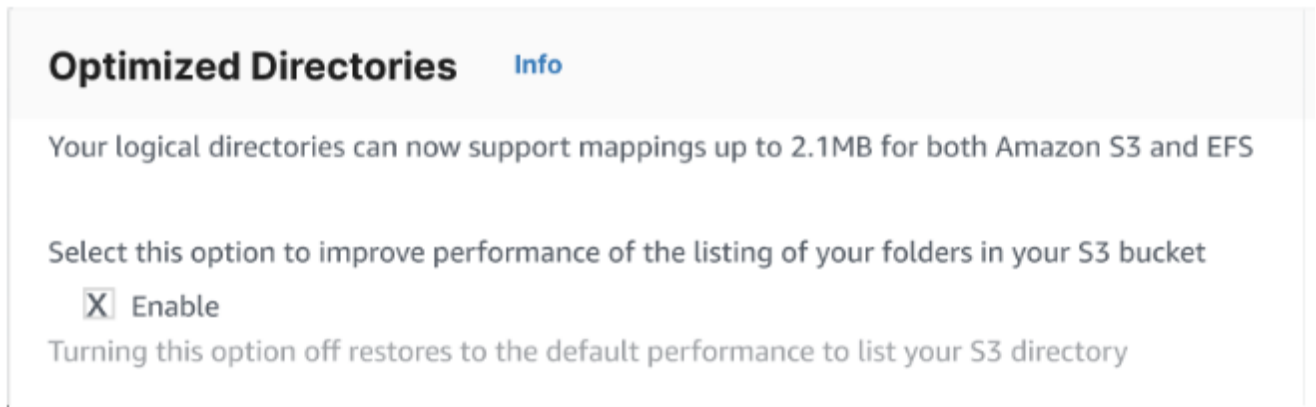
Add a description to differentiate between multiple private keys

Enter optional description

 You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (Facultatif) Pour les balises, pour la clé et la valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
- f. Vous pouvez optimiser les performances de vos annuaires Amazon S3. Supposons, par exemple, que vous vous rendiez dans votre répertoire personnel et que vous disposiez de 10 000 sous-répertoires. En d'autres termes, votre compartiment S3 contient 10 000 dossiers. Dans ce scénario, si vous exécutez la commande `ls` (list), l'opération de liste

prend entre six et huit minutes. Toutefois, si vous optimisez vos répertoires, cette opération ne prend que quelques secondes.



Optimized Directories [Info](#)

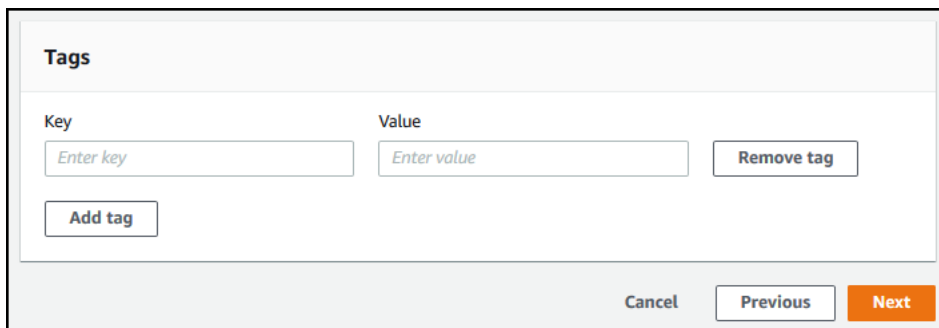
Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

g. Choisissez Suivant.



Tags

Key	Value	
Enter key	Enter value	Remove tag

h. (Facultatif) Vous pouvez configurer AWS Transfer Family les serveurs pour afficher des messages personnalisés tels que les politiques organisationnelles ou les conditions générales à l'intention de vos utilisateurs finaux. Vous pouvez également afficher un message du jour personnalisé (MOTD) aux utilisateurs qui se sont authentifiés avec succès.

Pour Afficher la bannière, dans la zone de texte de la bannière d'affichage préalable à l'authentification, entrez le message texte que vous souhaitez afficher à vos utilisateurs avant qu'ils ne s'authentifient, et dans la zone de texte de la bannière d'affichage après l'authentification, entrez le texte que vous souhaitez afficher à vos utilisateurs une fois qu'ils se sont authentifiés avec succès.

Display banners

Pre-authentication display banner - optional
Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

Post-authentication display banner - optional
Enter the message you want displayed after the client has connected to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

i SFTP clients will only be able to see the pre-authentication message. FTPS and FTP clients will be able to see both pre-authentication and post-authentication messages.

- i. (Facultatif) Vous pouvez configurer les options supplémentaires suivantes.
- **SetStat option** : activez cette option pour ignorer l'erreur générée lorsqu'un client tente de l'utiliser SETSTAT sur un fichier que vous téléchargez dans un compartiment Amazon S3. Pour plus de détails, consultez la [SetStatOption](#) documentation dans cette [ProtocolDetails](#) rubrique.
 - **TLS reprise de session** : fournit un mécanisme permettant de reprendre ou de partager une clé secrète négociée entre le contrôle et la connexion de données pour une FTPS session. Pour plus de détails, consultez la [TlsSessionResumptionMode](#) documentation dans cette [ProtocolDetails](#) rubrique.
 - **IP passive** : indique le mode passif, pour FTP et les FTPS protocoles. Entrez une IPv4 adresse unique, telle que l'adresse IP publique d'un pare-feu, d'un routeur ou d'un équilibreur de charge. Pour plus de détails, consultez la [PassiveIp](#) documentation dans cette [ProtocolDetails](#) rubrique.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce
☐ Enable
☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. Dans Réviser et créer, passez en revue vos choix.

- Si vous souhaitez modifier l'un d'entre eux, choisissez Modifier à côté de l'étape.

 Note

Vous devez passer en revue chaque étape après celle que vous avez choisi de modifier.

- Si aucune modification n'est apportée, choisissez Create server pour créer votre serveur. Vous êtes dirigé vers la page Servers (Serveurs), représentée ci-dessous, dans laquelle figure votre nouveau serveur.

Quelques minutes peuvent s'écouler avant que le statut de votre nouveau serveur passe à En ligne. À ce stade, votre serveur peut effectuer des opérations sur fichiers pour vos utilisateurs.

Servers (1)									Actions ▾	Add user	Create server
☐	Hostname	Server ID	State	users	Endpoint type	Domain					
☐	-	s-	 Starting	 No Users	Public	Amazon S3					

Prochaines étapes : Pour l'étape suivante, passez [Travailler avec des fournisseurs d'identité personnalisés](#) à la section Configuration des utilisateurs.

Création d'un FTP serveur activé

Le protocole de transfert de fichiers (FTP) est un protocole réseau utilisé pour le transfert de données. FTP utilise un canal séparé pour le contrôle et les transferts de données. Le canal de contrôle est ouvert jusqu'à son arrêt ou jusqu'à expiration du délai d'inactivité. Le canal de données est actif pendant toute la durée du transfert. FTP utilise du texte clair et ne prend pas en charge le chiffrement du trafic.

Note

Lorsque vous l'activez FTP, vous devez choisir l'option d'accès interne pour le point de terminaison VPC -hosted. Si vous avez besoin que les données de votre serveur transitent par le réseau public, vous devez utiliser des protocoles sécurisés, tels que SFTP ou FTPS.

Pour créer un FTP serveur activé

1. Ouvrez la AWS Transfer Family console sur <https://console.aws.amazon.com/transfer/> et sélectionnez Servers dans le volet de navigation, puis choisissez Create server.
2. Dans Choisir les protocoles, sélectionnez FTP, puis cliquez sur Suivant.

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☒ FTP (File Transfer Protocol) - unencrypted file transfer protocol

Cancel Next

3. Dans Choisir un fournisseur d'identité, choisissez le fournisseur d'identité que vous souhaitez utiliser pour gérer l'accès des utilisateurs. Vous avez les options suivantes :

- AWS Directory Service for Microsoft Active Directory— Vous fournissez un AWS Directory Service répertoire pour accéder au point de terminaison. Ce faisant, vous pouvez utiliser les informations d'identification stockées dans votre Active Directory pour authentifier vos utilisateurs. Pour en savoir plus sur la collaboration avec les fournisseurs AWS Managed Microsoft AD d'identité, consultez [Utilisation du fournisseur d'identité du AWS Directory Service](#).

Note

- Les annuaires multicomptes et partagés ne sont pas pris en charge pour AWS Managed Microsoft AD.
- Pour configurer un serveur avec Directory Service comme fournisseur d'identité, vous devez ajouter des AWS Directory Service autorisations. Pour plus de détails, consultez [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#).

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☒ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

Directory
TATER3 ▼ ↺

Cancel Previous Next

- Fournisseur d'identité personnalisé : choisissez l'une des options suivantes :
- AWS Lambda À utiliser pour connecter votre fournisseur d'identité : vous pouvez utiliser un fournisseur d'identité existant, soutenu par une fonction Lambda. Vous indiquez le nom de

la fonction Lambda. Pour de plus amples informations, veuillez consulter [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#).

- Utilisez Amazon API Gateway pour connecter votre fournisseur d'identité : vous pouvez créer une méthode API Gateway basée sur une fonction Lambda à utiliser en tant que fournisseur d'identité. Vous fournissez un Amazon API Gateway URL et un rôle d'invocation. Pour de plus amples informations, veuillez consulter [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#).

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☒ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function





Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ Password OR public key
☐ Password ONLY
☐ Public Key ONLY
☐ Password AND public key

 To choose an authentication method, enable SFTP as one of the protocols selected in Step 1

Cancel Previous Next

4. Choisissez Suivant.

5. Dans Choisir un point de terminaison, procédez comme suit :

 Note

FTP Les serveurs de Transfer Family fonctionnent sur le port 21 (canal de contrôle) et sur la plage de ports 8192 à 8200 (canal de données).

- a. Pour le type de point de terminaison, choisissez VPChébergé pour héberger le point de terminaison de votre serveur. Pour plus d'informations sur la configuration de votre point de terminaison VPC hébergé, consultez [Création d'un serveur dans un cloud privé virtuel](#).

 Note

Les points de terminaison accessibles au public ne sont pas pris en charge.

- b. Pour FIPSEnabled, laissez la case FIPSEnabled endpoint décochée.

 Note

FIPS Les points de terminaison compatibles ne sont pas pris en charge pour les FTP serveurs.

- c. Choisissez Suivant.

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

6. Sur la page Choisir un domaine, choisissez le service de AWS stockage que vous souhaitez utiliser pour stocker et accéder à vos données via le protocole sélectionné.
- Choisissez Amazon S3 pour stocker et accéder à vos fichiers sous forme d'objets via le protocole sélectionné.
 - Choisissez Amazon EFS pour stocker et accéder à vos fichiers dans votre système de EFS fichiers Amazon via le protocole sélectionné.

Choisissez Suivant.

7. Dans Configurer les détails supplémentaires, procédez comme suit :

- a. Pour la journalisation, spécifiez un groupe de journaux existant ou créez-en un nouveau (option par défaut).

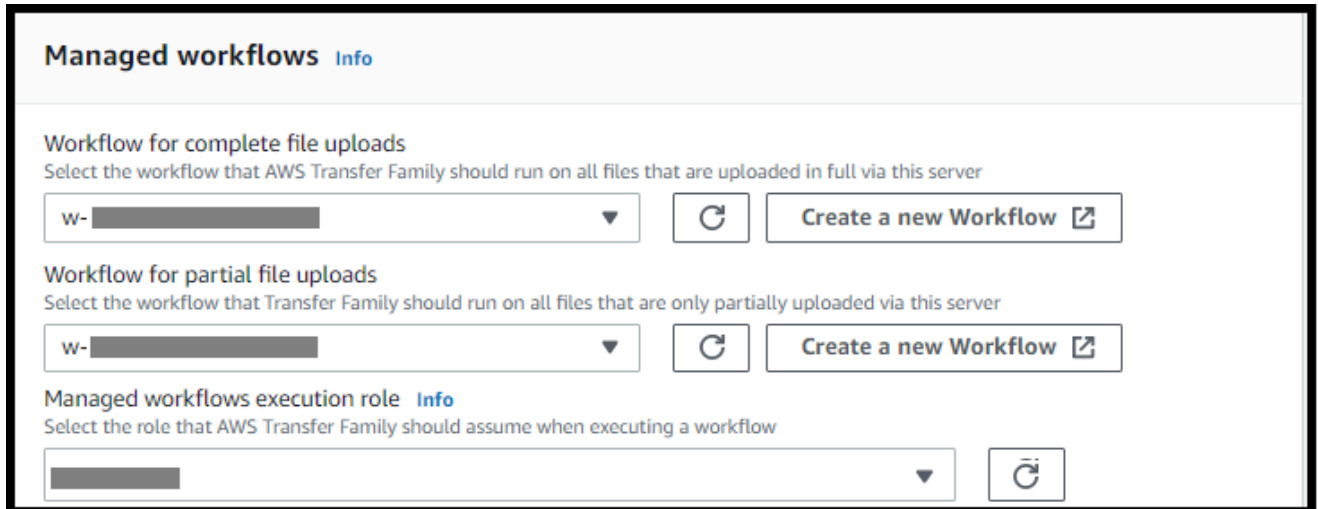
The screenshot shows the 'Configure additional details' step in the AWS Transfer Family console. On the left, a sidebar lists six steps: Step 1 (Choose protocols), Step 2 (Choose an identity provider), Step 3 (Choose an endpoint), Step 4 (Choose a domain), Step 5 (Configure additional details), and Step 6 (Review and create). Step 5 is currently selected. The main content area is titled 'Configure additional details' and contains a 'Logging' section. Under 'Log group', there are two radio buttons: 'Create a new log group' (which is selected) and 'Choose an existing log group'. Below these is a dropdown menu for 'Choose an existing log group' and a 'Create log group' button. Under 'Logging role', there are two radio buttons: 'Create a new role' and 'Choose an existing role'. A blue information box at the bottom states: 'Logging role is only required when selecting a workflow in the Managed workflows section below.'

Si vous choisissez un groupe de journaux existant, vous devez en sélectionner un qui est associé à votre Compte AWS.

This screenshot shows the same 'Configure additional details' step, but with 'Choose an existing log group' selected. The 'Log group' section now shows a dropdown menu with the path '/aws/transfer/' and a 'Create log group' button. The 'Logging role' section remains the same with 'Create a new role' selected. The same blue information box is present at the bottom.

Si vous choisissez Créer un groupe de journaux, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) s'ouvre sur la page Créer un groupe de journaux. Pour plus de détails, voir [Création d'un groupe de CloudWatch journaux dans Logs](#).

- b. (Facultatif) Pour les flux de travail gérés, choisissez le flux de travail IDs (et le rôle correspondant) que Transfer Family doit assumer lors de l'exécution du flux de travail. Vous pouvez choisir un flux de travail à exécuter lors d'un téléchargement complet et un autre à exécuter lors d'un téléchargement partiel. Pour en savoir plus sur le traitement de vos fichiers à l'aide de flux de travail gérés, consultez [AWS Transfer Family flux de travail gérés](#).



The screenshot displays the 'Managed workflows' section in the AWS Transfer Family console. It features three main configuration areas:

- Workflow for complete file uploads:** Includes a dropdown menu with a placeholder 'w-' and a refresh button, followed by a 'Create a new Workflow' button with an external link icon.
- Workflow for partial file uploads:** Similar to the first section, with a dropdown menu, a refresh button, and a 'Create a new Workflow' button.
- Managed workflows execution role:** Includes a dropdown menu with a refresh button.

Each section has an 'Info' link next to its title.

- c. Pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur.

Note

Transfer Family attribue la dernière politique de sécurité à votre FTP serveur. Cependant, comme le FTP protocole n'utilise aucun chiffrement, FTP les serveurs n'utilisent aucun algorithme de politique de sécurité. À moins que votre serveur n'utilise également le SFTP protocole FTPS or, la politique de sécurité reste inutilisée.

Cryptographic algorithm options [Info](#)

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05

▼



- d. Pour la clé d'hôte du serveur, laissez-la vide.

 Note

La section Server Host Key est utilisée uniquement pour migrer des utilisateurs depuis un serveur SFTP compatible existant.

Server Host Key [Info](#)

Private key - optional

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - optional

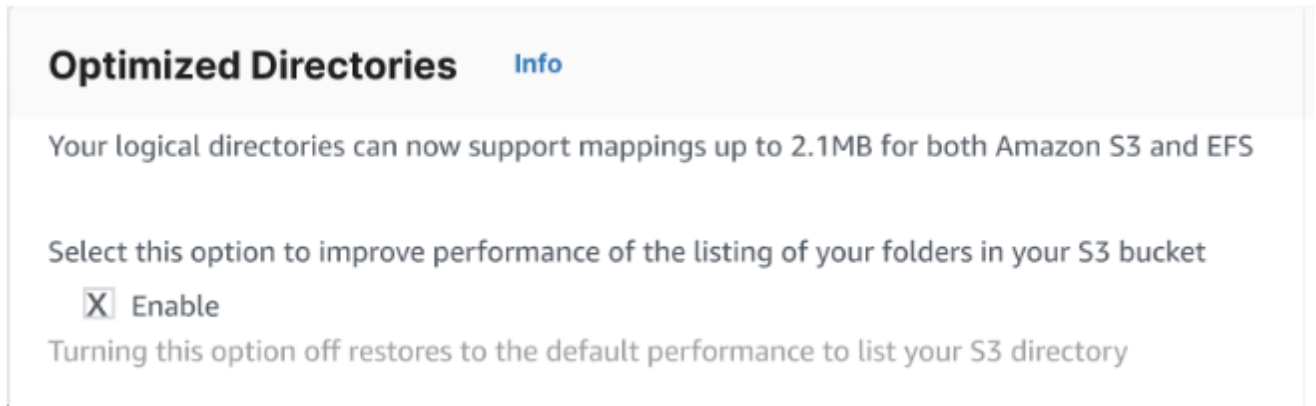
Add a description to differentiate between multiple private keys

Enter optional description

 You can ignore this section unless you are migrating users from an existing SFTP server.

- e. (Facultatif) Pour les balises, pour la clé et la valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
- f. Vous pouvez optimiser les performances de vos annuaires Amazon S3. Supposons, par exemple, que vous vous rendiez dans votre répertoire personnel et que vous disposiez de 10 000 sous-répertoires. En d'autres termes, votre compartiment S3 contient 10 000

dossiers. Dans ce scénario, si vous exécutez la commande `ls` (list), l'opération de liste prend entre six et huit minutes. Toutefois, si vous optimisez vos répertoires, cette opération ne prend que quelques secondes.



Optimized Directories [Info](#)

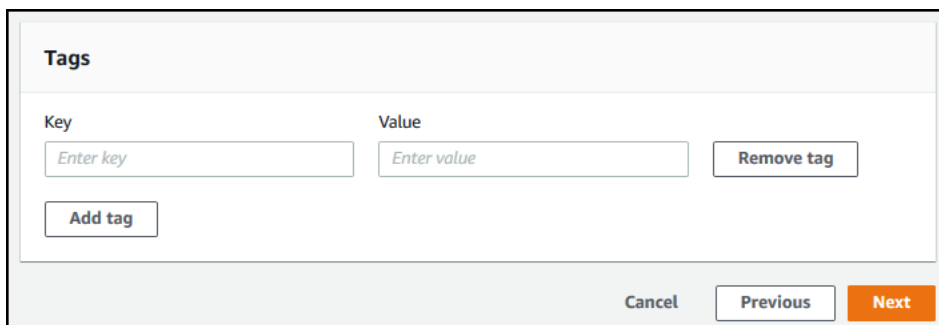
Your logical directories can now support mappings up to 2.1MB for both Amazon S3 and EFS

Select this option to improve performance of the listing of your folders in your S3 bucket

☒ Enable

Turning this option off restores to the default performance to list your S3 directory

g. Choisissez Suivant.



Tags

Key Value

h. (Facultatif) Vous pouvez configurer AWS Transfer Family les serveurs pour afficher des messages personnalisés tels que les politiques organisationnelles ou les conditions générales à l'intention de vos utilisateurs finaux. Vous pouvez également afficher un message du jour personnalisé (MOTD) aux utilisateurs qui se sont authentifiés avec succès.

Pour Afficher la bannière, dans la zone de texte de la bannière d'affichage préalable à l'authentification, entrez le message texte que vous souhaitez afficher à vos utilisateurs avant qu'ils ne s'authentifient, et dans la zone de texte de la bannière d'affichage après l'authentification, entrez le texte que vous souhaitez afficher à vos utilisateurs une fois qu'ils se sont authentifiés avec succès.

Display banners

Pre-authentication display banner - optional
Enter the message you want displayed before the client connects to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

Post-authentication display banner - optional
Enter the message you want displayed after the client has connected to your server

Optional display banner message

Message size cannot exceed 4096 characters. This message will be visible to all users who connect to your server.

i SFTP clients will only be able to see the pre-authentication message. FTPS and FTP clients will be able to see both pre-authentication and post-authentication messages.

- i. (Facultatif) Vous pouvez configurer les options supplémentaires suivantes.
- **SetStat option** : activez cette option pour ignorer l'erreur générée lorsqu'un client tente de l'utiliser SETSTAT sur un fichier que vous téléchargez dans un compartiment Amazon S3. Pour plus de détails, consultez la [SetStatOption](#) documentation dans cette [ProtocolDetails](#) rubrique.
 - **TLS reprise de session** : fournit un mécanisme permettant de reprendre ou de partager une clé secrète négociée entre le contrôle et la connexion de données pour une FTPS session. Pour plus de détails, consultez la [TlsSessionResumptionMode](#) documentation dans cette [ProtocolDetails](#) rubrique.
 - **IP passive** : indique le mode passif, pour FTP et les FTPS protocoles. Entrez une IPv4 adresse unique, telle que l'adresse IP publique d'un pare-feu, d'un routeur ou d'un équilibreur de charge. Pour plus de détails, consultez la [PassiveIp](#) documentation dans cette [ProtocolDetails](#) rubrique.

Additional configuration

SetStat option - optional [Info](#)
Select whether you want this server to ignore SetStat command

☐ Enable

TLS session resumption - optional [Info](#)
Choose how you want your server to process TLS session resumption requests

☒ Enforce

☐ Enable

☐ Disable

Passive IP - optional [Info](#)
Provide passive IP (PASV) that file transfer clients can use to connect this server

1.2.3.4

8. Dans Réviser et créer, passez en revue vos choix.

- Si vous souhaitez modifier l'un d'entre eux, choisissez Modifier à côté de l'étape.

 Note

Vous devez passer en revue chaque étape après celle que vous avez choisi de modifier.

- Si aucune modification n'est apportée, choisissez Create server pour créer votre serveur. Vous êtes dirigé vers la page Servers (Serveurs), représentée ci-dessous, dans laquelle figure votre nouveau serveur.

Quelques minutes peuvent s'écouler avant que le statut de votre nouveau serveur passe à En ligne. À ce stade, votre serveur peut effectuer des opérations sur fichiers pour vos utilisateurs.

Servers (1)									Actions ▾	Add user	Create server
☐	Hostname	Server ID	State	users	Endpoint type	Domain					
☐	-	s-	 Starting	 No Users	Public	Amazon S3					

Étapes suivantes — Pour l'étape suivante, passez [Travailler avec des fournisseurs d'identité personnalisés](#) à la section Configuration des utilisateurs.

Création d'un serveur dans un cloud privé virtuel

Vous pouvez héberger le point de terminaison de votre serveur dans un cloud privé virtuel (VPC) afin de transférer des données vers et depuis un compartiment Amazon S3 ou un système de EFS fichiers Amazon sans passer par Internet public.

Note

Après le 19 mai 2021, vous ne pourrez plus créer de serveur EndpointType=VPC_ENDPOINT à l'aide de votre AWS compte si celui-ci ne l'a pas déjà fait avant le 19 mai 2021. Si vous avez déjà créé des serveurs EndpointType=VPC_ENDPOINT dans votre AWS compte le 21 février 2021 ou avant, vous ne serez pas concerné. Après cette date, utilisez EndpointType =**VPC**. Pour de plus amples informations, veuillez consulter [the section called “Cessation de l'utilisation de _ VPC ENDPOINT”](#).

Si vous utilisez Amazon Virtual Private Cloud (AmazonVPC) pour héberger vos AWS ressources, vous pouvez établir une connexion privée entre vous VPC et un serveur. Vous pouvez ensuite utiliser ce serveur pour transférer des données via votre client vers et depuis votre compartiment Amazon S3 sans utiliser d'adresse IP publique ni nécessiter de passerelle Internet.

Amazon VPC vous permet de lancer AWS des ressources sur un réseau virtuel personnalisé. Vous pouvez utiliser a VPC pour contrôler vos paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles réseau. Pour plus d'informationsVPCs, consultez [Qu'est-ce qu'Amazon VPC ?](#) dans le guide de VPC l'utilisateur Amazon.

Dans les sections suivantes, vous trouverez des instructions sur la façon de créer un serveur et VPC de vous y connecter. En résumé, procédez comme suit :

1. Configurez un serveur à l'aide d'un VPC point de terminaison.
2. Connectez-vous à votre serveur à l'aide d'un client qui se trouve à l'intérieur de vous VPC via le VPC point de terminaison. Cela vous permet de transférer les données stockées dans votre compartiment Amazon S3 via votre client à l'aide de AWS Transfer Family. Vous pouvez effectuer ce transfert même si le réseau est déconnecté de l'Internet public.
3. En outre, si vous choisissez de faire en sorte que le point de terminaison de votre serveur soit connecté à Internet, vous pouvez associer des adresses IP élastiques à votre point de

terminaison. Cela permet à des clients extérieurs à vous de VPC se connecter à votre serveur. Vous pouvez utiliser des groupes VPC de sécurité pour contrôler l'accès aux utilisateurs authentifiés dont les demandes proviennent uniquement d'adresses autorisées.

Rubriques

- [Créez un point de terminaison de serveur accessible uniquement dans votre VPC](#)
- [Créez un point de terminaison connecté à Internet pour votre serveur](#)
- [Modifier le type de point de terminaison de votre serveur](#)
- [Cessation de l'utilisation de _ VPC ENDPOINT](#)
- [Mise à jour du type de point de terminaison du AWS Transfer Family serveur de VPC _ ENDPOINT à VPC](#)

Créez un point de terminaison de serveur accessible uniquement dans votre VPC

Dans la procédure suivante, vous allez créer un point de terminaison de serveur accessible uniquement aux ressources de votre VPC.

Pour créer un point de terminaison de serveur dans un VPC

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, sélectionnez Servers, puis Create server.
3. Dans Choisir des protocoles, sélectionnez un ou plusieurs protocoles, puis cliquez sur Suivant. Pour plus d'informations sur les protocoles, consultez [Étape 2 : Création d'un SFTP serveur compatible](#).
4. Dans Choisir un fournisseur d'identité, choisissez Service géré pour stocker les identités et les clés des utilisateurs AWS Transfer Family, puis cliquez sur Suivant.

Note

Cette procédure utilise l'option de gestion des services. Si vous choisissez Personnalisé, vous fournissez un point de terminaison Amazon API Gateway et un rôle AWS Identity and Access Management (IAM) pour accéder au point de terminaison. Ce faisant, vous pouvez intégrer votre service d'annuaire pour authentifier et autoriser vos utilisateurs. Pour en savoir plus sur l'utilisation de fournisseurs d'identité personnalisés, consultez [Travailler avec des fournisseurs d'identité personnalisés](#).

5. Dans Choisir un point de terminaison, procédez comme suit :

Note

FTPet FTPS les serveurs de Transfer Family fonctionnent sur le port 21 (canal de contrôle) et sur la plage de ports 8192 à 8200 (canal de données).

- a. Pour le type de point de terminaison, choisissez le type de point de terminaison VPC hébergé pour héberger le point de terminaison de votre serveur.
- b. Pour Accès, choisissez Internal pour que votre point de terminaison ne soit accessible qu'aux clients utilisant les adresses IP privées du point de terminaison.

Note

Pour plus de détails sur l'option Internet Facing, voir [Créez un point de terminaison connecté à Internet pour votre serveur](#). Un serveur créé uniquement VPC pour un accès interne ne prend pas en charge les noms d'hôte personnalisés.

- c. Pour VPC, choisissez un VPC identifiant existant ou choisissez Créer un VPC pour en créer un nouveau VPC.
- d. Dans la section Zones de disponibilité, choisissez jusqu'à trois zones de disponibilité et les sous-réseaux associés.
- e. Dans la section Groupes de sécurité, choisissez un ID de groupe de sécurité existant IDs ou choisissez Créer un groupe de sécurité pour créer un nouveau groupe de sécurité. Pour plus d'informations sur les groupes de sécurité, consultez [la section Groupes de sécurité correspondants VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud. Pour créer un groupe de sécurité, consultez la section [Création d'un groupe de sécurité](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Note

Vous êtes VPC automatiquement associé à un groupe de sécurité par défaut. Si vous ne spécifiez pas un ou plusieurs groupes de sécurité différents lorsque vous lancez le serveur, nous associons le groupe de sécurité par défaut à votre serveur.

En ce qui concerne les règles de trafic entrant pour le groupe de sécurité, vous pouvez configurer le SSH trafic pour qu'il utilise le port 22, le port 2222 ou les deux. Le port 22 est configuré par défaut. Pour utiliser le port 2222, vous devez ajouter une règle entrante à votre groupe de sécurité. Pour le type, choisissez Personnalisé TCP, puis entrez **2222** pour la plage de ports, et pour la source, entrez la même CIDR plage que celle que vous avez pour votre règle SSH du port 22.

The screenshot shows the 'Edit inbound rules' interface for a security group. It displays a table of inbound rules with columns for Security group rule ID, Type, Protocol, Port range, and Source. The rule for 'Custom TCP' on port '2222' is highlighted with a red rectangle. The source IP for this rule is '72.21.196.64/32'.

Security group rule ID	Type	Protocol	Port range	Source
sgr-...	HTTP	TCP	80	Custom 0.0.0.0/0
sgr-...	RDP	TCP	3389	Custom 0.0.0.0/0
sgr-...	HTTPS	TCP	443	Custom 0.0.0.0/0
sgr-...	Custom TCP	TCP	2222	Custom 72.21.196.64/32
sgr-...	SSH	TCP	22	Custom 72.21.196.64/32

- f. (Facultatif) Pour FIPSActivé, cochez la case FIPSEnabled endpoint pour vous assurer que le endpoint est conforme aux normes fédérales de traitement de l'information (FIPS).

Note

FIPSLes points de terminaison compatibles ne sont disponibles que dans les régions d'Amérique AWS du Nord. Pour les régions disponibles, consultez les [AWS Transfer Family points de terminaison et les quotas](#) dans le Références générales AWS. Pour plus d'informations surFIPS, voir [Federal Information Processing Standard \(FIPS\) 140-2](#).

- g. Choisissez Suivant.
6. Dans Configurer les détails supplémentaires, procédez comme suit :
- a. Pour la CloudWatch journalisation, choisissez l'une des options suivantes pour activer la CloudWatch journalisation de votre activité utilisateur par Amazon :

- Créez un nouveau rôle pour permettre à Transfer Family de le IAM créer automatiquement, à condition que vous disposiez des autorisations nécessaires pour créer un nouveau rôle. Le IAM rôle créé est appelé `AWSTransferLoggingAccess`.
- Choisissez un rôle existant pour choisir un IAM rôle existant dans votre compte. Sous Rôle de journalisation, choisissez le rôle. Ce IAM rôle doit inclure une politique de confiance avec le service défini sur `transfer.amazonaws.com`.

Pour plus d'informations sur la CloudWatch journalisation, consultez [Configurer le rôle de CloudWatch journalisation](#).

 Note

- Vous ne pouvez pas consulter l'activité de l'utilisateur final CloudWatch si vous ne spécifiez pas de rôle de journalisation.
- Si vous ne souhaitez pas configurer de rôle de CloudWatch journalisation, sélectionnez Choisir un rôle existant, mais ne sélectionnez pas de rôle de journalisation.

- b. Pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur.

 Note

Par défaut, la politique `TransferSecurityPolicy-2020-06` de sécurité est attachée à votre serveur, sauf si vous en choisissez une autre.

Pour plus d'informations sur les stratégies de sécurité, consultez [Politiques de sécurité pour AWS Transfer Family](#).

- c. (Facultatif) Pour la clé d'hôte du serveur RSAED25519, entrez une clé ECDSA privée ou une clé privée qui sera utilisée pour identifier votre serveur lorsque les clients s'y connecteront SFTP.

 Note

Cette section concerne uniquement la migration des utilisateurs depuis un serveur SFTP compatible existant.

- d. (Facultatif) Pour les balises, pour la clé et la valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
 - e. Choisissez Suivant.
7. Dans Réviser et créer, passez en revue vos choix. Si vous :
- Si vous souhaitez modifier l'un d'entre eux, choisissez Modifier à côté de l'étape.

 Note

Vous devrez passer en revue chaque étape après celle que vous avez choisi de modifier.

- Si aucune modification n'est apportée, choisissez Create server pour créer votre serveur. Vous êtes dirigé vers la page Servers (Serveurs), représentée ci-dessous, dans laquelle figure votre nouveau serveur.

Quelques minutes peuvent s'écouler avant que le statut de votre nouveau serveur passe à En ligne. À ce stade, votre serveur peut effectuer des opérations sur fichiers pour vos utilisateurs.

Créez un point de terminaison connecté à Internet pour votre serveur

Dans la procédure suivante, vous allez créer un point de terminaison de serveur. Ce point de terminaison n'est accessible via Internet qu'aux clients dont les adresses IP sources sont autorisées dans votre groupe VPC de sécurité par défaut. En outre, en utilisant des adresses IP élastiques pour rendre votre terminal connecté à Internet, vos clients peuvent utiliser l'adresse IP élastique pour autoriser l'accès à votre point de terminaison dans leurs pare-feux.

 Note

Uniquement SFTP et FTPS utilisable sur un terminal VPC hébergé connecté à Internet.

Pour créer un point de terminaison connecté à Internet

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, sélectionnez Servers, puis Create server.
3. Dans Choisir des protocoles, sélectionnez un ou plusieurs protocoles, puis cliquez sur Suivant. Pour plus d'informations sur les protocoles, consultez [Étape 2 : Création d'un SFTP serveur compatible](#).
4. Dans Choisir un fournisseur d'identité, choisissez Service géré pour stocker les identités et les clés des utilisateurs AWS Transfer Family, puis cliquez sur Suivant.

Note

Cette procédure utilise l'option de gestion des services. Si vous choisissez Personnalisé, vous fournissez un point de terminaison Amazon API Gateway et un rôle AWS Identity and Access Management (IAM) pour accéder au point de terminaison. Ce faisant, vous pouvez intégrer votre service d'annuaire pour authentifier et autoriser vos utilisateurs. Pour en savoir plus sur l'utilisation de fournisseurs d'identité personnalisés, consultez [Travailler avec des fournisseurs d'identité personnalisés](#).

5. Dans Choisir un point de terminaison, procédez comme suit :
 - a. Pour le type de point de terminaison, choisissez le type de point de terminaison VPChébergé pour héberger le point de terminaison de votre serveur.
 - b. Pour Access, choisissez Internet Facing pour rendre votre terminal accessible aux clients via Internet.

Note

Lorsque vous choisissez Internet Facing, vous pouvez choisir une adresse IP élastique existante dans chaque sous-réseau ou sous-réseaux. Vous pouvez également accéder à la VPC console (<https://console.aws.amazon.com/vpc/>) pour allouer une ou plusieurs nouvelles adresses IP élastiques. Ces adresses peuvent être détenues par vous AWS ou par vous. Vous ne pouvez pas associer les adresses IP élastiques déjà utilisées à votre point de terminaison.

- c. (Facultatif) Pour Nom d'hôte personnalisé, choisissez l'une des options suivantes :

 Note

Les clients qui AWS GovCloud (US) ont besoin de se connecter directement via l'adresse IP Elastic ou de créer un enregistrement de nom d'hôte dans Commercial Route 53 pointant vers leur EIP. Pour plus d'informations sur l'utilisation de Route 53 pour les GovCloud points de terminaison, consultez la section [Configuration d'Amazon Route 53 avec vos AWS GovCloud \(US\) ressources](#) dans le Guide de l'AWS GovCloud (US) utilisateur.

- DNSAlias Amazon Route 53 : si le nom d'hôte que vous souhaitez utiliser est enregistré auprès de Route 53. Vous pouvez ensuite saisir le nom d'hôte.
- Autre DNS : si le nom d'hôte que vous souhaitez utiliser est enregistré auprès d'un autre DNS fournisseur. Vous pouvez ensuite saisir le nom d'hôte.
- Aucun : pour utiliser le point de terminaison du serveur et ne pas utiliser de nom d'hôte personnalisé. Le nom d'hôte du serveur se présente sous la forme `server-id.server.transfer.region.amazonaws.com`.

 Note

Pour les clients inscrits AWS GovCloud (US), sélectionner Aucun ne crée pas de nom d'hôte dans ce format.

Pour en savoir plus sur l'utilisation de noms d'hôtes personnalisés, consultez [Utilisation de noms d'hôtes personnalisés](#).

- d. Pour VPC, choisissez un VPC existant ou choisissez Créer un VPC pour en créer un nouveau VPC.
- e. Dans la section Zones de disponibilité, choisissez jusqu'à trois zones de disponibilité et les sous-réseaux associés. Pour IPv4Adresses, choisissez une adresse IP élastique pour chaque sous-réseau. Il s'agit de l'adresse IP que vos clients peuvent utiliser pour autoriser l'accès à votre point de terminaison dans leurs pare-feux.
- f. Dans la section Groupes de sécurité, choisissez un ID de groupe de sécurité existant ou choisissez Créer un groupe de sécurité pour créer un nouveau groupe de sécurité. Pour plus d'informations sur les groupes de sécurité, consultez [la section Groupes de sécurité](#)

[correspondants VPC](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud. Pour créer un groupe de sécurité, consultez la section [Création d'un groupe de sécurité](#) dans le guide de l'utilisateur d'Amazon Virtual Private Cloud.

Note

Vous êtes VPC automatiquement associé à un groupe de sécurité par défaut. Si vous ne spécifiez pas un ou plusieurs groupes de sécurité différents lorsque vous lancez le serveur, nous associons le groupe de sécurité par défaut à votre serveur.

En ce qui concerne les règles de trafic entrant pour le groupe de sécurité, vous pouvez configurer le SSH trafic pour qu'il utilise le port 22, le port 2222 ou les deux. Le port 22 est configuré par défaut. Pour utiliser le port 2222, vous devez ajouter une règle entrante à votre groupe de sécurité. Pour le type, choisissez Personnalisé TCP, puis entrez **2222** pour la plage de ports, et pour la source, entrez la même CIDR plage que celle que vous avez pour votre règle SSH du port 22.

VPC > Security Groups > sg-...-default > Edit inbound rules

Edit inbound rules [info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type info	Protocol info	Port range info	Source info
sg-...	HTTP	TCP	80	Custom 0.0.0.0/0
sg-...	RDP	TCP	3389	Custom 0.0.0.0/0
sg-...	HTTPS	TCP	443	Custom 0.0.0.0/0
sg-...	Custom TCP	TCP	2222	Custom 72.21.196.64/32
sg-...	SSH	TCP	22	Custom 72.21.196.64/32

Add rule

- g. (Facultatif) Pour FIPSActivé, cochez la case FIPSEnabled endpoint pour vous assurer que le endpoint est conforme aux normes fédérales de traitement de l'information (FIPS).

Note

FIPSLes points de terminaison compatibles ne sont disponibles que dans les régions d'Amérique AWS du Nord. Pour les régions disponibles, consultez les [AWS Transfer Family points de terminaison et les quotas](#) dans le Références générales

AWS. Pour plus d'informations sur FIPS, voir [Federal Information Processing Standard \(FIPS\) 140-2](#).

h. Choisissez Suivant.

6. Dans Configurer les détails supplémentaires, procédez comme suit :

a. Pour la CloudWatch journalisation, choisissez l'une des options suivantes pour activer la CloudWatch journalisation de votre activité utilisateur par Amazon :

- Créez un nouveau rôle pour permettre à Transfer Family de le IAM créer automatiquement, à condition que vous disposiez des autorisations nécessaires pour créer un nouveau rôle. Le IAM rôle créé est appelé `AWSTransferLoggingAccess`.
- Choisissez un rôle existant pour choisir un IAM rôle existant dans votre compte. Sous Rôle de journalisation, choisissez le rôle. Ce IAM rôle doit inclure une politique de confiance avec le service défini sur `transfer.amazonaws.com`.

Pour plus d'informations sur la CloudWatch journalisation, consultez [Configurer le rôle de CloudWatch journalisation](#).

 Note

- Vous ne pouvez pas consulter l'activité de l'utilisateur final CloudWatch si vous ne spécifiez pas de rôle de journalisation.
- Si vous ne souhaitez pas configurer de rôle de CloudWatch journalisation, sélectionnez Choisir un rôle existant, mais ne sélectionnez pas de rôle de journalisation.

b. Pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur.

 Note

Par défaut, la politique `TransferSecurityPolicy-2020-06` de sécurité est attachée à votre serveur, sauf si vous en choisissez une autre.

Pour plus d'informations sur les stratégies de sécurité, consultez [Politiques de sécurité pour AWS Transfer Family](#).

- c. (Facultatif) Pour la clé d'hôte du serveur RSAED25519, entrez une clé ECDSA privée ou une clé privée qui sera utilisée pour identifier votre serveur lorsque les clients s'y connecteront SFTP.

Note

Cette section concerne uniquement la migration des utilisateurs depuis un serveur SFTP compatible existant.

- d. (Facultatif) Pour les balises, pour la clé et la valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
- e. Choisissez Suivant.
- f. (Facultatif) Pour les flux de travail gérés, choisissez le flux de travail IDs (et le rôle correspondant) que Transfer Family doit assumer lors de l'exécution du flux de travail. Vous pouvez choisir un flux de travail à exécuter lors d'un téléchargement complet et un autre à exécuter lors d'un téléchargement partiel. Pour en savoir plus sur le traitement de vos fichiers à l'aide de flux de travail gérés, consultez [AWS Transfer Family flux de travail gérés](#).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

- 7. Dans Réviser et créer, passez en revue vos choix. Si vous :
 - Si vous souhaitez modifier l'un d'entre eux, choisissez Modifier à côté de l'étape.

 Note

Vous devrez passer en revue chaque étape après celle que vous avez choisi de modifier.

- Si aucune modification n'est apportée, choisissez **Create server** pour créer votre serveur. Vous êtes dirigé vers la page **Servers (Serveurs)**, représentée ci-dessous, dans laquelle figure votre nouveau serveur.

Vous pouvez choisir l'ID du serveur pour voir les paramètres détaillés du serveur que vous venez de créer. Une fois que la colonne **IPv4Adresse publique** a été renseignée, les adresses IP élastiques que vous avez fournies sont correctement associées au point de terminaison de votre serveur.

 Note

Lorsque votre serveur VPC est en ligne, seuls les sous-réseaux peuvent être modifiés et uniquement via le [UpdateServer](#) API. Vous devez [arrêter le serveur](#) pour ajouter ou modifier les adresses IP élastiques du point de terminaison du serveur.

Modifier le type de point de terminaison de votre serveur

Si vous disposez d'un serveur existant accessible via Internet (c'est-à-dire doté d'un type de point de terminaison public), vous pouvez remplacer son point de terminaison par un point de VPC terminaison.

 Note

Si vous avez un serveur existant dans un format VPC affiché sous **VPC_ENDPOINT**, nous vous recommandons de le modifier pour le nouveau type de point de VPC terminaison. Avec ce nouveau type de point de terminaison, vous n'avez plus besoin d'utiliser un Network Load Balancer (NLB) pour associer des adresses IP élastiques au point de terminaison de votre serveur. Vous pouvez également utiliser des groupes VPC de sécurité pour restreindre l'accès au point de terminaison de votre serveur. Toutefois, vous pouvez continuer à utiliser le type de **VPC_ENDPOINT** point de terminaison selon vos besoins.

La procédure suivante suppose que vous disposez d'un serveur qui utilise soit le type de point de terminaison public actuel, soit l'ancien VPC_ENDPOINT type.

Pour modifier le type de point de terminaison de votre serveur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, choisissez Servers (Serveurs).
3. Cochez la case du serveur dont vous souhaitez modifier le type de point de terminaison.

 Important

Vous devez arrêter le serveur avant de pouvoir modifier son point de terminaison.

4. Pour Actions, choisissez Arrêter.
5. Dans la boîte de dialogue de confirmation qui apparaît, choisissez Stop pour confirmer que vous souhaitez arrêter le serveur.

 Note

Avant de passer à l'étape suivante, dans Détails du point de terminaison, attendez que le statut du serveur passe à Hors ligne ; cela peut prendre quelques minutes. Vous devrez peut-être sélectionner Actualiser sur la page Serveurs pour voir le changement d'état. Vous ne pourrez apporter aucune modification tant que le serveur ne sera pas hors ligne.

6. Dans Détails du point de terminaison, choisissez Modifier.
7. Dans Modifier la configuration du point de terminaison, procédez comme suit :
 - a. Pour Modifier le type de point de terminaison, choisissez VPChébergé.
 - b. Pour Access, choisissez l'une des options suivantes :
 - Interne pour que votre terminal ne soit accessible qu'aux clients utilisant les adresses IP privées du point de terminaison.
 - Internet Facing pour rendre votre terminal accessible aux clients via Internet public.

 Note

Lorsque vous choisissez Internet Facing, vous pouvez choisir une adresse IP élastique existante dans chaque sous-réseau ou sous-réseaux. Vous pouvez

également accéder à la VPC console (<https://console.aws.amazon.com/vpc/>) pour allouer une ou plusieurs nouvelles adresses IP élastiques. Ces adresses peuvent être détenues par vous AWS ou par vous. Vous ne pouvez pas associer les adresses IP élastiques déjà utilisées à votre point de terminaison.

c. (Facultatif pour l'accès à Internet uniquement) Pour le nom d'hôte personnalisé, choisissez l'une des options suivantes :

- DNSAlias Amazon Route 53 : si le nom d'hôte que vous souhaitez utiliser est enregistré auprès de Route 53. Vous pouvez ensuite saisir le nom d'hôte.
- Autre DNS : si le nom d'hôte que vous souhaitez utiliser est enregistré auprès d'un autre DNS fournisseur. Vous pouvez ensuite saisir le nom d'hôte.
- Aucun : pour utiliser le point de terminaison du serveur et ne pas utiliser de nom d'hôte personnalisé. Le nom d'hôte du serveur se présente sous la forme `serverId.server.transfer.regionId.amazonaws.com`.

Pour en savoir plus sur l'utilisation de noms d'hôtes personnalisés, consultez [Utilisation de noms d'hôtes personnalisés](#).

- d. Pour VPC, choisissez un VPC identifiant existant ou choisissez Créer un VPC pour en créer un nouveau VPC.
- e. Dans la section Zones de disponibilité, sélectionnez jusqu'à trois zones de disponibilité et les sous-réseaux associés. Si Internet Facing est sélectionné, choisissez également une adresse IP élastique pour chaque sous-réseau.

 Note

Si vous souhaitez un maximum de trois zones de disponibilité, mais qu'il n'y en a pas suffisamment, créez-les dans la VPC console (<https://console.aws.amazon.com/vpc/>).

Si vous modifiez les sous-réseaux ou les adresses IP élastiques, la mise à jour du serveur prend quelques minutes. Vous ne pouvez pas enregistrer vos modifications tant que la mise à jour du serveur n'est pas terminée.

f. Choisissez Save (Enregistrer).

8. Pour Actions, choisissez Démarrer et attendez que le statut du serveur passe à En ligne ; cela peut prendre quelques minutes.

 Note

Si vous avez remplacé un type de point de terminaison public par un type de VPC point de terminaison, notez que le type de point de terminaison de votre serveur est devenu VPC.

Le groupe de sécurité par défaut est attaché au point de terminaison. Pour modifier ou ajouter des groupes de sécurité supplémentaires, consultez la section [Création de groupes de sécurité](#).

Cessation de l'utilisation de _ VPC ENDPOINT

AWS Transfer Family supprime la possibilité de créer des serveurs `EndpointType=VPC_ENDPOINT` pour les nouveaux AWS comptes. À compter du 19 mai 2021, les AWS comptes qui ne possèdent pas de AWS Transfer Family serveurs dotés d'un type de point de terminaison ne `VPC_ENDPOINT` pourront pas créer de nouveaux serveurs avec `EndpointType=VPC_ENDPOINT`. Si vous possédez déjà des serveurs qui utilisent le type de `VPC_ENDPOINT` point de terminaison, nous vous recommandons de commencer à `EndpointType=VPC` les utiliser dès que possible. Pour plus de détails, voir [Mettre à jour le type de point de terminaison de votre AWS Transfer Family serveur de VPC _ ENDPOINT à VPC](#).

Nous avons lancé le nouveau type de VPC point de terminaison plus tôt en 2020. Pour plus d'informations, consultez la section [AWS Transfer Family relative aux groupes VPC de sécurité et aux adresses IP élastiques pris en SFTP charge](#). Ce nouveau point de terminaison est plus riche en fonctionnalités et plus rentable, et il est PrivateLink gratuit. Pour plus d'informations, consultez [AWS PrivateLink les tarifs](#).

Ce type de point de terminaison est fonctionnellement équivalent au type de point de terminaison précédent (`VPC_ENDPOINT`). Vous pouvez associer des adresses IP élastiques directement au point de terminaison pour le rendre accessible à Internet et utiliser des groupes de sécurité pour le filtrage des adresses IP source. Pour plus d'informations, consultez le billet de blog [intitulé Utiliser une adresse IP AWS Transfer Family autorisée pour sécuriser votre SFTP serveur](#).

Vous pouvez également héberger ce point de terminaison dans un VPC environnement partagé. Pour plus d'informations, voir [Supporte AWS Transfer Family désormais les VPC environnements de services partagés](#).

En outre SFTP, vous pouvez utiliser le VPC EndpointType pour activer FTPS et FTP. Nous n'avons pas l'intention d'ajouter ces fonctionnalités FTPS et/ou le FTP support à EndpointType=VPC_ENDPOINT. Nous avons également supprimé ce type de point de terminaison en tant qu'option de la AWS Transfer Family console.

Vous pouvez modifier le type de point de terminaison de votre serveur à l'aide de la console Transfer Family AWS CLI API, SDKs,, ou AWS CloudFormation. Pour modifier le type de point de terminaison de votre serveur, consultez [Mise à jour du type de point de terminaison du AWS Transfer Family serveur de VPC _ ENDPOINT à VPC](#).

Si vous avez des questions, contactez AWS Support l'équipe chargée de votre AWS compte.

 Note

Nous ne prévoyons pas d'ajouter ces fonctionnalités FTPS et/ou le FTP support à EndpointType = VPC_ENDPOINT. Nous ne le proposons plus en option sur la AWS Transfer Family console.

Si vous avez d'autres questions, vous pouvez nous contacter par l'intermédiaire AWS Support de l'équipe chargée de votre compte.

Mise à jour du type de point de terminaison du AWS Transfer Family serveur de VPC _ ENDPOINT à VPC

Vous pouvez utiliser le AWS Management Console AWS CloudFormation, ou le Transfer Family API pour mettre à jour le nom EndpointType d'un serveur VPC_ENDPOINT vers VPC. Des procédures détaillées et des exemples d'utilisation de chacune de ces méthodes pour mettre à jour un type de point de terminaison de serveur sont fournis dans les sections suivantes. Si vous avez des serveurs dans plusieurs AWS régions et sur plusieurs AWS comptes, vous pouvez utiliser l'exemple de script fourni dans la section suivante, avec des modifications, pour identifier les serveurs en utilisant le VPC_ENDPOINT type que vous devrez mettre à jour.

Rubriques

- [Identifier les serveurs à l'aide du type de VPC_ENDPOINT point de terminaison](#)
- [Mise à jour du type de point de terminaison du serveur à l'aide AWS Management Console](#)
- [Mise à jour du type de point de terminaison du serveur avec AWS CloudFormation](#)

- [Mettre à jour le serveur EndpointType à l'aide du API](#)

Identifier les serveurs à l'aide du type de **VPC_ENDPOINT** point de terminaison

Vous pouvez identifier les serveurs qui VPC_ENDPOINT utilisent le AWS Management Console.

Pour identifier les serveurs utilisant le type de **VPC_ENDPOINT** point de terminaison à l'aide de la console

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Choisissez Servers dans le volet de navigation pour afficher la liste des serveurs de votre compte dans cette région.
3. Triez la liste des serveurs par type de point de terminaison pour voir tous les serveurs utilisés VPC_ENDPOINT.

Pour identifier les serveurs utilisés **VPC_ENDPOINT** dans plusieurs AWS régions et comptes

Si vous avez des serveurs dans plusieurs AWS régions et dans plusieurs AWS comptes, vous pouvez utiliser l'exemple de script suivant, avec des modifications, pour identifier les serveurs à l'aide du type de point de VPC_ENDPOINT terminaison. L'exemple de script utilise les [ListServers](#) API appels Amazon EC2 [DescribeRegions](#) et Transfer Family pour obtenir une liste du serveur IDs et des régions de tous les serveurs que vous utilisez VPC_ENDPOINT. Si vous avez de nombreux AWS comptes, vous pouvez les parcourir en utilisant un IAM rôle avec accès auditeur en lecture seule si vous vous authentifiez à l'aide de profils de session auprès de votre fournisseur d'identité.

1. Voici un exemple simple.

```
import boto3

profile = input("Enter the name of the AWS account you'll be working in: ")
session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2")

regions = ec2.describe_regions()

for region in regions['Regions']:
    region_name = region['RegionName']
    if region_name=='ap-northeast-3': #https://github.com/boto/boto3/issues/1943
```

```
continue
transfer = session.client("transfer", region_name=region_name)
servers = transfer.list_servers()
for server in servers['Servers']:
    if server['EndpointType']=='VPC_ENDPOINT':
        print(server['ServerId'], region_name)
```

2. Une fois que vous avez la liste des serveurs à mettre à jour, vous pouvez utiliser l'une des méthodes décrites dans les sections suivantes pour mettre à jour le EndpointType versVPC.

Mise à jour du type de point de terminaison du serveur à l'aide AWS Management Console

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, choisissez Servers (Serveurs).
3. Cochez la case du serveur dont vous souhaitez modifier le type de point de terminaison.

Important

Vous devez arrêter le serveur avant de pouvoir modifier son point de terminaison.

4. Pour Actions, choisissez Arrêter.
5. Dans la boîte de dialogue de confirmation qui apparaît, choisissez Stop pour confirmer que vous souhaitez arrêter le serveur.

Note

Avant de passer à l'étape suivante, attendez que le statut du serveur passe à Hors ligne ; cela peut prendre quelques minutes. Vous devrez peut-être sélectionner Actualiser sur la page Serveurs pour voir le changement d'état.

6. Lorsque le statut passe à Hors ligne, choisissez le serveur pour afficher la page de détails du serveur.
7. Dans la section Détails du point de terminaison, choisissez Modifier.
8. Choisissez VPChébergé pour le type de point de terminaison.
9. Choisissez Enregistrer.
10. Pour Actions, choisissez Démarrer et attendez que le statut du serveur passe à En ligne ; cela peut prendre quelques minutes.

Mise à jour du type de point de terminaison du serveur avec AWS CloudFormation

Cette section décrit comment procéder pour mettre AWS CloudFormation à jour celui d'un serveur EndpointType versVPC. Utilisez cette procédure pour les serveurs Transfer Family que vous avez déployés avec AWS CloudFormation. Dans cet exemple, le AWS CloudFormation modèle d'origine utilisé pour déployer le serveur Transfer Family est présenté comme suit :

```
AWS::TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC_ENDPOINT endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        VpcEndpointId: !Ref VPCEndpoint
      EndpointType: VPC_ENDPOINT
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
  VPCEndpoint:
    Type: AWS::EC2::VPCEndpoint
    Properties:
      ServiceName: com.amazonaws.us-east-1.transfer.server
      SecurityGroupIds:
        - !Ref SecurityGroupId
      SubnetIds:
        - !Select [0, !Ref SubnetIds]
        - !Select [1, !Ref SubnetIds]
        - !Select [2, !Ref SubnetIds]
      VpcEndpointType: Interface
      VpcId: !Ref VpcId
```

Le modèle est mis à jour avec les modifications suivantes :

- Le EndpointType a été changé enVPC.

- La `AWS::EC2::VPCEndpoint` ressource est supprimée.
- Les `SecurityGroupIdSubnetIds`, et `VpcId` ont été déplacés vers la `EndpointDetails` section de la `AWS::Transfer::Server` ressource,
- La `VpcEndpointId` propriété de `EndpointDetails` a été supprimée.

Le modèle mis à jour se présente comme suit :

```
AWS TemplateFormatVersion: '2010-09-09'
Description: 'Create AWS Transfer Server with VPC endpoint type'
Parameters:
  SecurityGroupId:
    Type: AWS::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
  VpcId:
    Type: AWS::EC2::VPC::Id
Resources:
  TransferServer:
    Type: AWS::Transfer::Server
    Properties:
      Domain: S3
      EndpointDetails:
        SecurityGroupIds:
          - !Ref SecurityGroupId
        SubnetIds:
          - !Select [0, !Ref SubnetIds]
          - !Select [1, !Ref SubnetIds]
          - !Select [2, !Ref SubnetIds]
        VpcId: !Ref VpcId
      EndpointType: VPC
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
```

Pour mettre à jour le type de point de terminaison des serveurs Transfer Family déployés à l'aide de AWS CloudFormation

1. Arrêtez le serveur que vous souhaitez mettre à jour en procédant comme suit.
 - a. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.

- b. Dans le volet de navigation, choisissez Servers (Serveurs).
- c. Cochez la case du serveur dont vous souhaitez modifier le type de point de terminaison.

 Important

Vous devez arrêter le serveur avant de pouvoir modifier son point de terminaison.

- d. Pour Actions, choisissez Arrêter.
- e. Dans la boîte de dialogue de confirmation qui apparaît, choisissez Stop pour confirmer que vous souhaitez arrêter le serveur.

 Note

Avant de passer à l'étape suivante, attendez que le statut du serveur passe à Hors ligne ; cela peut prendre quelques minutes. Vous devrez peut-être sélectionner Actualiser sur la page Serveurs pour voir le changement d'état.

2. Mettre à jour la CloudFormation pile

- a. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
- b. Choisissez la pile utilisée pour créer le serveur Transfer Family.
- c. Choisissez Mettre à jour.
- d. Choisissez Remplacer le modèle actuel
- e. Téléchargez le nouveau modèle. CloudFormation Les ensembles de modifications vous aident à comprendre comment les modifications apportées aux modèles affecteront les ressources en cours d'exécution avant de les implémenter. Dans cet exemple, la ressource du serveur de transfert sera modifiée et supprimée. VPCEndpoint Le serveur de type de VPC point de VPC terminaison crée un point de terminaison en votre nom, en remplacement de la VPCEndpoint ressource d'origine.

Après avoir chargé le nouveau modèle, l'ensemble de modifications ressemblera à ce qui suit :

Change set preview				
Changes (2)				
Search changes				
Action	Logical ID	Physical ID	Resource type	Replacement
Modify	TransferServer	arn:aws:transfer:us-east-1:364810874344:server/s-6a7d04e12d494ec98	AWS::Transfer::Server	Conditional
Remove	VPCEndpoint	vpce-04e685f8702849573 ↗	AWS::EC2::VPCEndpoint	-

- f. Mettez à jour la pile.
3. Une fois la mise à jour de la pile terminée, accédez à la console de gestion Transfer Family à l'adresse <https://console.aws.amazon.com/transfer/>.
4. Redémarrez le serveur. Choisissez le serveur sur lequel vous avez effectué la mise à jour AWS CloudFormation, puis sélectionnez Démarrer dans le menu Actions.

Mettre à jour le serveur EndpointType à l'aide du API

Vous pouvez utiliser la commande [describe-server](#) ou la AWS CLI [UpdateServer](#) API commande. L'exemple de script suivant arrête le serveur Transfer Family, met à jour le EndpointType, supprime le VPC _ ENDPOINT et démarre le serveur.

```
import boto3
import time

profile = input("Enter the name of the AWS account you'll be working in: ")
region_name = input("Enter the AWS Region you're working in: ")
server_id = input("Enter the AWS Transfer Server Id: ")

session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2", region_name=region_name)
transfer = session.client("transfer", region_name=region_name)

group_ids=[]

transfer_description = transfer.describe_server(ServerId=server_id)
```



```

if transfer_description['Server']['EndpointType']=='VPC_ENDPOINT':
    transfer_vpc_endpoint = transfer_description['Server']['EndpointDetails']
['VpcEndpointId']
    transfer_vpc_endpoint_descriptions =
ec2.describe_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
    for transfer_vpc_endpoint_description in
transfer_vpc_endpoint_descriptions['VpcEndpoints']:
        subnet_ids=transfer_vpc_endpoint_description['SubnetIds']
        group_id_list=transfer_vpc_endpoint_description['Groups']
        vpc_id=transfer_vpc_endpoint_description['VpcId']
        for group_id in group_id_list:
            group_ids.append(group_id['GroupId'])
    if transfer_description['Server']['State']=='ONLINE':
        transfer_stop = transfer.stop_server(ServerId=server_id)
        print(transfer_stop)
        time.sleep(300) #safe
        transfer_update =
transfer.update_server(ServerId=server_id,EndpointType='VPC',EndpointDetails={'SecurityGroupId
        print(transfer_update)
        time.sleep(10)
        transfer_start = transfer.start_server(ServerId=server_id)
        print(transfer_start)
        delete_vpc_endpoint =
ec2.delete_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])

```

Utilisation de noms d'hôtes personnalisés

Le nom d'hôte de votre serveur est le nom d'hôte que vos utilisateurs saisissent dans leurs clients lorsqu'ils se connectent à votre serveur. Vous pouvez utiliser un domaine personnalisé que vous avez enregistré pour le nom d'hôte de votre serveur lorsque vous travaillez avec AWS Transfer Family. Par exemple, vous pouvez utiliser un nom d'hôte personnalisé tel `quemysftpservers.mysubdomain.domain.com`.

Pour rediriger le trafic de votre domaine personnalisé enregistré vers le point de terminaison de votre serveur, vous pouvez utiliser Amazon Route 53 ou n'importe quel fournisseur de système de noms de domaine (DNS). Route 53 est le DNS service qui prend en charge AWS Transfer Family nativement.

Rubriques

- [Utilisez Amazon Route 53 comme DNS fournisseur](#)
- [Utiliser d'autres DNS fournisseurs](#)
- [Noms d'hôte personnalisés pour les serveurs créés sans console](#)

Sur la console, vous pouvez choisir l'une des options suivantes pour configurer un nom d'hôte personnalisé :

- **DNSAlias Amazon Route 53** : si le nom d'hôte que vous souhaitez utiliser est enregistré auprès de Route 53. Vous pouvez ensuite saisir le nom d'hôte.
- **Autre DNS** : si le nom d'hôte que vous souhaitez utiliser est enregistré auprès d'un autre DNS fournisseur. Vous pouvez ensuite saisir le nom d'hôte.
- **Aucun** : pour utiliser le point de terminaison du serveur et ne pas utiliser de nom d'hôte personnalisé.

Vous définissez cette option lorsque vous créez un nouveau serveur ou que vous modifiez la configuration d'un serveur existant. Pour plus d'informations sur la création d'un nouveau serveur, consultez [Étape 2 : Création d'un SFTP serveur compatible](#). Pour plus d'informations sur la modification de la configuration d'un serveur existant, consultez [Modifier les détails du serveur](#).

Pour plus de détails sur l'utilisation de votre propre domaine comme nom d'hôte du serveur et sur l'AWS Transfer Family utilisation de Route 53, consultez les sections suivantes.

Utilisez Amazon Route 53 comme DNS fournisseur

Lorsque vous créez un serveur, vous pouvez utiliser Amazon Route 53 comme DNS fournisseur. Avant d'utiliser un domaine avec Route 53, vous devez enregistrer le domaine. Pour plus d'informations, consultez [Comment fonctionne l'enregistrement de domaines](#) dans le manuel Amazon Route 53 Developer Guide.

Lorsque vous utilisez Route 53 pour fournir le DNS routage à votre serveur, AWS Transfer Family utilise le nom d'hôte personnalisé que vous avez saisi pour extraire sa zone hébergée. Lors de l'extraction d'une zone hébergée, trois choses peuvent se produire :

1. Si vous utilisez Route 53 pour la première fois et que vous n'avez pas de zone hébergée AWS Transfer Family , ajoutez une nouvelle zone hébergée et un CNAME enregistrement. La valeur de cet CNAME enregistrement est le nom d'hôte du point de terminaison de votre serveur. A CNAMEest un nom de domaine alternatif.
2. Si vous avez une zone hébergée dans Route 53 sans aucun CNAME enregistrement, AWS Transfer Family ajoute un CNAME enregistrement à la zone hébergée.
3. Si le service détecte qu'il existe déjà un enregistrement CNAME dans la zone hébergée, vous obtenez une erreur indiquant qu'il existe déjà un enregistrement CNAME. Dans ce cas, remplacez la valeur de l'CNAMEenregistrement par le nom d'hôte de votre serveur.

 Note

Si cette étape fait partie d'un flux de travail de création de serveur, votre serveur est créé avec succès et votre nom d'hôte personnalisé est défini sur Aucun.

Pour plus d'informations sur les zones hébergées dans Route 53, consultez la section [Zone hébergée](#) dans le manuel Amazon Route 53 Developer Guide.

Utiliser d'autres DNS fournisseurs

Lorsque vous créez un serveur, vous pouvez également utiliser des DNS fournisseurs autres qu'Amazon Route 53. Si vous utilisez un autre DNS fournisseur, assurez-vous que le trafic provenant de votre domaine est dirigé vers le point de terminaison de votre serveur.

Pour ce faire, définissez votre domaine sur le nom d'hôte du point de terminaison du serveur. Le nom d'hôte d'un point de terminaison ressemble à ceci dans la console :

`serverid.server.transfer.region.amazonaws.com`

 Note

Si votre serveur possède un VPC point de terminaison, le format du nom d'hôte est différent de celui décrit ci-dessus. Pour trouver votre VPC point de terminaison, sélectionnez-le VPC sur la page de détails du serveur, puis sélectionnez l'ID du VPC point de terminaison sur le VPC tableau de bord. Le point de terminaison est le DNS prénom des personnes répertoriées.

Noms d'hôte personnalisés pour les serveurs créés sans console

Lorsque vous créez un serveur en utilisant AWS Cloud Development Kit (AWS CDK) ou via le CLI, vous devez ajouter une balise si vous souhaitez que ce serveur possède un nom d'hôte personnalisé. AWS CloudFormation Lorsque vous créez un serveur Transfer Family à l'aide de la console, le balisage est effectué automatiquement.

 Note

Vous devez également créer un DNS enregistrement pour rediriger le trafic de votre domaine vers le point de terminaison de votre serveur. Pour plus de détails, consultez la section [Travailler avec des enregistrements](#) dans le guide du développeur Amazon Route 53.

Utilisez les clés suivantes pour votre nom d'hôte personnalisé :

- Ajoutez `transfer:customHostname` pour afficher le nom d'hôte personnalisé dans la console.
- Si vous utilisez Route 53 comme DNS fournisseur, ajoutez `transfer:route53HostedZoneId`. Cette balise lie le nom d'hôte personnalisé à votre ID de zone hébergée Route 53.

Pour ajouter le nom d'hôte personnalisé, exécutez la CLI commande suivante.

```
aws transfer tag-resource --arn arn:aws:transfer:region:Compte AWS:server/server-ID --tags Key=transfer:customHostname,Value="custom-host-name"
```

Par exemple :

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

Si vous utilisez Route 53, exécutez la commande suivante pour lier votre nom d'hôte personnalisé à votre ID de zone hébergée Route 53.

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

Par exemple :

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

En utilisant les valeurs d'exemple de la commande précédente, exécutez la commande suivante pour afficher vos balises :

```
aws transfer list-tags-for-resource --arn arn:aws:transfer:us-east-1:111122223333:server/s-1234567890abcdef0
```

```
"Tags": [  
  {  
    "Key": "transfer:route53HostedZoneId",  
    "Value": "/hostedzone/ABCDE1111222233334444"  
  },  
  {  
    "Key": "transfer:customHostname",  
    "Value": "abc.example.com"  
  }  
]
```

Note

Vos zones hébergées publiques et IDs les leurs sont disponibles sur Amazon Route 53. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/route53/>.

Transfert de fichiers via un point de terminaison serveur à l'aide d'un client

Vous transférez des fichiers via le AWS Transfer Family service en spécifiant l'opération de transfert dans un client. AWS Transfer Family prend en charge les clients suivants :

- Nous prenons en charge la version 3 du SFTP protocole.
- Ouvrir SSH (macOS et Linux)

Note

Ce client fonctionne uniquement avec les serveurs activés pour le protocole de transfert de fichiers Secure Shell (SSH) (SFTP).

- Win SCP (Microsoft Windows uniquement)
- Cyberduck (Windows, macOS et Linux)

- FileZilla (Windows, macOS et Linux)

Les restrictions suivantes s'appliquent à tous les clients :

- Le nombre maximum de SFTP sessions multiplexées simultanées par connexion est de 10.
- Amazon S3 et Amazon EFS (en raison du NFSv4 protocole) nécessitent que les noms de fichiers soient encodés en UTF -8. L'utilisation d'un encodage différent peut entraîner des résultats inattendus. Pour Amazon S3, consultez les [directives de dénomination des clés d'objet](#).
- Pour le protocole de transfert de fichiers sur SSL (FTPS), seul le mode explicite est pris en charge. Le mode implicite n'est pas pris en charge.
- Pour les protocoles de transfert de fichiers (FTP) et FTPS, seul le mode passif est pris en charge.
- Pour FTP et FTPS, seul le STREAM mode est pris en charge.
- Pour FTP et FTPS, seul le mode image/binaire est pris en charge.
- Pour FTP et FTPS, TLS - PROT C (non protégé) TLS pour la connexion de données est la valeur par défaut, mais PROT C n'est pas pris en charge dans le AWS Transfer Family FTPS protocole. Donc FTPS, vous devez émettre PROT P pour que votre opération de données soit acceptée.
- Si vous utilisez Amazon S3 pour le stockage de votre serveur, et si votre client contient une option permettant d'utiliser plusieurs connexions pour un seul transfert, assurez-vous de désactiver cette option. Dans le cas contraire, les téléchargements de fichiers volumineux peuvent échouer de manière imprévisible. Notez que si vous utilisez Amazon EFS comme backend de stockage, EFS il prend en charge plusieurs connexions pour un seul transfert.

Voici une liste des commandes disponibles pour FTP et FTPS :

Commandes disponibles					
ABOR	FEAT	MLST	PASS	RETR	STOR
AUTH	LANG	MKD	PASV	RMD	STOU
CDUP	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	SYST
DELE	MFMT	NOOP	PWD	SIZE	TYPE

Commandes disponibles					
EPSV	MLSD	OPTS	QUIT	STAT	USER

 Note

APPE n'est pas pris en charge.

En SFTP effet, les opérations suivantes ne sont actuellement pas prises en charge pour les utilisateurs utilisant le répertoire de base logique sur des serveurs utilisant Amazon Elastic File System (AmazonEFS).

Commandes non prises en charge SFTP			
SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT lorsque le fichier demandé est un lien symbolique	SSH_FXP_ REALPATH lorsque le chemin demandé contient des composants de lien symbolique

Générer une paire de clés publique-privée

Avant de transférer un fichier, vous devez disposer d'une paire de clés publique-privée. Si vous n'avez pas encore généré de paire de clés, consultez [Génération de SSH clés pour les utilisateurs gérés par des services](#).

Rubriques

- [SFTP/FTPS/FTP Commandes disponibles](#)
- [Trouvez votre point de VPC terminaison Amazon](#)
- [Évitez les setstat erreurs](#)
- [Utiliser Open SSH](#)
- [Utilisez Win SCP](#)
- [Utilisez Cyberduck](#)

- [Utiliser FileZilla](#)
- [Utiliser un client Perl](#)
- [Traitement après le téléchargement](#)

SFTP/FTPS/FTP Commandes disponibles

Le tableau suivant décrit les commandes disponibles pour AWS Transfer Family, pour les SFTP FTP protocoles et. FTPS

Note

Le tableau mentionne les fichiers et les répertoires d'Amazon S3, qui ne prend en charge que les buckets et les objets : il n'y a pas de hiérarchie. Cependant, vous pouvez utiliser des préfixes dans les noms de clés d'objets pour indiquer une hiérarchie et organiser vos données de la même manière que les dossiers. Ce comportement est décrit dans la section [Utilisation des métadonnées d'objets](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

SFTP/FTPS/FTP Commandes

Command	Amazon S3	Amazon EFS
cd	Pris en charge	Pris en charge
chgrp	Non pris en charge	Supporté (root ou owner uniquement)
chmod	Non pris en charge	Supporté (root uniquement)
chmtime	Non pris en charge	Pris en charge
chown	Non pris en charge	Supporté (root uniquement)
get	Pris en charge	Supporté (y compris la résolution de liens symboliques)
ln -s	Non pris en charge	Pris en charge

Command	Amazon S3	Amazon EFS
<code>ls/dir</code>	Pris en charge	Pris en charge
<code>mkdir</code>	Pris en charge	Pris en charge
<code>put</code>	Pris en charge	Pris en charge
<code>pwd</code>	Pris en charge	Pris en charge
<code>rename</code>	Pris en charge uniquement pour les fichiers	Pris en charge  Note Le changement de nom qui remplacerait un fichier ou un répertoire existant n'est pas pris en charge.
<code>rm</code>	Pris en charge	Pris en charge
<code>rmdir</code>	Pris en charge (répertoires vides uniquement)	Pris en charge
<code>version</code>	Pris en charge	Pris en charge

Trouvez votre point de VPC terminaison Amazon

Si le type de point de terminaison de votre serveur Transfer Family est le suivant VPC, il n'est pas facile d'identifier le point de terminaison à utiliser pour le transfert de fichiers. Dans ce cas, suivez la procédure ci-dessous pour trouver votre point de VPC terminaison Amazon.

Trouvez votre point de VPC terminaison Amazon

1. Accédez à la page de détails de votre serveur.
2. Dans le volet des détails du point de terminaison, sélectionnez le VPC.

Endpoint details Edit

Status Online	Custom hostname -
Endpoint type VPC (vpce- [redacted])	Endpoint -
VPC vpc- [redacted]	Access Info Internal
FIPS Enabled No	

3. Dans le tableau de VPC bord Amazon, sélectionnez l'identifiant du VPC point de terminaison.
4. Dans la liste des DNSnoms, le point de terminaison de votre serveur est le premier répertorié.

VPC > Endpoints > vpce-[redacted]

vpce-[redacted] Actions ▼

Details

Endpoint ID vpce-[redacted]	Status Available	Creation time Monday, April 4, 2022 at 10:51:31 EDT	Endpoint type Interface
VPC ID vpc-515e1d14 (no-name-specified)	Status message -	Service name com.amazonaws.us-east-2.transfer.server.c-0002	Private DNS names enabled No
DNS record IP type ipv4	IP address type ipv4	DNS names vpce-[redacted] [redacted] [redacted].us-east-2 [redacted] [redacted] [redacted] [redacted].us-east-2	

Évitez les **setstat** erreurs

Certains clients de transfert de fichiers peuvent tenter de modifier les attributs des fichiers distants, notamment l'horodatage et les autorisations, à l'aide de commandes, par exemple SETSTAT lors du téléchargement du SFTP fichier. Cependant, ces commandes ne sont pas compatibles avec les systèmes de stockage d'objets, tels qu'Amazon S3. En raison de cette incompatibilité, les chargements de fichiers à partir de ces clients peuvent entraîner des erreurs, même si le fichier est correctement chargé.

- Lorsque vous appelez le `CreateServer` ou `UpdateServerAPI`, utilisez l'`ProtocolDetailOption SetStatOption` pour ignorer l'erreur générée lorsque le client tente de l'utiliser SETSTAT sur un fichier que vous téléchargez dans un compartiment S3.
- Définissez la valeur sur `ENABLE_NO_OP` pour que le serveur Transfer Family ignore la SETSTAT commande et télécharge les fichiers sans avoir à apporter de modifications à votre SFTP client.
- Notez que même si le `SetStatOption ENABLE_NO_OP` paramètre ignore l'erreur, il génère une entrée de journal dans CloudWatch Logs, afin que vous puissiez déterminer à quel moment le client passe un SETSTAT appel.

Pour API plus de détails sur cette option, consultez [ProtocolDetails](#).

Utiliser Open SSH

Suivez les instructions ci-dessous pour transférer des fichiers depuis la ligne de commande à l'aide d'OpenSSH.

Note

Ce client fonctionne uniquement avec un SFTP serveur activé.

Pour transférer des fichiers à l' AWS Transfer Family aide de l'utilitaire de ligne de SSH commande Open

1. Sur Linux, macOS ou Windows, ouvrez un terminal de commande.
2. À l'invite, entrez la commande suivante :

```
sftp -i transfer-key sftp_user@service_endpoint
```

Dans la commande précédente, *sftp_user* il s'agit du nom d'utilisateur et *transfer-key* de la clé SSH privée. *service_endpoint* Voici le point de terminaison du serveur tel qu'indiqué dans la AWS Transfer Family console du serveur sélectionné.

 Note

Cette commande utilise les paramètres figurant dans le `ssh_config` fichier par défaut. Sauf si vous avez déjà modifié ce fichier, il SFTP utilise le port 22. Vous pouvez spécifier un port différent (par exemple 2222) en ajoutant un `-P` drapeau à la commande, comme suit.

```
sftp -P 2222 -i transfer-key sftp_user@service_endpoint
```

Sinon, si vous souhaitez toujours utiliser le port 2222, vous pouvez mettre à jour votre port par défaut dans votre `ssh_config` fichier.

Une invite `sftp` doit s'afficher.

3. (Facultatif) Pour afficher le répertoire personnel de l'utilisateur, entrez la commande suivante à l'`sftp` invite :

```
pwd
```

4. Pour télécharger un fichier depuis votre système de fichiers vers le serveur Transfer Family, utilisez la `put` commande. Par exemple, pour charger `hello.txt` (en supposant que le fichier se trouve dans le répertoire actuel de votre système de fichiers), exécutez la commande suivante à l'`sftp` invite :

```
put hello.txt
```

Un message similaire au suivant apparaît, indiquant que le transfert du fichier est en cours ou terminé.

```
Uploading hello.txt to /my-bucket/home/sftp_user/hello.txt
```

```
hello.txt 100% 127 0.1KB/s 00:00
```

 Note

Une fois votre serveur créé, le nom d'hôte du point de terminaison du serveur peut prendre quelques minutes pour être résolu par le DNS service dans votre environnement.

Utilisez Win SCP

Suivez les instructions ci-dessous pour transférer des fichiers depuis la ligne de commande à l'aide de WinSCP.

 Note

Si vous utilisez Win SCP 5.19, vous pouvez vous connecter directement à Amazon S3 à l'aide de vos AWS informations d'identification et télécharger/télécharger des fichiers. Pour plus de détails, consultez [Connexion au service Amazon S3](#).

Pour transférer des fichiers à AWS Transfer Family l'aide de Win SCP

1. Ouvrez le SCP client Win.
2. Dans la boîte de dialogue de connexion, pour Protocole de fichier, choisissez un protocole : SFTP ou FTP.

Si vous avez choisi FTP, pour Chiffrement, choisissez l'une des options suivantes :

- Aucun cryptage pour FTP
 - TLS/Chiffrement SSL explicite pour FTPS
3. Dans Nom d'hôte, entrez le point de terminaison de votre serveur. Le point de terminaison du serveur se trouve sur la page des détails du serveur. Pour de plus amples informations, veuillez consulter [Afficher SFTP FTPS et détails FTP du serveur](#).

 Note

Si votre serveur utilise un VPC point de terminaison, consultez [Trouvez votre point de VPC terminaison Amazon](#).

4. Pour le numéro de port, entrez ce qui suit :

- **22** pour SFTP
 - **21** pour FTP/FTPS
5. Dans Nom d'utilisateur, entrez le nom de l'utilisateur que vous avez créé pour votre fournisseur d'identité spécifique.

 Note

Le nom d'utilisateur doit être l'un des utilisateurs que vous avez créés ou configurés pour votre fournisseur d'identité. AWS Transfer Family fournit les fournisseurs d'identité suivants :

- [Travailler avec des utilisateurs gérés par des services](#)
- [Utilisation du fournisseur d'identité du AWS Directory Service](#)
- [Travailler avec des fournisseurs d'identité personnalisés](#)

6. Choisissez Avancé pour ouvrir la boîte de dialogue Paramètres avancés du site. Dans la SSHsection, choisissez Authentification.
7. Pour le fichier de clé privée, recherchez et sélectionnez le fichier de clé SSH privée dans votre système de fichiers.

 Note

Si Win SCP propose de convertir votre clé SSH privée au PPK format, choisissez OK.

8. Choisissez OK pour revenir à la boîte de dialogue Login, puis choisissez Sauver.
9. Dans la boîte de dialogue Enregistrer la session en tant que site, cliquez sur OK pour terminer la configuration de votre connexion.
10. Dans la boîte de dialogue de connexion, choisissez Outils, puis Préférences.
11. Dans la boîte de dialogue Préférences, pour Transfer, choisissez Endurance.

Pour l'option Activer la reprise du transfert/le transfert vers un nom de fichier temporaire pour, choisissez Désactiver.

 Note

Si vous laissez cette option activée, cela augmente les coûts de téléchargement, diminuant ainsi considérablement les performances de téléchargement. Cela peut également entraîner l'échec des téléchargements de fichiers volumineux.

12. Pour Transférer, choisissez Background et décochez la case Utiliser plusieurs connexions pour un seul transfert.

 Note

Si vous laissez cette option sélectionnée, les téléchargements de fichiers volumineux peuvent échouer de manière imprévisible. Par exemple, des téléchargements partitionnés orphelins qui entraînent des frais Amazon S3 peuvent être créés. Une corruption silencieuse des données peut également se produire.

13. Effectuez le transfert de vos fichiers.

Vous pouvez utiliser drag-and-drop des méthodes pour copier des fichiers entre les fenêtres cible et source. Vous pouvez utiliser les icônes de la barre d'outils pour charger, télécharger, supprimer, modifier ou modifier les propriétés des fichiers dans WinSCP.

 Note

Cette remarque ne s'applique pas si vous utilisez Amazon EFS pour le stockage. Les commandes qui tentent de modifier les attributs des fichiers distants, y compris les horodatages, ne sont pas compatibles avec les systèmes de stockage d'objets tels qu'Amazon S3. Par conséquent, si vous utilisez Amazon S3 pour le stockage, veillez à désactiver les paramètres d' SCP horodatage de Win (ou à les utiliser `SetStatOption` comme décrit dans [Évitez les setstat erreurs](#)) avant d'effectuer des transferts de fichiers. Pour ce faire, dans la boîte de dialogue des paramètres de Win SCP Transfer, désactivez l'option Définir les autorisations de téléchargement et l'option Conserver l'horodatage commun.

Utilisez Cyberduck

Suivez les instructions ci-dessous pour transférer des fichiers depuis la ligne de commande en utilisant Cyberduck.

Pour transférer des fichiers à AWS Transfer Family l'aide de Cyberduck

1. Ouvrez le client [Cyberduck](#).
2. Choisissez Open Connection.
3. Dans la boîte de dialogue Ouvrir une connexion, choisissez un protocole : SFTP(Protocole de transfert de SSH fichiers), FTP- SSL (Explicit AUTHTLS) ou FTP(Protocole de transfert de fichiers).
4. Pour Serveur, entrez le point de terminaison de votre serveur. Le point de terminaison du serveur se trouve sur la page des détails du serveur. Pour de plus amples informations, veuillez consulter [Afficher SFTP FTPS et détails FTP du serveur](#).

Note

Si votre serveur utilise un VPC point de terminaison, consultez [Trouvez votre point de VPC terminaison Amazon](#).

5. Pour le numéro de port, entrez ce qui suit :
 - **22** pour SFTP
 - **21** pour FTP/FTPS
6. Dans Nom d'utilisateur, entrez le nom de l'utilisateur que vous avez créé dans [Gestion des utilisateurs pour les points de terminaison du serveur](#).
7. Si SFTP cette option est sélectionnée, choisissez ou entrez la clé SSH privée dans le champ Clé SSH privée.
8. Choisissez Se connecter.
9. Effectuez le transfert de vos fichiers.

Selon l'emplacement de vos fichiers, effectuez l'une des actions suivantes :

- Dans votre répertoire local (la source), choisissez les fichiers que vous souhaitez transférer, puis faites-les glisser dans le répertoire Amazon S3 (la cible).

- Dans le répertoire Amazon S3 (la source), choisissez les fichiers que vous souhaitez transférer, puis faites-les glisser dans votre répertoire local (la cible).

Utiliser FileZilla

Suivez les instructions ci-dessous pour transférer des fichiers à l'aide de FileZilla.

FileZilla Pour configurer un transfert de fichiers

1. Ouvrez le FileZilla client.
2. Choisissez Fichier, puis Gestionnaire de site.
3. Dans la boîte de dialogue Gestionnaire de sites, sélectionnez Nouveau site.
4. Dans l'onglet Général, pour Protocole, choisissez un protocole : SFTP ou FTP.

Si vous avez choisi FTP, pour Chiffrement, choisissez l'une des options suivantes :

- Utilisez uniquement le langage clair FTP (non sécurisé) — pour FTP
 - Utilisez un FTP over explicite, TLS si disponible, pour FTPS
5. Dans Nom d'hôte, entrez le protocole que vous utilisez, suivi du point de terminaison de votre serveur. Le point de terminaison du serveur se trouve sur la page des détails du serveur. Pour de plus amples informations, veuillez consulter [Afficher SFTP FTPS et détails FTP du serveur](#).

Note

Si votre serveur utilise un VPC point de terminaison, consultez [Trouvez votre point de VPC terminaison Amazon](#).

- Si vous utilisez SFTP, entrez : `sftp://hostname`
- Si vous utilisez FTPS, entrez : `ftps://hostname`

Assurez-vous de remplacer *hostname* avec le point de terminaison de votre serveur actuel.

6. Pour le numéro de port, entrez ce qui suit :
 - **22** pour SFTP
 - **21** pour FTP/FTPS

7. Si cette option SFTP est sélectionnée, pour Type d'ouverture de session, choisissez Fichier clé.

Pour Fichier clé, choisissez ou entrez la clé SSH privée.
8. Pour Utilisateur, entrez le nom de l'utilisateur que vous avez créé dans [Gestion des utilisateurs pour les points de terminaison du serveur](#).
9. Choisissez Se connecter.
10. Effectuez le transfert de vos fichiers.

Note

Si vous interrompez un transfert de fichier en cours, vous AWS Transfer Family pouvez écrire un objet partiel dans votre compartiment Amazon S3. Si vous interrompez un chargement, vérifiez que la taille du fichier dans le compartiment Amazon S3 correspond à celle de l'objet source avant de continuer.

Utiliser un client Perl

Si vous utilisez le client `Net::SFTP::Foreign` Perl, vous devez définir la valeur `surqueue_size`. 1 Par exemple :

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

Note

Cette solution de contournement est nécessaire pour les révisions `Net::SFTP::Foreign` antérieures à la version [1.92.02](#).

Traitement après le téléchargement

Vous pouvez consulter les informations de traitement après le téléchargement, notamment les métadonnées des objets Amazon S3 et les notifications d'événements.

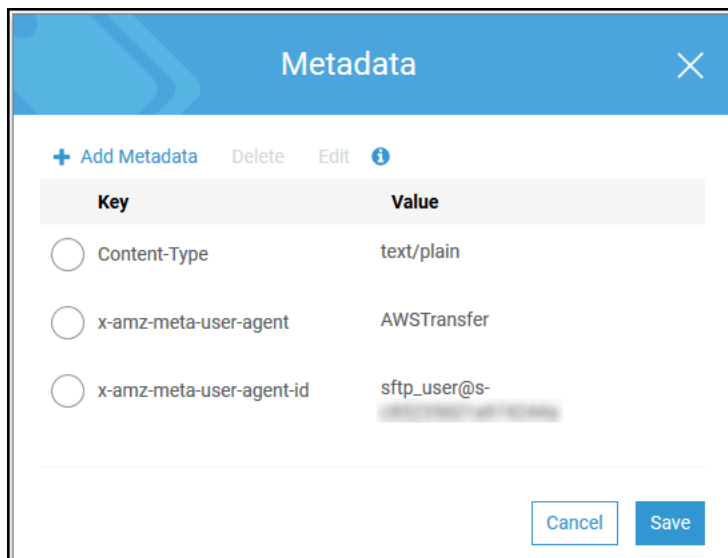
Rubriques

- [Métadonnées d'objets Amazon S3](#)

- [Notifications d'événements Amazon S3](#)

Métadonnées d'objets Amazon S3

Dans les métadonnées de votre objet, vous pouvez voir une clé appelée `x-amz-meta-user-agent` dont la valeur est `AWSTransfer` et `x-amz-meta-user-agent-id` dont la valeur est `username@server-id`. `username` s'agit de l'utilisateur de Transfer Family qui a chargé `server-id` le fichier et du serveur utilisé pour le téléchargement. Ces informations sont accessibles à l'aide de l'[HeadObject](#) opération sur l'objet S3 dans votre fonction Lambda.



Notifications d'événements Amazon S3

Lorsqu'un objet est chargé dans votre compartiment S3 à l'aide de Transfer Family, `RoleSessionName` il est contenu dans le champ `Requester` de la [structure de notification des événements S3 sous la](#) forme `[AWS:Role Unique Identifier]/username.sessionid@server-id`. Par exemple, voici le contenu d'un exemple de champ `Demandeur` issu d'un journal d'accès S3 pour un fichier copié dans le compartiment S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

Dans le champ `Demandeur` ci-dessus, il indique le IAM rôle appelé `IamRoleName`. Pour plus d'informations sur la configuration des notifications d'événements S3, consultez [la section Configuration des notifications d'événements Amazon S3](#) dans le guide du développeur Amazon Simple Storage Service. Pour plus d'informations sur les identifiants uniques de rôle AWS Identity

and Access Management (IAM), consultez la section [Identifiants uniques](#) dans le guide de l'AWS Identity and Access Management utilisateur.

Gestion des utilisateurs pour les points de terminaison du serveur

Dans les sections suivantes, vous trouverez des informations sur la façon d'ajouter des utilisateurs à l'aide d' AWS Transfer Family un fournisseur d'identité personnalisé AWS Directory Service for Microsoft Active Directory ou d'un fournisseur d'identité.

Si vous utilisez un type d'identité géré par un service, vous ajoutez des utilisateurs à votre serveur compatible avec le protocole de transfert de fichiers. Dans ce cas, chaque nom d'utilisateur doit être unique sur votre serveur.

Dans le cadre des propriétés de chaque utilisateur, vous stockez également la clé publique Secure Shell (SSH) de cet utilisateur. Cela est nécessaire pour l'authentification par clé, utilisée par cette procédure. La clé privée est stockée localement sur l'ordinateur de votre utilisateur. Lorsque votre utilisateur envoie une demande d'authentification à votre serveur à l'aide d'un client, celui-ci confirme d'abord que l'utilisateur a accès à la clé SSH privée associée. Le serveur authentifie ensuite correctement l'utilisateur.

En outre, vous spécifiez le répertoire personnel, ou répertoire de destination, d'un utilisateur et vous lui attribuez un rôle AWS Identity and Access Management (IAM). Vous pouvez éventuellement fournir une politique de session pour limiter l'accès des utilisateurs uniquement au répertoire de base de votre compartiment Amazon S3.

Important

AWS Transfer Family empêche les noms d'utilisateur de 1 ou 2 caractères de s'authentifier auprès SFTP des serveurs. De plus, nous bloquons également le nom `root` d'utilisateur. Cela s'explique par le grand nombre de tentatives de connexion malveillantes effectuées par des scanners de mots de passe.

Amazon EFS contre Amazon S3

Caractéristiques de chaque option de stockage :

- Pour limiter l'accès : Amazon S3 prend en charge les politiques de session ; Amazon EFS prend en charge les POSIX utilisateurs, les groupes et les groupes secondaires IDs

- Les deux prennent en charge les clés publiques/privées
- Les deux prennent en charge les répertoires personnels
- Les deux prennent en charge les répertoires logiques

Note

Pour Amazon S3, la plupart des répertoires logiques sont pris en charge via API/CLI. Vous pouvez utiliser la case à cocher Restreint de la console pour verrouiller l'accès d'un utilisateur à son répertoire personnel, mais vous ne pouvez pas spécifier de structure de répertoire virtuel.

Répertoires logiques

Si vous spécifiez des valeurs de répertoire logiques pour votre utilisateur, le paramètre que vous utilisez dépend du type d'utilisateur.

- Pour les utilisateurs gérés par des services, fournissez des valeurs de répertoire logiques dans `HomeDirectoryMappings`
- Pour les utilisateurs de fournisseurs d'identité personnalisés, fournissez des valeurs de répertoire logiques dans `HomeDirectoryDetails`.

Rubriques

- [Travailler avec des utilisateurs gérés par des services](#)
- [Utilisation du fournisseur d'identité du AWS Directory Service](#)
- [Travailler avec des fournisseurs d'identité personnalisés](#)

Travailler avec des utilisateurs gérés par des services

Vous pouvez ajouter des utilisateurs EFS gérés par Amazon S3 ou Amazon Service à votre serveur, en fonction du paramètre de domaine du serveur. Pour de plus amples informations, veuillez consulter [Configuration d'un point SFTP de FTPS terminaison ou d'FTP un serveur](#).

[Pour ajouter un utilisateur géré par un service par programmation, consultez l'exemple du `CreateUserAPI`](#)

 Note

Pour les utilisateurs gérés par des services, il existe une limite de 2 000 entrées de répertoire logique. Pour plus d'informations sur l'utilisation de répertoires logiques, consultez [Utilisation de répertoires logiques pour simplifier vos structures de répertoires Transfer Family](#).

Rubriques

- [Ajouter des utilisateurs gérés par le service Amazon S3](#)
- [Ajouter des utilisateurs gérés par le EFS service Amazon](#)
- [Gestion des utilisateurs gérés par des services](#)

Ajouter des utilisateurs gérés par le service Amazon S3

 Note

Si vous souhaitez configurer un bucket Amazon S3 multi-comptes, suivez les étapes décrites dans cet article du centre de connaissances : [Comment configurer mon AWS Transfer Family serveur pour utiliser un bucket Amazon Simple Storage Service qui se trouve dans un autre AWS compte ?](#).

Pour ajouter un utilisateur géré par le service Amazon S3 à votre serveur

1. Ouvrez la AWS Transfer Family console sur <https://console.aws.amazon.com/transfer/>, puis sélectionnez Serveurs dans le volet de navigation.
2. Sur la page Serveurs, cochez la case du serveur auquel vous souhaitez ajouter un utilisateur.
3. Sélectionnez Ajouter un utilisateur.
4. Dans la section Configuration utilisateur, pour Nom d'utilisateur, entrez le nom d'utilisateur. Ce nom d'utilisateur doit comporter au minimum 3 caractères et au maximum 100 caractères. Vous pouvez utiliser les caractères suivants dans le nom d'utilisateur : a—z, A-Z, 0—9, trait de soulignement « _ », tiret « - », point ' . ', et au panneau « @ ». Le nom d'utilisateur ne peut pas commencer par un tiret « - », point ' . ', ou au panneau « @ ».
5. Pour Access, choisissez le IAM rôle que vous avez créé précédemment et qui donne accès à votre compartiment Amazon S3.

Vous avez créé ce IAM rôle à l'aide de la procédure décrite dans [Création d'un IAM rôle et d'une politique](#). Ce IAM rôle inclut une IAM politique qui fournit l'accès à votre compartiment Amazon S3. Cela inclut également une relation de confiance avec le AWS Transfer Family service, définie dans une autre IAM politique. Si vous avez besoin d'un contrôle d'accès précis pour vos utilisateurs, consultez le billet de blog [Enhance data access control with AWS Transfer Family and Amazon S3](#).

6. (Facultatif) Pour Politique, sélectionnez l'une des options suivantes :

- Aucun
- Politique existante
- Sélectionnez une politique parmi IAM : vous permet de choisir une politique de session existante. Choisissez Afficher pour voir un JSON objet contenant les détails de la politique.
- Génération automatique d'une politique basée sur le dossier de base : génère une politique de session pour vous. Choisissez Afficher pour voir un JSON objet contenant les détails de la politique.

 Note

Si vous choisissez Générer automatiquement une politique basée sur le dossier de base, ne sélectionnez pas Restreint pour cet utilisateur.

Pour en savoir plus sur les règles de session, voir [Création d'un IAM rôle et d'une politique](#). Pour en savoir plus sur la création d'une politique de session, consultez [Création d'une politique de session pour un compartiment Amazon S3](#).

7. Pour le répertoire personnel, choisissez le compartiment Amazon S3 dans lequel stocker les données à transférer AWS Transfer Family. Entrez le chemin d'accès au home répertoire dans lequel votre utilisateur atterrit lorsqu'il se connecte à l'aide de son client.

Si vous laissez ce paramètre vide, le root répertoire de votre compartiment Amazon S3 est utilisé. Dans ce cas, assurez-vous que votre IAM rôle donne accès à ce root répertoire.

 Note

Nous vous recommandons de choisir un chemin de répertoire contenant le nom d'utilisateur de l'utilisateur, afin d'utiliser efficacement une politique de session. La

politique de session limite l'accès des utilisateurs dans le compartiment Amazon S3 au home répertoire de cet utilisateur.

8. (Facultatif) Pour Restreint, cochez la case afin que vos utilisateurs ne puissent accéder à rien en dehors de ce dossier et ne puissent pas voir le nom du compartiment ou du dossier Amazon S3.

 Note

L'attribution d'un répertoire personnel à l'utilisateur et la restriction de l'utilisateur à ce répertoire personnel devraient suffire à verrouiller l'accès de l'utilisateur au dossier désigné. Si vous devez appliquer des contrôles supplémentaires, utilisez une politique de session.

Si vous sélectionnez Restreint pour cet utilisateur, vous ne pouvez pas sélectionner Générer automatiquement une politique basée sur le dossier de base, car le dossier de base n'est pas une valeur définie pour les utilisateurs restreints.

9. Pour clé SSH publique, entrez la partie SSH clé publique de la paire de SSH clés.

Votre clé est validée par le service avant que vous puissiez ajouter votre nouvel utilisateur.

 Note

Pour obtenir des instructions sur la façon de générer une paire de SSH clés, consultez [Génération de SSH clés pour les utilisateurs gérés par des services](#).

10. (Facultatif) Pour Clé et Valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
11. Choisissez Add (Ajouter) pour ajouter votre nouvel utilisateur au serveur que vous avez choisi.

Le nouvel utilisateur apparaît dans la section Utilisateurs de la page de détails du serveur.

Prochaines étapes — Pour l'étape suivante, passez à [Transfert de fichiers via un point de terminaison serveur à l'aide d'un client](#).

Ajouter des utilisateurs gérés par le EFS service Amazon

Amazon EFS utilise le modèle d'autorisation de fichier Portable Operating System Interface (POSIX) pour représenter la propriété des fichiers.

- Pour plus de détails sur la propriété des EFS fichiers Amazon, consultez la section [Propriété des EFS fichiers Amazon](#).
- Pour plus de détails sur la configuration des annuaires pour vos EFS utilisateurs, consultez [Configurer les EFS utilisateurs Amazon pour Transfer Family](#).

Pour ajouter un utilisateur EFS géré par le service Amazon à votre serveur

1. Ouvrez la AWS Transfer Family console sur <https://console.aws.amazon.com/transfer/>, puis sélectionnez Serveurs dans le volet de navigation.
2. Sur la page Servers, sélectionnez le EFS serveur Amazon auquel vous souhaitez ajouter un utilisateur.
3. Choisissez Ajouter un utilisateur pour afficher la page Ajouter un utilisateur.
4. Dans la section Configuration utilisateur, utilisez les paramètres suivants.
 - a. Le nom d'utilisateur doit comporter un minimum de 3 et un maximum de 100 caractères. Vous pouvez utiliser les caractères suivants dans le nom d'utilisateur : a—z, A-Z, 0—9, trait de soulignement « _ », tiret « - », point ' . ', et au panneau « @ ». Le nom d'utilisateur ne peut pas commencer par un tiret « - », point ' . ', ou au panneau « @ ».
 - b. Pour l'ID utilisateur et l'ID de groupe, notez ce qui suit :
 - Pour le premier utilisateur que vous créez, nous vous recommandons de saisir une valeur égale à la fois **0** pour l'ID de groupe et l'ID utilisateur. Cela accorde à l'utilisateur des privilèges d'administrateur pour AmazonEFS.
 - Pour les utilisateurs supplémentaires, entrez l'ID utilisateur et POSIX l'ID de groupe de l'utilisateur. Ils IDs sont utilisés pour toutes les opérations Amazon Elastic File System effectuées par l'utilisateur.
 - Pour l'ID utilisateur et l'ID de groupe, n'utilisez pas de zéros en début de liste. Par exemple, **12345** c'est acceptable, ne l'**012345**est pas.
 - c. (Facultatif) Pour Groupe secondaire IDs, entrez un ou plusieurs POSIX groupes supplémentaires IDs pour chaque utilisateur, séparés par des virgules.
 - d. Pour Access, choisissez le IAM rôle qui :
 - Permet à l'utilisateur d'accéder uniquement aux EFS ressources Amazon (systèmes de fichiers) auxquelles vous souhaitez qu'il accède.

- Définit les opérations de système de fichiers que l'utilisateur peut ou ne peut pas effectuer.

Nous vous recommandons d'utiliser le IAM rôle pour sélectionner le système de EFS fichiers Amazon avec un accès au montage et des autorisations de lecture/écriture. Par exemple, la combinaison des deux politiques AWS gérées suivantes, bien que très permissive, accorde les autorisations nécessaires à votre utilisateur :

- AmazonElasticFileSystemClientFullAccess
- AWSTransferConsoleFullAccess

Pour plus d'informations, consultez le billet de blog sur la [AWS Transfer Family prise en charge d'Amazon Elastic File System](#).

e. Pour le répertoire personnel, procédez comme suit :

- Choisissez le système de EFS fichiers Amazon que vous souhaitez utiliser pour stocker les données à transférer AWS Transfer Family.
- Décidez si le répertoire de base doit être défini sur Restreint. Le fait de définir le répertoire de base sur Restreint a les effets suivants :
 - EFS Les utilisateurs d'Amazon ne peuvent accéder à aucun fichier ou répertoire en dehors de ce dossier.
 - EFS Les utilisateurs d'Amazon ne peuvent pas voir le nom EFS du système de fichiers Amazon (fs-xxxxxxx).

 Note

Lorsque vous sélectionnez l'option Restreint, les liens symboliques ne sont pas résolus pour les EFS utilisateurs d'Amazon.

- (Facultatif) Entrez le chemin du répertoire de base dans lequel vous souhaitez que les utilisateurs se trouvent lorsqu'ils se connectent à l'aide de leur client.

Si vous ne spécifiez pas de répertoire personnel, le répertoire racine de votre système de EFS fichiers Amazon est utilisé. Dans ce cas, assurez-vous que votre IAM rôle donne accès à ce répertoire racine.

5. Pour clé SSH publique, entrez la partie SSH clé publique de la paire de SSH clés.

Votre clé est validée par le service avant que vous puissiez ajouter votre nouvel utilisateur.

 Note

Pour obtenir des instructions sur la façon de générer une paire de SSH clés, consultez [Génération de SSH clés pour les utilisateurs gérés par des services](#).

6. (Facultatif) Entrez des balises pour l'utilisateur. Pour Clé et Valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur, puis choisissez Ajouter une balise.
7. Choisissez Add (Ajouter) pour ajouter votre nouvel utilisateur au serveur que vous avez choisi.

Le nouvel utilisateur apparaît dans la section Utilisateurs de la page de détails du serveur.

Problèmes que vous pourriez rencontrer lorsque vous accédez pour la première fois SFTP à votre serveur Transfer Family :

- Si vous exécutez la `sftp` commande et que l'invite ne s'affiche pas, le message suivant peut s'afficher :

```
Couldn't canonicalize: Permission denied
```

```
Need cwd
```

Dans ce cas, vous devez augmenter les autorisations liées à la politique pour le rôle de votre utilisateur. Vous pouvez ajouter une politique AWS gérée, telle que `AmazonElasticFileSystemClientFullAccess`.

- Si vous entrez `pwd` à l'invite `sftp` pour consulter le répertoire personnel de l'utilisateur, le message suivant peut s'afficher, où ***USER-HOME-DIRECTORY*** est le répertoire personnel de l'SFTP utilisateur :

```
remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
```

Dans ce cas, vous devriez pouvoir accéder au répertoire parent (`cd ..`) et créer le répertoire personnel de l'utilisateur (`mkdir username`).

Prochaines étapes — Pour l'étape suivante, passez à [Transfert de fichiers via un point de terminaison serveur à l'aide d'un client](#).

Gestion des utilisateurs gérés par des services

Dans cette section, vous trouverez des informations sur la façon d'afficher une liste d'utilisateurs, de modifier les détails des utilisateurs et d'ajouter une clé SSH publique.

- [Afficher la liste des utilisateurs](#)
- [Afficher ou modifier les informations de l'utilisateur](#)
- [Suppression d'un utilisateur](#)
- [Ajouter une clé SSH publique](#)
- [Supprimer SSH la clé publique](#)

Pour trouver la liste de vos utilisateurs

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Sélectionnez Serveurs dans le volet de navigation pour afficher la page Serveurs.
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur.
4. Sous Utilisateurs, consultez la liste des utilisateurs.

Pour afficher ou modifier les informations de l'utilisateur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Sélectionnez Serveurs dans le volet de navigation pour afficher la page Serveurs.
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur.
4. Sous Utilisateurs, choisissez un nom d'utilisateur pour afficher la page de détails de l'utilisateur.

Vous pouvez modifier les propriétés de l'utilisateur sur cette page en choisissant Modifier.

5. Sur la page Détails des utilisateurs, choisissez Modifier à côté de Configuration utilisateur.

Edit configuration

User configuration

Access [Info](#)
User's IAM role for Amazon S3 access

Admin ▼ ↻

Policy [Info](#)
Scope down policy to apply to the user

☒ None
☐ Existing policy
☐ Select a policy from IAM

View

Home directory
User's login directory

Choose an S3 bucket ▼

Enter optional folder

☐ Restricted [Info](#)

Cancel Save

6. Sur la page Modifier la configuration, pour Access, choisissez le IAM rôle que vous avez créé précédemment et qui donne accès à votre compartiment Amazon S3.

Vous avez créé ce IAM rôle à l'aide de la procédure décrite dans [Création d'un IAM rôle et d'une politique](#). Ce IAM rôle inclut une IAM politique qui fournit l'accès à votre compartiment Amazon S3. Cela inclut également une relation de confiance avec le AWS Transfer Family service, définie dans une autre IAM politique.

7. (Facultatif) Dans le champ Politique, sélectionnez l'une des options suivantes :

- Aucun
- Politique existante
- Sélectionnez une politique IAM pour choisir une politique existante. Choisissez Afficher pour voir un JSON objet contenant les détails de la politique.

Pour en savoir plus sur les règles de session, voir [Création d'un IAM rôle et d'une politique](#). Pour en savoir plus sur la création d'une politique de session, consultez [Création d'une politique de session pour un compartiment Amazon S3](#).

8. Pour le répertoire personnel, choisissez le compartiment Amazon S3 dans lequel stocker les données à transférer AWS Transfer Family. Entrez le chemin d'accès au home répertoire dans lequel votre utilisateur atterrit lorsqu'il se connecte à l'aide de son client.

Si vous laissez ce paramètre vide, le root répertoire de votre compartiment Amazon S3 est utilisé. Dans ce cas, assurez-vous que votre IAM rôle donne accès à ce root répertoire.

 Note

Nous vous recommandons de choisir un chemin de répertoire contenant le nom d'utilisateur de l'utilisateur, afin d'utiliser efficacement une politique de session. La politique de session limite l'accès des utilisateurs dans le compartiment Amazon S3 au home répertoire de cet utilisateur.

9. (Facultatif) Pour Restreint, cochez la case afin que vos utilisateurs ne puissent accéder à rien en dehors de ce dossier et ne puissent pas voir le nom du compartiment ou du dossier Amazon S3.

 Note

Lorsque vous attribuez un répertoire personnel à l'utilisateur et que vous le limitez à ce répertoire personnel, cela devrait être suffisant pour verrouiller l'accès de l'utilisateur au dossier désigné. Utilisez une politique de session lorsque vous devez appliquer des contrôles supplémentaires.

10. Choisissez Save pour enregistrer les changements.

Pour supprimer un utilisateur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Sélectionnez Serveurs dans le volet de navigation pour afficher la page Serveurs.
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur.
4. Sous Utilisateurs, choisissez un nom d'utilisateur pour afficher la page de détails de l'utilisateur.
5. Sur la page des détails de l'utilisateur, choisissez Supprimer à droite du nom d'utilisateur.
6. Dans la boîte de dialogue de confirmation qui s'affiche **delete**, entrez le mot, puis choisissez Supprimer pour confirmer que vous souhaitez supprimer l'utilisateur.

L'utilisateur est supprimé de la liste des utilisateurs.

Pour ajouter une clé SSH publique pour un utilisateur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, choisissez Servers (Serveurs).
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur.
4. Sous Utilisateurs, choisissez un nom d'utilisateur pour afficher la page de détails de l'utilisateur.
5. Choisissez Ajouter une clé SSH publique pour ajouter une nouvelle clé SSH publique à un utilisateur.

 Note

SSHles clés ne sont utilisées que par les serveurs activés pour le protocole de transfert de fichiers Secure Shell (SSH) (SFTP). Pour plus d'informations sur la génération d'une paire de SSH clés, consultez [Génération de SSH clés pour les utilisateurs gérés par des services](#).

6. Pour clé SSH publique, entrez la partie clé SSH publique de la paire de SSH clés.

Votre clé est validée par le service avant que vous puissiez ajouter votre nouvel utilisateur. Le format de la SSH clé est `ssh-rsa string`. Pour générer une paire de SSH clés, consultez [Génération de SSH clés pour les utilisateurs gérés par des services](#).

7. Sélectionnez Ajouter une clé.

Pour supprimer une clé SSH publique pour un utilisateur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, choisissez Servers (Serveurs).
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur.
4. Sous Utilisateurs, choisissez un nom d'utilisateur pour afficher la page de détails de l'utilisateur.
5. Pour supprimer une clé publique, cochez SSH la case correspondante et choisissez Supprimer.

Utilisation du fournisseur d'identité du AWS Directory Service

Cette rubrique décrit comment utiliser le fournisseur d'identité du AWS Directory Service pour AWS Transfer Family.

Rubriques

- [En utilisant AWS Directory Service for Microsoft Active Directory](#)
- [Utilisation du service d' AWS annuaire pour les services de domaine Azure Active Directory](#)

En utilisant AWS Directory Service for Microsoft Active Directory

Vous pouvez l'utiliser AWS Transfer Family pour authentifier les utilisateurs finaux de votre transfert de fichiers à l'aide AWS Directory Service for Microsoft Active Directory de. Il permet une migration fluide des flux de transfert de fichiers qui reposent sur l'authentification Active Directory sans modifier les informations d'identification des utilisateurs finaux ni avoir besoin d'un autorisateur personnalisé.

Vous pouvez ainsi fournir aux AWS Managed Microsoft AD AWS Directory Service utilisateurs et aux groupes un accès sécurisé SFTP FTP aux données stockées dans Amazon Simple Storage Service (Amazon S3) ou Amazon Elastic File System (AmazonEFS) et pour ces données. FTPS Si vous utilisez Active Directory pour stocker les informations d'identification de vos utilisateurs, vous disposez désormais d'un moyen plus simple d'activer les transferts de fichiers pour ces utilisateurs.

Vous pouvez fournir un accès aux groupes Active Directory AWS Managed Microsoft AD dans votre environnement sur site ou dans le AWS cloud à l'aide de connecteurs Active Directory. Vous pouvez donner aux utilisateurs déjà configurés dans votre environnement Microsoft Windows, que ce soit dans le AWS Cloud ou sur leur réseau local, l'accès à un AWS Transfer Family serveur qui utilise AWS Managed Microsoft AD l'identité.

Note

- AWS Transfer Family ne prend pas en charge Simple AD.
- Transfer Family ne prend pas en charge les configurations Active Directory interrégionales : nous prenons uniquement en charge les intégrations Active Directory situées dans la même région que celle du serveur Transfer Family.
- Transfer Family ne prend pas en charge l'utilisation d'AD Connector AWS Managed Microsoft AD ou d'AD Connector pour activer l'authentification multifactorielle (MFA) pour votre RADIUS MFA infrastructure existante.

- AWS Transfer Family ne prend pas en charge les régions répliquées de Managed Active Directory.

Pour l'utiliser AWS Managed Microsoft AD, vous devez suivre les étapes suivantes :

1. Créez un ou plusieurs AWS Managed Microsoft AD répertoires à l'aide de la AWS Directory Service console.
2. Utilisez la console Transfer Family pour créer un serveur utilisé AWS Managed Microsoft AD comme fournisseur d'identité.
3. Ajoutez l'accès depuis un ou plusieurs de vos AWS Directory Service groupes.
4. Bien que cela ne soit pas obligatoire, nous vous recommandons de tester et de vérifier l'accès des utilisateurs.

Rubriques

- [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#)
- [Utilisation des domaines Active Directory](#)
- [Choisir AWS Managed Microsoft AD comme fournisseur d'identité](#)
- [Octroi de l'accès aux groupes](#)
- [Tester les utilisateurs](#)
- [Supprimer l'accès au serveur pour un groupe](#)
- [Connexion au serveur à l'aide de SSH \(Secure Shell\)](#)
- [Connexion AWS Transfer Family à un Active Directory autogéré à l'aide de forêts et d'approbations](#)

Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory

Fournissez un identifiant unique pour vos groupes AD

Avant de pouvoir l'utiliser AWS Managed Microsoft AD, vous devez fournir un identifiant unique pour chaque groupe de votre annuaire Microsoft AD. Pour ce faire, vous pouvez utiliser l'identifiant de sécurité (SID) de chaque groupe. Les utilisateurs du groupe que vous associez ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family.

Utilisez la PowerShell commande Windows suivante pour récupérer le nom SID d'un groupe, en remplaçant *YourGroupName* avec le nom du groupe.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select  
SamAccountName, ObjectSid
```

Note

Si vous utilisez AWS Directory Service comme fournisseur d'identité, `userPrincipalName` et si vous `SamAccountName` avez des valeurs différentes, AWS Transfer Family accepte la valeur dans `SamAccountName`. Transfer Family n'accepte pas la valeur spécifiée dans `userPrincipalName`.

Ajoutez AWS Directory Service des autorisations à votre rôle

Vous avez également besoin d' AWS Directory Service API autorisations pour l'utiliser AWS Directory Service en tant que fournisseur d'identité. Les autorisations suivantes sont requises ou suggérées :

- `ds:DescribeDirectories` est nécessaire pour que Transfer Family puisse consulter le répertoire
- `ds:AuthorizeApplication` est nécessaire pour ajouter une autorisation pour Transfer Family
- `ds:UnauthorizeApplication` est suggéré de supprimer toutes les ressources créées de manière provisoire, au cas où quelque chose ne tournerait pas rond pendant le processus de création du serveur

Ajoutez ces autorisations au rôle que vous utilisez pour créer vos serveurs Transfer Family. Pour plus de détails sur ces autorisations, voir [AWS Directory Service API Autorisations : référence aux actions, aux ressources et aux conditions](#).

Utilisation des domaines Active Directory

Lorsque vous réfléchissez à la manière dont vos utilisateurs Active Directory peuvent accéder aux AWS Transfer Family serveurs, gardez à l'esprit le domaine de l'utilisateur et celui de son groupe. Idéalement, le domaine de l'utilisateur et celui de son groupe devraient correspondre. En d'autres termes, l'utilisateur et le groupe se trouvent dans le domaine par défaut, ou les deux dans le domaine de confiance. Si ce n'est pas le cas, l'utilisateur ne peut pas être authentifié par Transfer Family.

Vous pouvez tester l'utilisateur pour vous assurer que la configuration est correcte. Pour plus de détails, consultez [Tester les utilisateurs](#). En cas de problème avec le domaine utilisateur/groupe, vous recevez le message d'erreur « Aucun accès associé trouvé pour les groupes d'utilisateurs ».

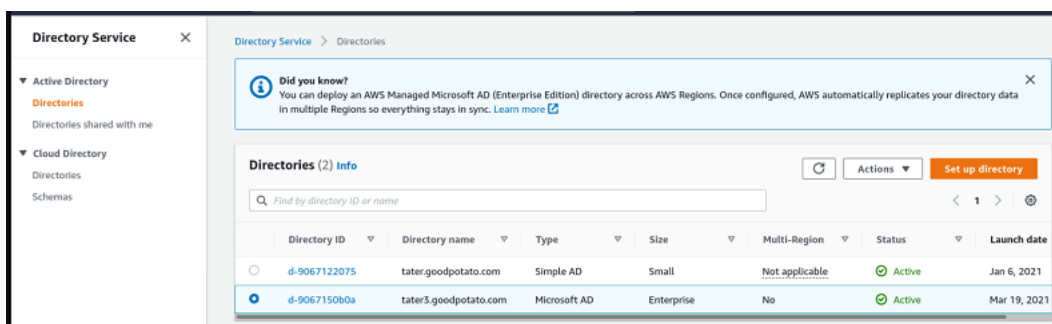
Choisir AWS Managed Microsoft AD comme fournisseur d'identité

Cette section décrit comment l'utiliser AWS Directory Service for Microsoft Active Directory avec un serveur.

À utiliser AWS Managed Microsoft AD avec Transfer Family

1. Connectez-vous à la AWS Directory Service console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.

Utilisez la AWS Directory Service console pour configurer un ou plusieurs annuaires gérés. Pour plus d'informations, veuillez consulter la rubrique [AWS Managed Microsoft AD](#) dans le Guide de l'administrateur AWS Directory Service .



2. Ouvrez la AWS Transfer Family console à <https://console.aws.amazon.com/transfer/>, puis choisissez Create server.
3. Sur la page Choisir des protocoles, sélectionnez un ou plusieurs protocoles dans la liste.

Note

Si vous le sélectionnez FTPS, vous devez fournir le AWS Certificate Manager certificat.

4. Pour Choisir un fournisseur d'identité, choisissez AWS Directory Service.

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☒ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

Directory

TATER3 ▼ 

Cancel Previous Next

5. La liste des annuaires contient tous les annuaires gérés que vous avez configurés. Choisissez un répertoire dans la liste, puis cliquez sur Next.

Note

- Les annuaires multicomptes et partagés ne sont pas pris en charge pour AWS Managed Microsoft AD.
- Pour configurer un serveur avec Directory Service comme fournisseur d'identité, vous devez ajouter des AWS Directory Service autorisations. Pour plus de détails, consultez [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#).

6. Pour terminer la création du serveur, appliquez l'une des procédures suivantes :
- [Création d'un SFTP serveur activé](#)
 - [Création d'un FTPS serveur activé](#)
 - [Création d'un FTP serveur activé](#)

Dans ces procédures, passez à l'étape qui suit le choix d'un fournisseur d'identité.

 Important

Vous ne pouvez pas supprimer un répertoire Microsoft AD AWS Directory Service si vous l'avez utilisé sur un serveur Transfer Family. Vous devez d'abord supprimer le serveur, puis vous pouvez supprimer le répertoire.

Octroi de l'accès aux groupes

Après avoir créé le serveur, vous devez choisir les groupes du répertoire qui doivent avoir accès au chargement et au téléchargement de fichiers via les protocoles activés à l'aide de AWS Transfer Family. Pour ce faire, créez un accès.

 Note

Les utilisateurs doivent appartenir directement au groupe auquel vous accordez l'accès. Par exemple, supposons que Bob est un utilisateur et qu'il appartient à GroupA, et que GroupA lui-même est inclus dans GroupB.

- Si vous accordez l'accès à GroupA, Bob est autorisé à y accéder.
- Si vous accordez l'accès au groupe B (et non au groupe A), Bob n'y a pas accès.

Pour accorder l'accès à un groupe

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Accédez à la page des détails de votre serveur.
3. Dans la section Accès, choisissez Ajouter un accès.
4. Entrez SID le AWS Managed Microsoft AD répertoire auquel vous souhaitez accéder à ce serveur.

 Note

Pour plus d'informations sur la manière de trouver le SID correspondant à votre groupe, consultez [the section called “Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory”](#).

5. Pour Access, choisissez un AWS Identity and Access Management (IAM) rôle pour le groupe.

6. Dans la section Stratégie, choisissez une stratégie. Le paramètre par défaut est Aucun.
7. Pour le répertoire personnel, choisissez un compartiment S3 correspondant au répertoire personnel du groupe.

 Note

Vous pouvez limiter les parties du bucket visibles par les utilisateurs en créant une politique de session. Par exemple, pour limiter les utilisateurs à leur propre dossier dans le /filetest répertoire, entrez le texte suivant dans le champ.

```
/filetest/${transfer:UserName}
```

Pour en savoir plus sur la création d'une politique de session, consultez [Création d'une politique de session pour un compartiment Amazon S3](#).

8. Choisissez Ajouter pour créer l'association.
9. Choisissez votre serveur.
10. Choisissez Ajouter un accès.
 - Entrez le SID pour le groupe.

 Note

Pour plus d'informations sur la façon de les trouverSID, consultez [the section called "Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory"](#).

11. Choisissez Ajouter un accès.

Dans la section Accès, les accès au serveur sont répertoriés.

Endpoint configuration

Availability Zone	Subnet ID	Private IPv4 Address
us-east-1a	subnet-XXXX	172.31.80.36

Accesses (1)

Actions Associate access

External Id	Home directory	Role
☒ S...	/padbucket3	ADGuy_S3_And_EFS

Additional details Edit

Logging role [Info](#)
Server activity not logged to Amazon CloudWatch

Server host key [Info](#)

Security Policy [Info](#)
TransferSecurityPolicy-2018-11

Domain
Amazon S3

Tester les utilisateurs

Vous pouvez vérifier si un utilisateur a accès à l' AWS Managed Microsoft AD annuaire de votre serveur.

Note

Un utilisateur doit appartenir exactement à un groupe (un ID externe) répertorié dans la section Accès de la page de configuration du point de terminaison. Si l'utilisateur ne fait partie d'aucun groupe, ou s'il fait partie de plusieurs groupes, il n'est pas autorisé à y accéder.

Pour vérifier si un utilisateur spécifique a accès

1. Sur la page de détails du serveur, choisissez Actions, puis sélectionnez Test.
2. Pour tester le fournisseur d'identité, entrez les informations de connexion d'un utilisateur appartenant à l'un des groupes ayant accès.
3. Sélectionnez Tester).

Vous voyez un test du fournisseur d'identité réussi, indiquant que l'utilisateur sélectionné a obtenu l'accès au serveur.

Identity provider testing

User configuration [Info](#)

Username:
Password:

Response

```
{
  "Response": {
    "homeDirectory": {"/padbucket3"},
    "homeDirectoryDetails": null,
    "homeDirectoryType": "PATH",
    "posixProfile": {
      "publicKeys": null,
      "role": "arn:aws:iam::195886157073:role/ADGuy_53_Aud_EFS",
      "policy": null,
      "userName": "transferuser1",
      "identityProviderType": null,
      "userConfigMessage": null
    },
    "StatusCode": 200,
    "Message": ""
  }
}
```

Cancel **Test**

Si l'utilisateur appartient à plusieurs groupes ayant accès, vous recevez la réponse suivante.

```
"Response": "",
"StatusCode": 200,
"Message": "More than one associated access found for user's groups."
```

Supprimer l'accès au serveur pour un groupe

Pour supprimer l'accès au serveur pour un groupe

1. Sur la page de détails du serveur, choisissez Actions, puis sélectionnez Supprimer l'accès.
2. Dans la boîte de dialogue, confirmez que vous souhaitez supprimer l'accès à ce groupe.

Lorsque vous revenez à la page des détails du serveur, vous constatez que l'accès à ce groupe n'est plus répertorié.

Connexion au serveur à l'aide de SSH (Secure Shell)

Après avoir configuré votre serveur et vos utilisateurs, vous pouvez vous connecter au serveur en utilisant SSH et utiliser le nom d'utilisateur complet d'un utilisateur qui y a accès.

```
sftp user@active-directory-domain@vpc-endpoint
```

Par exemple :

```
transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-  
svc-987654zyxabc.us-east-1.vpce.amazonaws.com.
```

Ce format cible la recherche de la fédération, limitant ainsi la recherche dans un Active Directory potentiellement volumineux.

Note

Vous pouvez spécifier le nom d'utilisateur simple. Toutefois, dans ce cas, le code Active Directory doit effectuer une recherche dans tous les annuaires de la fédération. Cela peut limiter la recherche et l'authentification peut échouer même si l'utilisateur doit y avoir accès.

Une fois authentifié, l'utilisateur se trouve dans le répertoire de base que vous avez spécifié lors de sa configuration.

Connexion AWS Transfer Family à un Active Directory autogéré à l'aide de forêts et d'approbations

Les utilisateurs de votre Active Directory (AD) autogéré peuvent également utiliser l'authentification unique AWS IAM Identity Center pour accéder aux serveurs Transfer Family Comptes AWS et les utiliser. Pour ce faire, AWS Directory Service les options suivantes sont-elles disponibles :

- La confiance forestière unidirectionnelle (sortante AWS Managed Microsoft AD et entrante pour Active Directory sur site) ne fonctionne que pour le domaine racine.
- Pour les domaines enfants, vous pouvez utiliser l'une des options suivantes :
 - Utilisez une confiance bidirectionnelle entre Active AWS Managed Microsoft AD Directory et sur site
 - Utilisez une confiance externe unidirectionnelle pour chaque domaine enfant.

Lors de la connexion au serveur via un domaine sécurisé, l'utilisateur doit spécifier le domaine sécurisé, par exemple `transferuserexample@mycompany.com`.

Utilisation du service d' AWS annuaire pour les services de domaine Azure Active Directory

- Pour tirer parti de votre forêt Active Directory existante pour vos besoins de SFTP transfert, vous pouvez utiliser le [connecteur Active Directory](#).
- Si vous souhaitez bénéficier des avantages d'Active Directory et de la haute disponibilité dans un service entièrement géré, vous pouvez utiliser AWS Directory Service for Microsoft Active Directory. Pour plus de détails, consultez [Utilisation du fournisseur d'identité du AWS Directory Service](#).

Cette rubrique décrit comment utiliser un connecteur Active Directory et [Azure Active Directory Domain Services \(AzureADDS\)](#) pour authentifier les utilisateurs de SFTP Transfer auprès d'[Azure Active Directory](#).

Rubriques

- [Avant de commencer à utiliser AWS Directory Service pour Azure Active Directory Domain Services](#)
- [Étape 1 : ajout des services de domaine Azure Active Directory](#)
- [Étape 2 : Création d'un compte de service](#)
- [Étape 3 : Configuration de l' AWS annuaire à l'aide d'AD Connector](#)
- [Étape 4 : Configuration AWS Transfer Family du serveur](#)
- [Étape 5 : Accorder l'accès aux groupes](#)
- [Étape 6 : Tester les utilisateurs](#)

Avant de commencer à utiliser AWS Directory Service pour Azure Active Directory Domain Services

Pour cela AWS, vous avez besoin des éléments suivants :

- Un cloud privé virtuel (VPC) dans une AWS région où vous utilisez vos serveurs Transfer Family
- Au moins deux sous-réseaux privés dans votre VPC
- La connectivité Internet VPC indispensable
- Une passerelle client et une passerelle privée virtuelle pour la site-to-site VPN connexion à Microsoft Azure

Pour Microsoft Azure, vous avez besoin des éléments suivants :

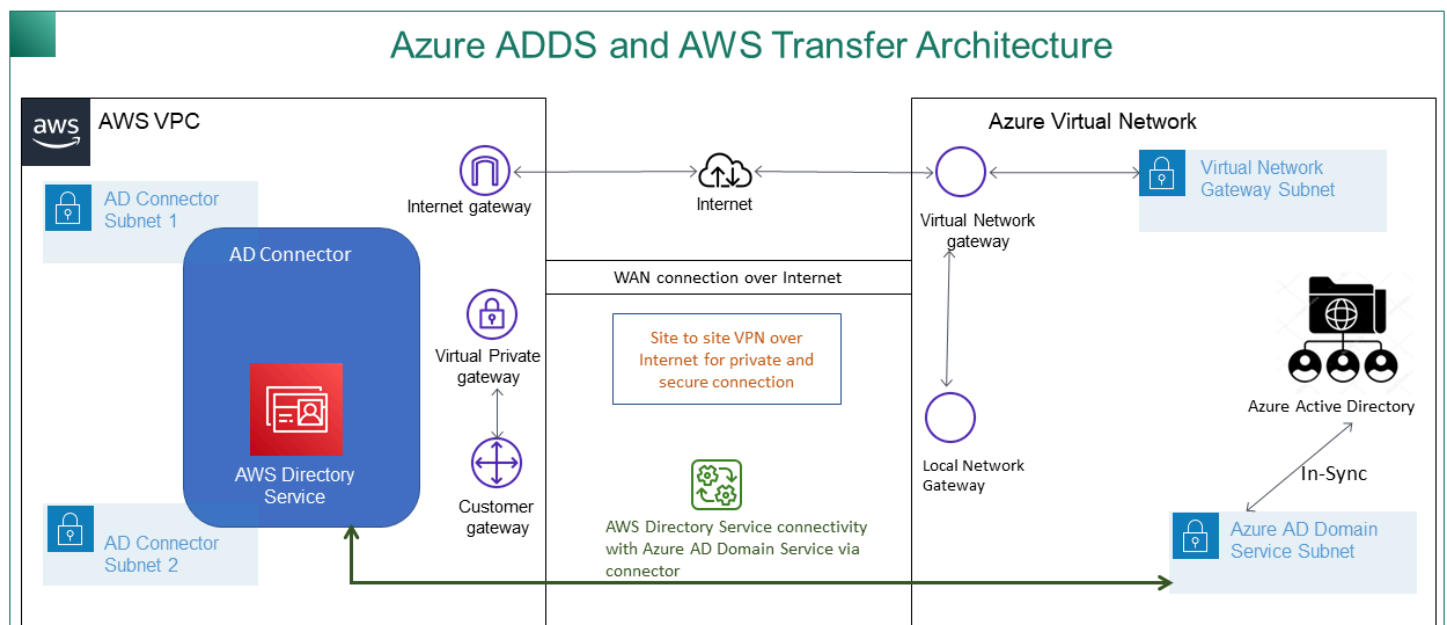
- Un service de domaine Azure Active Directory et Active Directory (AzureADDS)
- Un groupe de ressources Azure
- Un réseau virtuel Azure
- VPNconnectivité entre votre Amazon VPC et votre groupe de ressources Azure

Note

Cela peut se faire par le biais de IPSEC tunnels natifs ou d'VPNappareils. Dans cette rubrique, nous utilisons IPSEC des tunnels entre une passerelle réseau virtuelle Azure et une passerelle réseau locale. Les tunnels doivent être configurés pour autoriser le trafic entre vos ADDS points de terminaison Azure et les sous-réseaux qui les hébergent. AWS VPC

- Une passerelle client et une passerelle privée virtuelle pour la site-to-site VPN connexion à Microsoft Azure

Le schéma suivant montre la configuration requise avant de commencer.



Étape 1 : ajout des services de domaine Azure Active Directory

Azure AD ne prend pas en charge les instances de jointure de domaines par défaut. Pour effectuer des actions telles que l'adhésion à un domaine et utiliser des outils tels que la stratégie de groupe,

les administrateurs doivent activer les services de domaine Azure Active Directory. Si vous n'avez pas encore ajouté Azure AD DS ou si votre implémentation existante n'est pas associée au domaine que vous souhaitez que votre serveur de SFTP transfert utilise, vous devez ajouter une nouvelle instance.

Pour plus d'informations sur l'activation des services de domaine Azure Active Directory (AzureADDS), voir [Tutoriel : création et configuration d'un domaine géré par les services de domaine Azure Active Directory](#).

Note

Lorsque vous activez AzureADDS, assurez-vous qu'il est configuré pour le groupe de ressources et le domaine Azure AD auxquels vous connectez votre serveur de SFTP transfert.

The screenshot shows the Azure AD Domain Services interface for a domain named 'bob.us'. On the left, there is a navigation pane with options: Overview (selected), Activity log, Access control (IAM), Tags, Settings, and Properties. The main area displays the domain 'bob.us' with a status of 'Running' (indicated by a green checkmark). A 'View health' button is visible. Above the domain card, there is a search bar and buttons for 'Refresh' and 'Delete'. A warning banner at the top of the main area states: 'Configuration issues for your managed domain were detected. Run configuration diagnostics'.

Étape 2 : Création d'un compte de service

Azure AD doit disposer d'un compte de service faisant partie d'un groupe d'administrateurs dans AzureADDS. Ce compte est utilisé avec le connecteur AWS Active Directory. Assurez-vous que ce compte est synchronisé avec AzureADDS.

Home > Default Directory > Users > bobatusa

bobatusa | Profile

User

<<

[Edit](#) [Reset password](#) [Revoke sessions](#) [Delete](#) [Refresh](#) | [Got feedback?](#)

✖ Diagnose and solve problems

Manage

- Profile
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-in logs
- Audit logs

bobatusa

bobsmith@xyz.com



Creation time
10/6/2021, 1:32:27 AM

User Sign-ins

30

20

10

0

Oct 10 Oct 17 Oct 24 Oct 31

Group memberships

2

Identity

Name	First name	Last name
bobatusa	Bob	Smith
User Principal Name	User type	
bobsmith@xyz.com	Member	

Tip

L'authentification multifactorielle pour Azure Active Directory n'est pas prise en charge pour les serveurs Transfer Family qui utilisent le SFTP protocole. Le serveur Transfer Family ne peut pas fournir le MFA jeton une fois qu'un utilisateur s'est authentifié auprès de SFTP lui. Assurez-vous de le désactiver MFA avant de tenter de vous connecter.

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users

Multi-Factor Auth status: Any

bulk update

☐	DISPLAY NAME ^	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Christopher	admin@christopher[REDACTED].com	Disabled
☐	Robert	test@christopher[REDACTED].com	Disabled

Select a user

Étape 3 : Configuration de l' AWS annuaire à l'aide d'AD Connector

Après avoir configuré Azure ADDS et créé un compte de service avec des IPSEC VPN tunnels entre votre réseau virtuel AWS VPC et Azure, vous pouvez tester la connectivité en envoyant un ping à l'adresse ADDS DNS IP Azure depuis n'importe quelle AWS EC2 instance.

Après avoir vérifié que la connexion est active, vous pouvez continuer ci-dessous.

Pour configurer votre AWS annuaire à l'aide d'AD Connector

1. Ouvrez la console [Directory Service](#) et sélectionnez Directories.
2. Sélectionnez Configurer le répertoire.
3. Pour le type de répertoire, choisissez AD Connector.
4. Sélectionnez une taille de répertoire, sélectionnez Suivant, puis sélectionnez vos sous-réseaux VPC et sous-réseaux.
5. Sélectionnez Suivant, puis renseignez les champs comme suit :
 - DNSNom du répertoire : entrez le nom de domaine que vous utilisez pour votre AzureADDS.
 - DNSAdresses IP : entrez vos adresses ADDS IP Azure.
 - Nom d'utilisateur et mot de passe du compte serveur : entrez les détails du compte de service que vous avez créé à l'étape 2 : créer un compte de service.
6. Complétez les écrans pour créer le service d'annuaire.

Le statut du répertoire doit maintenant être Actif et il est prêt à être utilisé avec un serveur SFTP de transfert.

[Directory Service](#) > Directories

 **Did you know?**
You can deploy an AWS Managed Microsoft AD (Enterprise Edition) directory across AWS Regions. Once configured, AWS automatically replicates your directory data in multiple Regions so everything stays in sync. [Learn more](#)

Directories (1) [Info](#)

 **Actions** ▼ **Set up directory**

< 1 > 

Directory ID	Directory name	Type	Size	Multi-Region	Status	Launch date
 d-906752c0d7		AD Connector	Small	Not applicable	 Active	Nov 3, 2021

Étape 4 : Configuration AWS Transfer Family du serveur

Créez un serveur Transfer Family avec le SFTP protocole et le type de fournisseur d'identité de AWS Directory Service. Dans la liste déroulante Répertoire, sélectionnez le répertoire que vous avez ajouté à l'étape 3 : Configuration du AWS répertoire à l'aide d'AD Connector.

Note

Vous ne pouvez pas supprimer un répertoire Microsoft AD dans AWS Directory Service si vous l'avez utilisé sur un serveur Transfer Family. Vous devez d'abord supprimer le serveur, puis vous pouvez supprimer le répertoire.

Étape 5 : Accorder l'accès aux groupes

Après avoir créé le serveur, vous devez choisir les groupes du répertoire qui doivent avoir accès au chargement et au téléchargement de fichiers via les protocoles activés à l'aide de AWS Transfer Family. Pour ce faire, créez un accès.

Note

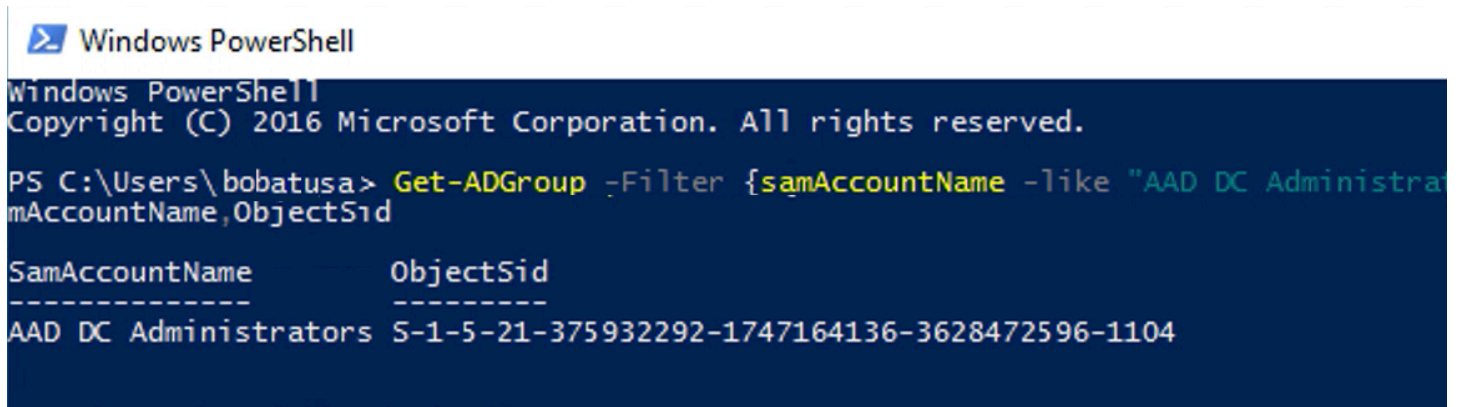
Les utilisateurs doivent appartenir directement au groupe auquel vous accordez l'accès. Par exemple, supposons que Bob est un utilisateur et qu'il appartient à GroupA, et que GroupA lui-même est inclus dans GroupB.

- Si vous accordez l'accès à GroupA, Bob est autorisé à y accéder.
- Si vous accordez l'accès au groupe B (et non au groupe A), Bob n'y a pas accès.

Pour accorder l'accès, vous devez récupérer le SID pour le groupe.

Utilisez la PowerShell commande Windows suivante pour récupérer le nom SID d'un groupe, en remplaçant *YourGroupName* avec le nom du groupe.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select SamAccountName, ObjectSid
```



```

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\bobatusa> Get-ADGroup -Filter {samAccountName -like "AAD DC Administrators"}
SamAccountName      ObjectSid
-----
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
  
```

Accorder l'accès aux groupes

1. Ouvert <https://console.aws.amazon.com/transfer/>.
2. Accédez à la page des détails de votre serveur et dans la section Accès, sélectionnez Ajouter un accès.
3. Entrez le SID résultat de la procédure précédente.
4. Pour Access, choisissez un AWS Identity and Access Management rôle pour le groupe.
5. Dans la section Stratégie, choisissez une stratégie. La valeur par défaut est Aucune.
6. Pour le répertoire personnel, choisissez un compartiment S3 correspondant au répertoire personnel du groupe.
7. Choisissez Ajouter pour créer l'association.

Les informations provenant de votre serveur de transfert doivent ressembler à ce qui suit :

Protocols
Edit

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider
Edit

Identity provider type
AWS Directory Service

 Directory ID
d-123456789a

Accesses (1)

Actions
 Add access

< 1 >

☐	External Id	Home directory	Role
☐	S-1-5-21-375932292-1747164136-3628472596-1104	/sftp-home-dir	sftp-user-role

Étape 6 : Tester les utilisateurs

Vous pouvez tester ([Tester les utilisateurs](#)) si un utilisateur a accès au AWS Managed Microsoft AD répertoire de votre serveur. Un utilisateur doit appartenir exactement à un groupe (un ID externe) répertorié dans la section Accès de la page de configuration du point de terminaison. Si l'utilisateur ne fait partie d'aucun groupe, ou s'il fait partie de plusieurs groupes, il n'est pas autorisé à y accéder.

Travailler avec des fournisseurs d'identité personnalisés

Pour authentifier vos utilisateurs, vous pouvez utiliser votre fournisseur d'identité existant avec AWS Transfer Family. Vous intégrez votre fournisseur d'identité à l'aide d'une AWS Lambda fonction qui authentifie et autorise vos utilisateurs à accéder à Amazon S3 ou Amazon Elastic File System (AmazonEFS). Pour plus de détails, consultez [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#). Vous pouvez également accéder à CloudWatch des graphiques pour des indicateurs tels que le nombre de fichiers et d'octets transférés dans la console de AWS Transfer Family gestion, ce qui vous permet de surveiller les transferts de fichiers à l'aide d'un tableau de bord centralisé.

Vous pouvez également fournir une RESTful interface avec une seule méthode Amazon API Gateway. Transfer Family utilise cette méthode pour se connecter à votre fournisseur d'identité, qui authentifie et autorise vos utilisateurs à accéder à Amazon S3 ou Amazon EFS. Utilisez cette option si vous avez besoin d'API RESTful pour intégrer votre fournisseur d'identité ou si vous souhaitez tirer parti de ses capacités AWS WAF de blocage géographique ou de limitation de débit des demandes. Pour plus de détails, consultez [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#).

Dans les deux cas, vous pouvez créer un nouveau serveur à l'aide de la [AWS Transfer Family console](#) ou du [CreateServerAPI](#) opération.

Note

Vous pouvez participer à un atelier au cours duquel vous pouvez créer une solution de transfert de fichiers. Cette solution s'appuie sur les FTPS points de terminaison gérés SFTP et sur Amazon Cognito et DynamoDB AWS Transfer Family pour la gestion des utilisateurs. Vous pouvez consulter les détails de cet atelier [ici](#).

AWS Transfer Family propose les options suivantes pour travailler avec des fournisseurs d'identité personnalisés.

- **AWS Lambda** À utiliser pour connecter votre fournisseur d'identité : vous pouvez utiliser un fournisseur d'identité existant, soutenu par une fonction Lambda. Vous indiquez le nom de la fonction Lambda. Pour de plus amples informations, veuillez consulter [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#).
- Utilisez **Amazon API Gateway** pour connecter votre fournisseur d'identité : vous pouvez créer une méthode API Gateway basée sur une fonction Lambda à utiliser en tant que fournisseur d'identité. Vous fournissez un Amazon API Gateway URL et un rôle d'invocation. Pour de plus amples informations, veuillez consulter [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#).

Pour l'une ou l'autre option, vous pouvez également spécifier le mode d'authentification.

- **Mot de passe OU clé** : les utilisateurs peuvent s'authentifier à l'aide de leur mot de passe ou de leur clé. C'est la valeur par défaut.
- **Mot de passe ONLY** : les utilisateurs doivent fournir leur mot de passe pour se connecter.
- **Clé ONLY** : les utilisateurs doivent fournir leur clé privée pour se connecter.
- **ANDClé de mot de passe** : les utilisateurs doivent fournir leur clé privée et leur mot de passe pour se connecter. Le serveur vérifie d'abord la clé, puis si la clé est valide, le système demande un mot de passe. Si la clé privée fournie ne correspond pas à la clé publique stockée, l'authentification échoue.

Utilisation de plusieurs méthodes d'authentification pour vous authentifier auprès de votre fournisseur d'identité personnalisé

Le serveur Transfer Family contrôle la AND logique lorsque vous utilisez plusieurs méthodes d'authentification. Transfer Family traite cela comme deux demandes distinctes adressées à votre fournisseur d'identité personnalisé : toutefois, leur effet est combiné.

Les deux demandes doivent être renvoyées avec succès avec la bonne réponse pour permettre à l'authentification de se terminer. Transfer Family exige que les deux réponses soient complètes, c'est-à-dire qu'elles contiennent tous les éléments requis (rôle, répertoire personnel, politique et POSIX profil si vous utilisez Amazon EFS pour le stockage). Transfer Family exige également que la réponse au mot de passe ne contienne pas de clés publiques.

La demande de clé publique doit faire l'objet d'une réponse distincte de la part du fournisseur d'identité. Ce comportement reste inchangé lors de l'utilisation du mot de passe OR ou de la AND clé de passe.

Le SFTP protocoleSSH/défie d'abord le client logiciel avec une authentification par clé publique, puis demande une authentification par mot de passe. Cette opération garantit la réussite des deux opérations avant que l'utilisateur ne soit autorisé à terminer l'authentification.

Rubriques

- [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#)
- [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#)

Utilisation AWS Lambda pour intégrer votre fournisseur d'identité

Créez une AWS Lambda fonction qui se connecte à votre fournisseur d'identité personnalisé. Vous pouvez utiliser n'importe quel fournisseur d'identité personnalisé, tel qu'Okta, Secrets Manager OneLogin, ou un magasin de données personnalisé incluant une logique d'autorisation et d'authentification.

Note

Avant de créer un serveur Transfer Family qui utilise Lambda comme fournisseur d'identité, vous devez créer la fonction. Pour obtenir un exemple de fonction Lambda, veuillez consulter [Exemples de fonctions Lambda](#). Vous pouvez également déployer une CloudFormation pile qui utilise l'un des [Modèles de fonctions Lambda](#). Assurez-vous également que votre fonction Lambda utilise une politique basée sur les ressources qui fait confiance à Transfer Family. Pour un exemple de politique, consultez [Politique basée sur les ressources Lambda](#).

1. Ouvrez la [AWS Transfer Family console](#).
2. Choisissez Create server pour ouvrir la page Create server. Pour Choisir un fournisseur d'identité, choisissez le fournisseur d'identité personnalisé, comme illustré dans la capture d'écran suivante.

Choose an identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type

An identity provider manages user access for authentication and authorization

☐ Service managed

Create and manage users within the service

☐ AWS Directory Service [Info](#)

Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ Custom Identity Provider [Info](#)

Manage users by integrating an identity provider of your choice

☒ Use AWS Lambda to connect your identity provider [Info](#)

Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)

Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

Choose a Lambda function



Authentication methods

Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel

Previous

Next

Note

Le choix des méthodes d'authentification n'est disponible que si vous les activez SFTP comme l'un des protocoles de votre serveur Transfer Family.

3. Assurez-vous que la valeur par défaut, Utiliser AWS Lambda pour connecter votre fournisseur d'identité, est sélectionnée.
4. Pour AWS Lambda fonction, choisissez le nom de votre fonction Lambda.

5. Remplissez les cases restantes, puis choisissez **Create server**. Pour plus de détails sur les étapes restantes de création d'un serveur, consultez [Configuration d'un point SFTP de FTPS terminaison ou d'FTPun serveur](#).

Politique basée sur les ressources Lambda

Vous devez disposer d'une politique qui fait référence au serveur Transfer Family et à LambdaARNs. Par exemple, vous pouvez utiliser la politique suivante avec votre fonction Lambda qui se connecte à votre fournisseur d'identité. La politique est échappée JSON sous forme de chaîne.

```
"Policy":
"{
  "Version": "2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "AllowTransferInvocation",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:transfer:region:account-id:function:my-lambda-auth-  
function",
      "Condition": {
        "ArnLike": {
          "AWS:SourceArn": "arn:aws:transfer:region:account-id:server/server-id"
        }
      }
    }
  ]
}"
```

Note

Dans l'exemple de politique ci-dessus, remplacez chaque *user input placeholder* avec vos propres informations.

Structure des messages d'événements

La structure du message d'événement envoyé par le SFTP serveur à la fonction Lambda d'autorisation pour une IDP personnalisation est la suivante.

```
{
  'username': 'value',
  'password': 'value',
  'protocol': 'SFTP',
  'serverId': 's-abcd123456',
  'sourceIp': '192.168.0.100'
}
```

Où username et password quelles sont les valeurs des informations de connexion envoyées au serveur.

Par exemple, vous entrez la commande suivante pour vous connecter :

```
sftp bobusa@server_hostname
```

Vous êtes ensuite invité à saisir votre mot de passe :

```
Enter password:
mysecretpassword
```

Vous pouvez le vérifier à partir de votre fonction Lambda en imprimant l'événement transmis depuis la fonction Lambda. Il doit ressembler au bloc de texte suivant.

```
{
  'username': 'bobusa',
  'password': 'mysecretpassword',
  'protocol': 'SFTP',
  'serverId': 's-abcd123456',
  'sourceIp': '192.168.0.100'
}
```

La structure de l'événement est similaire pour FTP et FTPS : la seule différence est que les valeurs sont utilisées pour le protocol paramètre, plutôt queSFTP.

Fonctions Lambda pour l'authentification

Pour implémenter différentes stratégies d'authentification, modifiez la fonction Lambda. Pour répondre aux besoins de votre application, vous pouvez déployer une CloudFormation pile. Pour plus d'informations sur Lambda, consultez le [guide du AWS Lambda développeur](#) ou la création de fonctions [Lambda](#) avec Node.js.

Rubriques

- [Modèles de fonctions Lambda](#)
- [Valeurs Lambda valides](#)
- [Exemples de fonctions Lambda](#)
- [Tester votre configuration](#)

Modèles de fonctions Lambda

Vous pouvez déployer une AWS CloudFormation pile qui utilise une fonction Lambda pour l'authentification. Nous proposons plusieurs modèles qui authentifient et autorisent vos utilisateurs à l'aide de leurs identifiants de connexion. Vous pouvez modifier ces modèles ou ce AWS Lambda code pour personnaliser davantage l'accès des utilisateurs.

Note

Vous pouvez créer un FIPS AWS Transfer Family serveur compatible AWS CloudFormation en spécifiant une politique de sécurité FIPS activée dans votre modèle. Les politiques de sécurité disponibles sont décrites dans [Politiques de sécurité pour AWS Transfer Family](#)

Pour créer une AWS CloudFormation pile à utiliser pour l'authentification

1. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Suivez les instructions pour déployer une AWS CloudFormation pile à partir d'un modèle existant dans la section [Sélection d'un modèle de pile](#) dans le guide de AWS CloudFormation l'utilisateur.
3. Utilisez l'un des modèles suivants pour créer une fonction Lambda à utiliser pour l'authentification dans Transfer Family.
 - [Modèle de pile classique \(Amazon Cognito\)](#)

Un modèle de base pour créer un AWS Lambda à utiliser en tant que fournisseur d'identité personnalisé dans AWS Transfer Family. Il s'authentifie auprès d'Amazon Cognito pour l'authentification par mot de passe et les clés publiques sont renvoyées depuis un compartiment Amazon S3 si l'authentification par clé publique est utilisée. Après le déploiement, vous pouvez modifier le code de la fonction Lambda pour faire quelque chose de différent.

- [AWS Secrets Manager modèle de pile](#)

Modèle de base à utiliser AWS Lambda avec un AWS Transfer Family serveur pour intégrer Secrets Manager en tant que fournisseur d'identité. Il s'authentifie par le biais d'une entrée au AWS Secrets Manager format `aws/transfer/server-id/username`. En outre, le secret doit contenir les paires clé-valeur pour toutes les propriétés utilisateur renvoyées à Transfer Family. Après le déploiement, vous pouvez modifier le code de la fonction Lambda pour faire quelque chose de différent.

- Modèle de [pile Okta : modèle](#) de base utilisé AWS Lambda avec un AWS Transfer Family serveur pour intégrer Okta en tant que fournisseur d'identité personnalisé.
- Modèle de [pile Okta-MFA : modèle](#) de base utilisé AWS Lambda avec un AWS Transfer Family serveur pour intégrer Okta, avec MultiFactor Authentication, en tant que fournisseur d'identité personnalisé.
- [Modèle Azure Active Directory](#) : les détails de cette pile sont décrits dans le billet de blog [Authentication to AWS Transfer Family with Azure Active Directory et AWS Lambda](#).

Une fois la pile déployée, vous pouvez consulter les détails la concernant dans l'onglet Sorties de la CloudFormation console.

Le déploiement de l'une de ces piles est le moyen le plus simple d'intégrer un fournisseur d'identité personnalisé dans le flux de travail Transfer Family.

Valeurs Lambda valides

Le tableau suivant décrit en détail les valeurs acceptées par Transfer Family pour les fonctions Lambda utilisées par les fournisseurs d'identité personnalisés.

Valeur	Description	Obligatoire
Role	Spécifie le nom de ressource Amazon (ARN) du IAM rôle qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre système de EFS fichiers Amazon S3 ou Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs. Pour plus de détails sur l'établissement d'une relation de confiance, voir Étape 1 : Établir une relation d'approbation.	Obligatoire
PosixProfile	L'POSIXidentité complète, y compris l'ID utilisateur (Uid), l'ID de groupe (Gid) et tout groupe secondaire IDs (SecondaryGids), qui contrôle l'accès de vos utilisateurs à vos systèmes	Nécessaire pour le stockage de EFS sauvegarde sur Amazon

Valeur	Description	Obligatoire
	de EFS fichiers Amazon. Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.	
PublicKeys	Liste des valeurs de clé SSH publique valides pour cet utilisateur. Une liste vide indique qu'il ne s'agit pas d'un identifiant valide. Ne doit pas être renvoyé lors de l'authentification du mot de passe.	Facultatif
Policy	Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même IAM rôle pour plusieurs utilisateurs. Cette stratégie étend l'accès de l'utilisateur à des parties de son compartiment Amazon S3.	Facultatif

Valeur	Description	Obligatoire
HomeDirectoryType	Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. • Si vous le définissez surPATH, l'utilisateur voit le bucket Amazon S3 absolu ou les EFS chemins Amazon tels quels dans leurs clients de protocole de transfert de fichiers. • Si vous le définissez surLOGICAL, vous devez fournir des mappages dans le HomeDirectoryDetails paramètre afin que les EFS chemins Amazon S3 ou Amazon soient visibles pour vos utilisateurs.	Facultatif

Valeur	Description	Obligatoire
HomeDirectoryDetails	Des mappages de répertoires logiques qui spécifient quels EFS chemins et clés Amazon S3 ou Amazon doivent être visibles par votre utilisateur et comment vous souhaitez les rendre visibles. Vous devez spécifier la Target paire Entry et, qui Entry indique comment le chemin est rendu visible et Target correspond au EFS chemin Amazon S3 ou Amazon réel.	Obligatoire s'HomeDirectoryType il a une valeur de LOGICAL
HomeDirectory	Le répertoire de destination d'un utilisateur lorsqu'il se connecte au serveur à l'aide du client.	Facultatif

Note

HomeDirectoryDetail est une représentation sous forme de chaîne d'une JSON carte. Cela contraste avec un objet JSON cartographique réel et PublicKeys un JSON tableau de chaînes. Consultez les exemples de code pour les détails spécifiques au langage.

Exemples de fonctions Lambda

Cette section présente quelques exemples de fonctions Lambda, à la fois en NodeJS et en Python.

Note

Dans ces exemples, les détails de l'utilisateur, du rôle, du POSIX profil, du mot de passe et du répertoire de base sont tous des exemples et doivent être remplacés par vos valeurs réelles.

Logical home directory, NodeJS

[L'exemple de fonction NodeJS suivant fournit les informations relatives à un utilisateur disposant d'un répertoire de base logique.](#)

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
  check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
    ];
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
      authenticated if and only if the Role field is not blank
      PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
      not needed for S3
      HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
      HomeDirectoryType: "LOGICAL",
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
    }
    // Check if password is correct
  }
```

```

    } else if (event.password !== 'Password1234') {
        // Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {};
    }
} else {
    // Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {};
}
callback(null, response);
};

```

Path-based home directory, NodeJS

L'exemple de fonction NodeJS suivant fournit les informations relatives à un utilisateur qui possède un répertoire de base basé sur un chemin.

```

// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
    console.log("Username:", event.username, "ServerId: ", event.serverId);

    var response;
    // Check if the username presented for authentication is correct. This doesn't
    check the value of the server ID, only that it is provided.
    // There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    (e.g., "127.0.0.1") to further restrict logins.
    if (event.serverId !== "" && event.username == 'example-user') {
        response = {
            Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
            authenticated if and only if the Role field is not blank
            Policy: '', // Optional, JSON stringified blob to further restrict this user's
            permissions
            HomeDirectory: '/fs-faa1a123' // Not required, defaults to '/'
        };

        // Check if password is provided
        if (!event.password) {
            // If no password provided, return the user's SSH public key
            response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
            // Check if password is correct

```

```

    } else if (event.password !== 'Password1234') {
        // Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {};
    }
} else {
    // Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {};
}
callback(null, response);
};

```

Logical home directory, Python

L'exemple de fonction Python suivant fournit les informations relatives à un utilisateur disposant d'un [répertoire de base logique](#).

```

# GetUserConfig Python Lambda with LOGICAL HomeDirectoryDetails
import json

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    # check the value of the server ID, only that it is provided.
    if event['serverId'] != '' and event['username'] == 'example-user':
        homeDirectoryDetails = [
            {
                'Entry': '/',
                'Target': '/fs-faa1a123'
            }
        ]
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            # be authenticated if and only if the Role field is not blank
            'PosixProfile': {"Gid": 65534, "Uid": 65534}, # Required for EFS access, but
            # not needed for S3
            'HomeDirectoryDetails': json.dumps(homeDirectoryDetails),
            'HomeDirectoryType': "LOGICAL"
        }
    }

```

```

# Check if password is provided
if event.get('password', '') == '':
    # If no password provided, return the user's SSH public key
    response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789" ]
# Check if password is correct
elif event['password'] != 'Password1234':
    # Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {}
else:
    # Return HTTP status 200 but with no role in the response to indicate
    authentication failure
    response = {}

return response

```

Path-based home directory, Python

L'exemple de fonction Python suivant fournit les informations relatives à un utilisateur qui possède un répertoire de base basé sur un chemin.

```

# GetUserConfig Python Lambda with PATH HomeDirectory

def lambda_handler(event, context):
    print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

    response = {}

    # Check if the username presented for authentication is correct. This doesn't
    # check the value of the server ID, only that it is provided.
    # There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
    # (e.g., "127.0.0.1") to further restrict logins.
    if event['serverId'] != '' and event['username'] == 'example-user':
        response = {
            'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
            # be authenticated if and only if the Role field is not blank
            'Policy': '', # Optional, JSON stringified blob to further restrict this
            # user's permissions
            'HomeDirectory': '/fs-fs-faa1a123',
            'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH
        }

```



```
# Check if password is provided
if event.get('password', '') == '':
    # If no password provided, return the user's SSH public key
    response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}
    else:
        # Return HTTP status 200 but with no role in the response to indicate
        authentication failure
        response = {}

return response
```

Tester votre configuration

Après avoir créé votre fournisseur d'identité personnalisé, vous devez tester votre configuration.

Console

Pour tester votre configuration à l'aide de la AWS Transfer Family console

1. Ouvrez la [AWS Transfer Family console](#).
2. Sur la page Serveurs, choisissez votre nouveau serveur, sélectionnez Actions, puis sélectionnez Test.
3. Entrez le texte du nom d'utilisateur et du mot de passe que vous avez définis lors du déploiement de la AWS CloudFormation pile. Si vous avez conservé les options par défaut, le nom d'utilisateur est myuser et le mot de passe est MySuperSecretPassword.
4. Choisissez le protocole du serveur et entrez l'adresse IP de l'adresse IP source, si vous les avez définies lors du déploiement de la AWS CloudFormation pile.

CLI

Pour tester votre configuration à l'aide du AWS CLI

1. Exécutez la commande [test-identity-provider](#). Remplacez chacune *user input placeholder* par vos propres informations, comme décrit dans les étapes suivantes.

```
aws transfer test-identity-provider --server-id s-1234abcd5678efgh --user-name myuser --user-password MySuperSecretPassword --server-protocol FTP --source-ip 127.0.0.1
```

2. Entrez l'ID du serveur.
3. Entrez le nom d'utilisateur et le mot de passe que vous avez définis lors du déploiement de la AWS CloudFormation pile. Si vous avez conservé les options par défaut, le nom d'utilisateur est myuser et le mot de passe est MySuperSecretPassword.
4. Entrez le protocole du serveur et l'adresse IP source, si vous les avez définis lors du déploiement de la AWS CloudFormation pile.

Si l'authentification de l'utilisateur réussit, le test renvoie une `StatusCode: 200` HTTP réponse, une chaîne vide `Message: ""` (qui contiendrait la raison de l'échec dans le cas contraire) et un `Response` champ.

Note

Dans l'exemple de réponse ci-dessous, le `Response` champ est un JSON objet « stringifié » (converti en JSON chaîne plate utilisable dans un programme) et contient les détails des rôles et autorisations de l'utilisateur.

```
{
  "Response": "{\\\"Policy\\\":\\\"{\\\"Version\\\":\\\"2012-10-17\\\",\\\"Statement\\\":[\\\"{\\\"Sid\\\":\\\"ReadAndListAllBuckets\\\",\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\\":[\\\"s3:ListAllMybuckets\\\",\\\"s3:GetBucketLocation\\\",\\\"s3:ListBucket\\\",\\\"s3:GetObjectVersion\\\",\\\"s3:GetObjectVersion\\\"]\\\",\\\"Resource\\\":\\\"*\\\"}]}\\\",\\\"Role\\\":\\\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\\\",\\\"HomeDirectory\\\":\\\"/\\\"}\\\"\",
  \"StatusCode\": 200,
  \"Message\": \"\"
}
```

Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité

Cette rubrique décrit comment utiliser une AWS Lambda fonction pour sauvegarder une méthode API Gateway. Utilisez cette option si vous avez besoin d'RESTfulAPIintégrer votre fournisseur d'identité ou si vous souhaitez tirer parti de ses capacités AWS WAF de blocage géographique ou de limitation de débit des demandes.

Limitations liées à l'utilisation d'une API passerelle pour intégrer votre fournisseur d'identité

- Cette configuration ne prend pas en charge les domaines personnalisés.
- Cette configuration ne prend pas en charge une API passerelle privéeURL.

Si vous avez besoin de l'une ou l'autre de ces options, vous pouvez utiliser Lambda comme fournisseur d'identité, sans API Gateway. Pour plus de détails, consultez [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#).

Authentification à l'aide d'une méthode API Gateway

Vous pouvez créer une méthode API Gateway à utiliser en tant que fournisseur d'identité pour Transfer Family. Cette approche constitue un moyen hautement sécurisé de créer et de fournirAPIs. Avec API Gateway, vous pouvez créer un HTTPS point de terminaison afin que tous les API appels entrants soient transmis avec une plus grande sécurité. Pour plus de détails sur le service API Gateway, consultez le [guide du développeur API Gateway](#).

APIGateway propose une méthode d'autorisation nomméeAWS_IAM, qui vous donne la même authentification basée sur AWS Identity and Access Management (IAM) que celle AWS utilisée en interne. Si vous activez l'authentification avecAWS_IAM, seuls les appelants disposant d'autorisations explicites pour appeler et API peuvent accéder à cette API méthode API Gateway.

Pour utiliser votre méthode API Gateway en tant que fournisseur d'identité personnalisé pour Transfer Family, activez IAM votre méthode API Gateway. Dans le cadre de ce processus, vous fournissez un IAM rôle avec des autorisations permettant à Transfer Family d'utiliser votre passerelle.

Note

Pour améliorer la sécurité, vous pouvez configurer un pare-feu pour applications Web. AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les HTTPS demandes HTTP et les demandes qui sont transmises à Amazon API Gateway. Pour plus de détails, consultez [Ajouter un pare-feu pour applications Web](#).

Pour utiliser votre méthode API Gateway pour une authentification personnalisée avec Transfer Family

1. Créez une AWS CloudFormation pile. Pour cela :

Note

Les modèles de pile ont été mis à jour pour utiliser des mots de passe BASE64 codés : pour plus de détails, voir [Améliorations apportées aux AWS CloudFormation modèles](#).

- a. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
- b. Suivez les instructions pour déployer une AWS CloudFormation pile à partir d'un modèle existant dans la section [Sélection d'un modèle de pile](#) dans le guide de AWS CloudFormation l'utilisateur.
- c. Utilisez l'un des modèles de base suivants pour créer une méthode API Gateway basée sur AWS Lambda-backed à utiliser en tant que fournisseur d'identité personnalisé dans Transfer Family.

- [Modèle de pile de base](#)

Par défaut, votre méthode API Gateway est utilisée en tant que fournisseur d'identité personnalisé pour authentifier un seul utilisateur sur un seul serveur à l'aide d'une clé ou d'un mot de passe codé en dur SSH (Secure Shell). Après le déploiement, vous pouvez modifier le code de la fonction Lambda pour faire quelque chose de différent.

- [AWS Secrets Manager modèle de pile](#)

Par défaut, votre méthode API Gateway s'authentifie par rapport à une entrée du format `aws/transfer/server-id/username` Secrets Manager. En outre, le secret doit contenir les paires clé-valeur pour toutes les propriétés utilisateur renvoyées à Transfer Family. Après le déploiement, vous pouvez modifier le code de la fonction Lambda pour faire quelque chose de différent. Pour plus d'informations, consultez le billet de blog [Activer l'authentification par mot de passe pour AWS Transfer Family l'utilisation AWS Secrets Manager](#).

- [Modèle Okta Stack](#)

Votre méthode API Gateway s'intègre à Okta en tant que fournisseur d'identité personnalisé dans Transfer Family. Pour plus d'informations, consultez le billet de blog [Utiliser Okta comme fournisseur d'identité avec AWS Transfer Family](#).

Le déploiement de l'une de ces piles est le moyen le plus simple d'intégrer un fournisseur d'identité personnalisé dans le flux de travail Transfer Family. Chaque pile utilise la fonction Lambda pour prendre en charge votre API méthode basée sur API Gateway. Vous pouvez ensuite utiliser votre API méthode en tant que fournisseur d'identité personnalisé dans Transfer Family. Par défaut, la fonction Lambda authentifie un seul utilisateur appelé `myuser` avec un mot de passe de `MySuperSecretPassword`. Après le déploiement, vous pouvez modifier ces informations d'identification ou mettre à jour le code de fonction Lambda pour faire quelque chose de différent.

 Important

Nous vous recommandons de modifier les informations d'identification de l'utilisateur et du mot de passe par défaut.

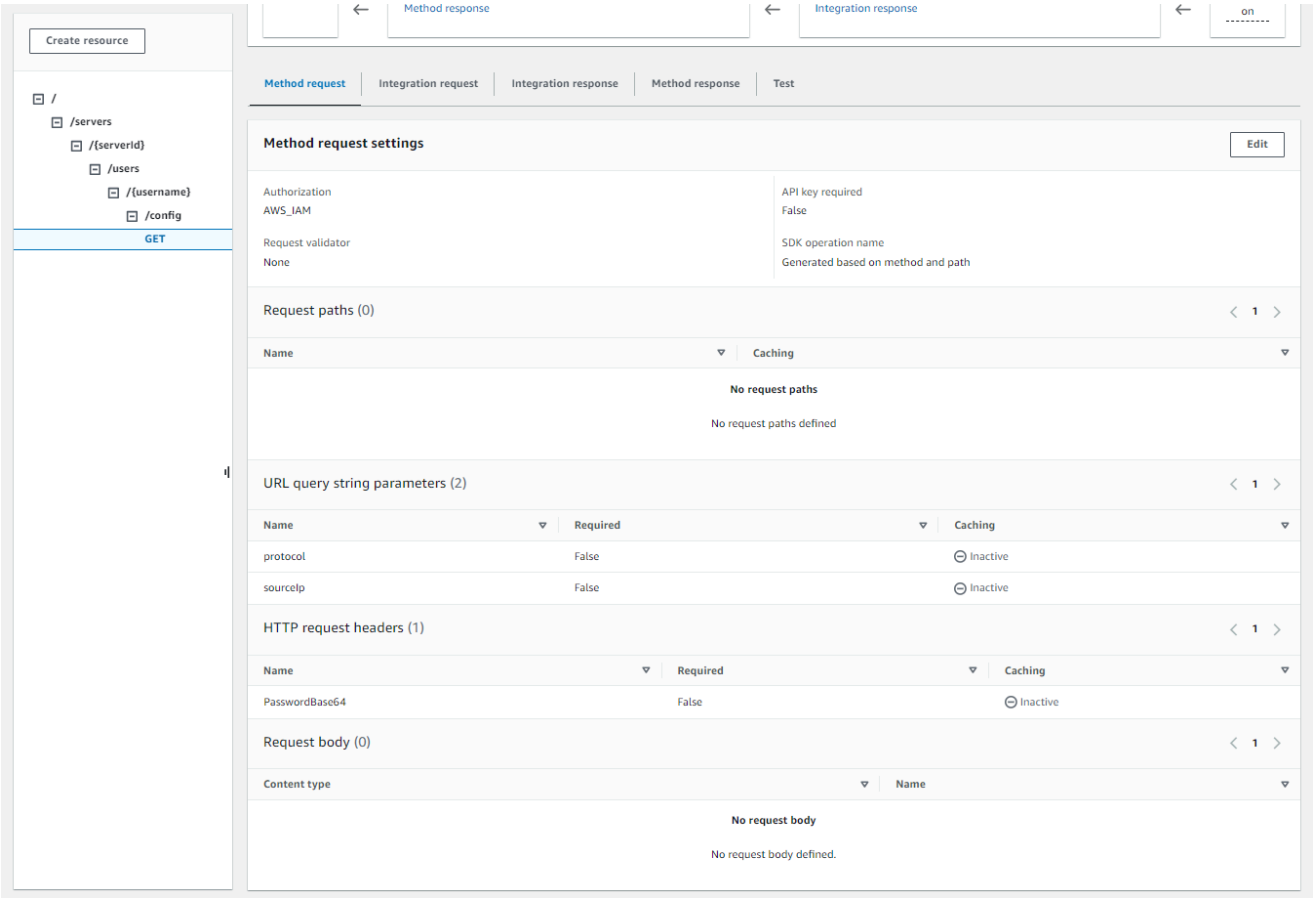
Une fois la pile déployée, vous pouvez consulter les détails la concernant dans l'onglet Sorties de la CloudFormation console. Ces informations incluent le nom de ressource Amazon de la pile (ARN), le ARN IAM rôle créé par la pile et le rôle URL de votre nouvelle passerelle.

 Note

Si vous utilisez l'option de fournisseur d'identité personnalisé pour activer l'authentification par mot de passe pour vos utilisateurs, et si vous activez l'enregistrement des demandes et des réponses fourni par API Gateway, API Gateway enregistre les mots de passe de vos utilisateurs dans vos Amazon Logs. CloudWatch Nous vous déconseillons d'utiliser ce journal dans votre environnement de production. Pour plus d'informations, consultez la section [Configurer la CloudWatch API connexion à API Gateway](#) dans le guide du développeur de API Gateway.

2. Vérifiez la configuration de la méthode API Gateway pour votre serveur. Pour cela :
 - a. Ouvrez la console API Gateway à l'adresse <https://console.aws.amazon.com/apigateway/>.

- b. Choisissez le modèle API de base Transfer Custom Identity Provider généré par le AWS CloudFormation modèle. Vous devrez peut-être sélectionner votre région pour voir vos passerelles.
- c. Dans le volet Ressources, choisissez GET. La capture d'écran suivante montre la configuration correcte de la méthode.



- À ce stade, votre API passerelle est prête à être déployée.
3. Pour Actions, sélectionnez Déployer API. Pour l'étape de déploiement, choisissez prod, puis Deploy.
- Une fois la méthode API Gateway déployée avec succès, visualisez ses performances dans Stages > Détails de l'étape, comme illustré dans la capture d'écran suivante.

Note

Copiez l'URL d'adresse Invoke qui apparaît en haut de l'écran. Vous en aurez peut-être besoin pour l'étape suivante.

The screenshot shows the AWS API Gateway console for a stage named 'prod'. The 'Stage details' section includes the following information:

Field	Value
Stage name	prod
Rate	10000
API cache	Inactive
Burst	5000
Web ACL	-
Client certificate	-
Invoke URL	https://[redacted].execute-api.us-east-1.amazonaws.com/prod

The 'Invoke URL' is highlighted with a red box. Below this, the 'Active deployment' is shown as 't8aqrm on December 12, 2023, 10:49 (UTC-05:00)'. The 'Logs and tracing' section shows 'CloudWatch logs' as 'Error and info logs', 'Detailed metrics' as 'Inactive', and 'X-Ray tracing' as 'Inactive'. The 'Stage variables' section is empty, showing 'No variables associated with the stage.' and a 'Manage variables' button.

4. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
5. Une Transfer Family aurait dû être créée pour vous, lorsque vous avez créé la pile. Si ce n'est pas le cas, configurez votre serveur en suivant ces étapes.
 - a. Choisissez Create server pour ouvrir la page Create server. Pour Choisir un fournisseur d'identité, choisissez Personnalisé, puis sélectionnez Utiliser Amazon API Gateway pour vous connecter à votre fournisseur d'identité, comme illustré dans la capture d'écran ci-dessous.

Choose an identity provider

Identity provider

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory**
Service Info
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider**
Info
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** **Info**
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ **Use Amazon API Gateway to connect your identity provider** **Info**
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

Role
IAM role for the service to invoke your Amazon API Gateway URL

- b. Dans la zone de URL texte Provide an Amazon API Gateway, collez l'URL adresse Invoke du point de terminaison API Gateway que vous avez créé à l'étape 3 de cette procédure.
- c. Pour Rôle, choisissez le IAM rôle créé par le AWS CloudFormation modèle. Ce rôle permet à Transfer Family d'invoquer votre méthode de API passerelle.

Le rôle d'invocation contient le nom de AWS CloudFormation pile que vous avez sélectionné pour la pile que vous avez créée à l'étape 1. Il a le format suivant : *CloudFormation-stack-name-TransferIdentityProviderRole-ABC123DEF456GHI*.

- d. Remplissez les cases restantes, puis choisissez Create server. Pour plus de détails sur les étapes restantes de création d'un serveur, consultez [Configuration d'un point SFTP de FTPS terminaison ou d'FTP un serveur](#).

Implémentation de votre méthode API Gateway

Pour créer un fournisseur d'identité personnalisé pour Transfer Family, votre méthode API Gateway doit implémenter une méthode unique dont le chemin de ressource est de `/servers/serverId/users/username/config`. Les *username* valeurs *serverId* et proviennent du chemin de la RESTful ressource. Ajoutez également `sourceIp` et `protocol` tant que paramètres de chaîne de URL requête dans la demande de méthode, comme indiqué dans l'image suivante.

The screenshot displays the AWS API Gateway console for a specific resource. On the left, a tree view shows the hierarchy: `/` > `/servers` > `/servers/{serverId}` > `/servers/{serverId}/users` > `/servers/{serverId}/users/{username}` > `/servers/{serverId}/users/{username}/config`. The selected resource is `/servers/{serverId}/users/{username}/config` with the `GET` method.

The main panel shows the **Method request settings** for the `GET` method. The **Method request settings** section includes:

- Authorization:** AWS_IAM
- Request validator:** None
- API key required:** False
- SDK operation name:** Generated based on method and path

The **Request paths (0)** section is empty, indicating no request paths are defined.

The **URL query string parameters (2)** section shows two parameters:

Name	Required	Caching
protocol	False	Inactive
sourceIp	False	Inactive

Note

Le nom d'utilisateur doit comporter au minimum 3 caractères et au maximum 100 caractères. Vous pouvez utiliser les caractères suivants dans le nom d'utilisateur : `a—z`, `A—Z`, `0—9`, trait de soulignement (`_`), tiret (`-`), point (`.`) et signe arobase (`@`). Toutefois, le nom d'utilisateur ne peut pas commencer par un tiret (`-`), un point (`.`) ou un signe (`@`).

Si Transfer Family tente d'authentifier votre utilisateur par mot de passe, le service fournit un champ d'`Password:en-tête`. En l'absence d'`Password:en-tête`, Transfer Family tente de s'authentifier par clé publique pour authentifier votre utilisateur.

Lorsque vous utilisez un fournisseur d'identité pour authentifier et autoriser les utilisateurs finaux, en plus de valider leurs informations d'identification, vous pouvez autoriser ou refuser les demandes d'accès en fonction des adresses IP des clients utilisés par vos utilisateurs finaux. Vous pouvez utiliser cette fonctionnalité pour garantir que les données stockées dans vos compartiments S3 ou dans votre système de EFS fichiers Amazon ne sont accessibles via les protocoles pris en charge qu'à partir d'adresses IP que vous avez spécifiées comme fiables. Pour activer cette fonctionnalité, vous devez inclure `sourceIp` dans la chaîne de requête.

Si plusieurs protocoles sont activés pour votre serveur et que vous souhaitez fournir un accès en utilisant le même nom d'utilisateur sur plusieurs protocoles, vous pouvez le faire à condition que les informations d'identification spécifiques à chaque protocole aient été configurées dans votre fournisseur d'identité. Pour activer cette fonctionnalité, vous devez inclure la *protocol* valeur dans le chemin de la RESTful ressource.

Votre méthode API Gateway doit toujours renvoyer le code HTTP d'état 200. Tout autre code d'HTTP état signifie qu'une erreur s'est produite lors de l'accès au API.

Exemple de réponse Amazon S3

Le corps de réponse d'exemple est un JSON document au format suivant pour Amazon S3.

```
{
  "Role": "IAM role with configured S3 permissions",
  "PublicKeys": [
    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "Policy": "STS Assume role session policy",
  "HomeDirectory": "/bucketName/path/to/home/directory"
}
```

Note

La politique est échappée JSON sous forme de chaîne. Par exemple :

```
"Policy":
```

```
"{
  \"Version\": \"2012-10-17\",
  \"Statement\":
    [
      {\"Condition\":
        {\"StringLike\":
          {\"s3:prefix\":
            [\"user/*\", \"user/\"]}},
        \"Resource\": \"arn:aws:s3:::bucket\",
        \"Action\": \"s3:ListBucket\",
        \"Effect\": \"Allow\",
        \"Sid\": \"ListHomeDir\"},
      {\"Resource\": \"arn:aws:s3:::*\",
        \"Action\": [\"s3:PutObject\",
          \"s3:GetObject\",
          \"s3:DeleteObjectVersion\",
          \"s3:DeleteObject\",
          \"s3:GetObjectVersion\",
          \"s3:GetObjectACL\",
          \"s3:PutObjectACL\"],
        \"Effect\": \"Allow\",
        \"Sid\": \"HomeDirObjectAccess\"}]
    ]
}"
```

L'exemple de réponse suivant montre qu'un utilisateur possède un type de répertoire de base logique.

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{\"Entry\": \"\\\", \"Target\": \"\\\"/MY-HOME-BUCKET\\\"}]\"",
  "PublicKeys": ["" ]
}
```

EFSExemple de réponse Amazon

Le corps de réponse de l'exemple est un JSON document du formulaire suivant pour AmazonEFS.

```
{
  "Role": "IAM role with configured EFS permissions",
  "PublicKeys": [
```

```

    "ssh-rsa public-key1",
    "ssh-rsa public-key2"
  ],
  "PosixProfile": {
    "Uid": "POSIX user ID",
    "Gid": "POSIX group ID",
    "SecondaryGids": [Optional list of secondary Group IDs],
  },
  "HomeDirectory": "/fs-id/path/to/home/directory"
}

```

Le `Role` champ indique que l'authentification a été réussie. Lors de l'authentification par mot de passe (lorsque vous fournissez un `Password` : en-tête), vous n'avez pas besoin de fournir de clés SSH publiques. Si un utilisateur ne peut pas être authentifié, par exemple si le mot de passe est incorrect, votre méthode doit renvoyer une réponse non `Role` définie. Un exemple d'une telle réponse est un JSON objet vide.

L'exemple de réponse suivant montre un utilisateur dont le type de répertoire de base est logique.

```

{
  "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectoryDetails": "[{"Entry": "\", \"Target": \"/faa1a123\"}]",
  "PublicKeys": [""],
  "PosixProfile": {"Uid": 65534, "Gid": 65534}
}

```

Vous pouvez inclure des politiques utilisateur dans la fonction Lambda au JSON format. Pour plus d'informations sur la configuration des politiques utilisateur dans Transfer Family, consultez [Gestion des contrôles d'accès](#).

Fonction Lambda par défaut

Pour implémenter différentes stratégies d'authentification, modifiez la fonction Lambda utilisée par votre passerelle. Pour vous aider à répondre aux besoins de votre application, vous pouvez utiliser les exemples de fonctions Lambda suivants dans le fichier `Node.js`. Pour plus d'informations sur Lambda, consultez le [guide du AWS Lambda développeur](#) ou la création de fonctions [Lambda](#) avec `Node.js`.

L'exemple de fonction Lambda suivant prend votre nom d'utilisateur, votre mot de passe (si vous effectuez une authentification par mot de passe), l'ID du serveur, le protocole et l'adresse IP du client.

Vous pouvez utiliser une combinaison de ces entrées pour rechercher votre fournisseur d'identité et déterminer si la connexion doit être acceptée.

 Note

Si plusieurs protocoles sont activés pour votre serveur et que vous souhaitez fournir un accès en utilisant le même nom d'utilisateur sur plusieurs protocoles, vous pouvez le faire à condition que les informations d'identification spécifiques au protocole aient été configurées dans votre fournisseur d'identité.

Pour le protocole de transfert de fichiers (FTP), nous vous recommandons de conserver des informations d'identification distinctes pour le protocole de transfert de fichiers Secure Shell (SSH/SFTP) et le protocole de transfert de fichiers sur SSL (FTPS). Nous vous recommandons de conserver des informations d'identification distinctes FTP car, contrairement à SFTP et FTPS, les FTP informations d'identification sont transmises en texte clair. En isolant les FTP informations d'identification de vos charges de travail SFTP ou FTPS, si FTP elles sont partagées ou exposées, en utilisant SFTP ou en préservant leur sécurité FTPS.

Cet exemple de fonction renvoie le rôle et les détails du répertoire de base logique, ainsi que les clés publiques (si elle effectue une authentification par clé publique).

Lorsque vous créez des utilisateurs gérés par des services, vous définissez leur répertoire de base, qu'il soit logique ou physique. De même, nous avons besoin des résultats de la fonction Lambda pour transmettre la structure de répertoire physique ou logique souhaitée par l'utilisateur. Les paramètres que vous définissez dépendent de la valeur du [HomeDirectoryType](#) champ.

- `HomeDirectoryType` défini sur `PATH` : le `HomeDirectory` champ doit alors être un préfixe de compartiment Amazon S3 absolu ou un chemin EFS absolu Amazon visible par vos utilisateurs.
- `HomeDirectoryType` set to `LOGICAL` — Ne définit aucun `HomeDirectory` champ. Au lieu de cela, nous avons défini un `HomeDirectoryDetails` champ qui fournit les mappages d'entrée/cible souhaités, similaires aux valeurs décrites dans le [HomeDirectoryDetails](#) paramètre pour les utilisateurs gérés par des services.

Les exemples de fonctions sont répertoriés dans [Exemples de fonctions Lambda](#).

Fonction Lambda à utiliser avec AWS Secrets Manager

Pour l'utiliser AWS Secrets Manager comme fournisseur d'identité, vous pouvez utiliser la fonction Lambda dans l'exemple de modèle AWS CloudFormation . La fonction Lambda interroge le service Secrets Manager avec vos informations d'identification et, en cas de succès, renvoie un secret désigné. Pour plus d'informations sur Secrets Manager, consultez le [Guide de l'utilisateur AWS Secrets Manager](#).

Pour télécharger un exemple de AWS CloudFormation modèle utilisant cette fonction Lambda, accédez au compartiment [Amazon S3 fourni par](#). AWS Transfer Family

Améliorations apportées aux AWS CloudFormation modèles

Des améliorations ont été apportées à l'interface API Gateway dans les CloudFormation modèles publiés. Les modèles utilisent désormais des mots de passe BASE64 codés avec la API passerelle. Vos déploiements existants continuent de fonctionner sans cette amélioration, mais n'autorisent pas les mots de passe contenant des caractères autres que le jeu de ASCII caractères américain de base.

Les modifications apportées au modèle pour activer cette fonctionnalité sont les suivantes :

- La `GetUserConfigRequest` `AWS::ApiGateway::Method` ressource doit avoir ce `RequestTemplates` code (la ligne en italique est la ligne mise à jour)

```
RequestTemplates:
  application/json: |
    {
      "username": "$util.urlDecode($input.params('username'))",
      "password":
        "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll('\\"', '\"')",
      "protocol": "$input.params('protocol')",
      "serverId": "$input.params('serverId')",
      "sourceIp": "$input.params('sourceIp')"
    }
```

- Le `RequestParameters` nom de la `GetUserConfig` ressource doit changer pour utiliser l'`PasswordBase64` en-tête (la ligne en italique est la ligne mise à jour) :

```
RequestParameters:
  method.request.header.PasswordBase64: false
  method.request.querystring.protocol: false
```

```
method.request.querystring.sourceIp: false
```

Pour vérifier si le modèle de votre stack est le plus récent

1. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Dans la liste des piles, choisissez votre pile.
3. Dans le panneau de détails, choisissez l'onglet Modèle.
4. Recherchez les éléments suivants :
 - Recherchez RequestTemplates cette ligne et assurez-vous que vous disposez de cette ligne :

```
"password":  
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(  
    \",\"\", \"'\", \"'\")",
```

- Recherchez RequestParameters cette ligne et assurez-vous que vous disposez de cette ligne :

```
method.request.header.PasswordBase64: false
```

Si les lignes mises à jour ne s'affichent pas, modifiez votre pile. Pour plus de détails sur la mise à jour de votre AWS CloudFormation pile, consultez la section [Modification d'un modèle de pile](#) dans le AWS CloudFormation guide de l'utilisateur.

Utilisation de répertoires logiques pour simplifier vos structures de répertoires Transfer Family

Pour simplifier la structure des répertoires de votre AWS Transfer Family serveur, vous pouvez utiliser des répertoires logiques. Avec les répertoires logiques, vous pouvez créer une structure de répertoire virtuel qui utilise des noms faciles à utiliser par vos utilisateurs lorsqu'ils se connectent à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Lorsque vous utilisez des répertoires logiques, vous pouvez éviter de divulguer les chemins de répertoire absolus, les noms des compartiments Amazon S3 et les noms des systèmes de EFS fichiers à vos utilisateurs finaux.

 Note

Bien que cela dépende de votre utilisation des politiques de session et d'autres exigences internes, vous n'avez généralement pas besoin à la fois de stratégies de session et de répertoires logiques pour garantir que vos utilisateurs accèdent uniquement aux fichiers que vous souhaitez qu'ils utilisent. Si vous configurez des répertoires logiques, ne créez pas également de politiques de session, car le fait de disposer des deux peut entraîner des erreurs de refus d'autorisation.

Vous pouvez utiliser des répertoires logiques pour placer le répertoire racine de l'utilisateur à l'emplacement souhaité dans votre hiérarchie de stockage, en effectuant ce que l'on appelle une chroot opération. Dans ce mode, les utilisateurs ne peuvent pas accéder à un répertoire en dehors du répertoire de base ou du répertoire racine que vous avez configuré pour eux.

Par exemple, bien qu'un utilisateur Amazon S3 ait été limité à l'accès uniquement `/mybucket/home/${transfer:UserName}`, certains clients autorisent les utilisateurs à parcourir un dossier vers `/mybucket/home` le haut. Dans ce cas, l'utilisateur revient sur le répertoire de base prévu uniquement après s'être déconnecté et reconnecté au serveur Transfer Family. L'exécution d'une chroot opération peut empêcher cette situation de se produire.

Vous pouvez créer votre propre structure de répertoire à partir de buckets et de préfixes. Cette fonctionnalité est utile si votre flux de travail attend une structure de répertoire spécifique que vous ne pouvez pas répliquer via des préfixes de compartiment. Vous pouvez également créer un lien vers plusieurs emplacements non contigus dans Amazon S3, comme pour créer un lien symbolique dans un système de fichiers Linux où le chemin de votre répertoire fait référence à un emplacement différent dans le système de fichiers.

 FILEMappages de répertoires logiques

Le type de `HomeDirectoryMapEntry` données inclut désormais un `Type` paramètre. Avant que ce paramètre n'existe, vous auriez pu créer un mappage de répertoire logique dont la cible était un fichier. Si vous avez déjà créé l'un de ces types de mappages de répertoires logiques, vous devez définir explicitement le `Type` `toFILE`, sinon ces mappages ne fonctionneront plus correctement à l'avenir.

Pour ce faire `UpdateUserAPI`, vous pouvez appeler le et définir le `Type` `to FILE` pour le mappage existant.

Règles d'utilisation des répertoires logiques

Avant de créer vos mappages de répertoires logiques, vous devez comprendre les règles suivantes :

- Dans Entry ce cas "/", vous ne pouvez avoir qu'un seul mappage car les chemins qui se chevauchent ne sont pas autorisés.
- Les répertoires logiques prennent en charge des mappages allant jusqu'à 2,1 Mo (pour les utilisateurs gérés par des services, cette limite est de 2 000 entrées). C'est-à-dire que la structure de données contenant les mappages a une taille maximale de 2,1 Mo. Si vous avez un grand nombre de mappages, vous pouvez calculer la taille de vos mappages comme suit :
 1. Rédigez un mappage type dans le format{"Entry": "/*entry-path*", "Target": "/*target-path*"}, où *entry-path* et *target-path* sont les valeurs réelles que vous allez utiliser.
 2. Comptez les caractères de cette chaîne, puis ajoutez-en un (1).
 3. Multipliez ce nombre par le nombre approximatif de mappages dont vous disposez pour votre serveur.

Si le nombre que vous avez estimé à l'étape 3 est inférieur à 2,1 Mo, vos mappages se situent dans la limite acceptable.

- Les cibles peuvent utiliser la `${transfer:UserName}` variable si le chemin du bucket ou du système de fichiers a été paramétré en fonction du nom d'utilisateur.
- Les cibles peuvent être des chemins situés dans différents compartiments ou systèmes de fichiers, mais vous devez vous assurer que le rôle mapped AWS Identity and Access Management (IAM) (le Role paramètre de la réponse) donne accès à ces compartiments ou systèmes de fichiers.
- Ne spécifiez pas le HomeDirectory paramètre, car cette valeur est implicite par les Entry Target paires lorsque vous utilisez la LOGICAL valeur du HomeDirectoryType paramètre.
- Les cibles doivent commencer par une barre oblique (/), mais n'utilisez pas de barre oblique (/) lorsque vous spécifiez le Target. Par exemple, `/DOC-EXAMPLE-BUCKET/images` c'est acceptable, mais `/DOC-EXAMPLE-BUCKET/images/` ne `DOC-EXAMPLE-BUCKET/images` l'est pas.
- Amazon S3 est un magasin d'objets, ce qui signifie que les dossiers sont un concept virtuel et qu'il n'existe aucune hiérarchie de répertoires réelle. Si votre application émet une stat opération depuis un client, tout est classé dans un fichier lorsque vous utilisez Amazon S3 pour le stockage. Ce comportement est décrit dans la section [Organisation des objets dans la console Amazon S3 à l'aide de dossiers](#) du guide de l'utilisateur d'Amazon Simple Storage Service. Si votre application

nécessite d'indiquer `stat` avec précision s'il s'agit d'un fichier ou d'un dossier, vous pouvez utiliser Amazon Elastic File System (AmazonEFS) comme option de stockage pour vos serveurs Transfer Family.

- Si vous spécifiez des valeurs de répertoire logiques pour votre utilisateur, le paramètre que vous utilisez dépend du type d'utilisateur :
 - Pour les utilisateurs gérés par des services, fournissez des valeurs de répertoire logiques dans `HomeDirectoryMappings`.
 - Pour les utilisateurs de fournisseurs d'identité personnalisés, fournissez des valeurs de répertoire logiques dans `HomeDirectoryDetails`.

Important

À moins que vous ne choisissiez d'optimiser les performances de vos annuaires Amazon S3 (lorsque vous créez ou mettez à jour un serveur), le répertoire racine doit exister au démarrage. Pour Amazon S3, cela signifie que vous devez déjà avoir créé un objet de zéro octet se terminant par une barre oblique (/) pour créer le dossier racine. Éviter ce problème est une raison pour envisager d'optimiser les performances d'Amazon S3.

Implémentation de répertoires logiques et **chroot**

Pour utiliser les répertoires et les `chroot` fonctionnalités logiques, vous devez effectuer les opérations suivantes :

Activez les répertoires logiques pour chaque utilisateur. Pour ce faire, définissez le `HomeDirectoryType` paramètre sur `LOGICAL` lorsque vous créez ou mettez à jour votre utilisateur.

```
"HomeDirectoryType": "LOGICAL"
```

chroot

Pour `chroot` créer une structure de répertoire composée d'un répertoire unique `Entry` et d'un `Target` appariement pour chaque utilisateur. Le dossier racine est le `Entry` point et l'`Target` emplacement de votre bucket ou de votre système de fichiers vers lequel mapper.

Exemple for Amazon S3

```
[{"Entry": "/", "Target": "/mybucket/jane"}]
```

Exemple for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

Vous pouvez utiliser un chemin absolu comme dans l'exemple précédent, ou vous pouvez utiliser une substitution dynamique pour le nom d'utilisateur par `${transfer:UserName}`, comme dans l'exemple suivant.

```
[{"Entry": "/", "Target":  
"/mybucket/${transfer:UserName}"]}]
```

Dans l'exemple précédent, l'utilisateur est verrouillé dans son répertoire racine et ne peut pas monter plus haut dans la hiérarchie.

Structure du répertoire virtuel

Pour une structure de répertoire virtuel, vous pouvez créer plusieurs Entry Target paires, avec des cibles n'importe où dans vos compartiments ou systèmes de fichiers S3, y compris dans plusieurs compartiments ou systèmes de fichiers, à condition que le mappage des IAM rôles de l'utilisateur soit autorisé à y accéder.

Dans l'exemple de structure virtuelle suivant, lorsque l'utilisateur se connecte AWS SFTP, il se trouve dans le répertoire racine avec les sous-répertoires `/pics`, `/doc/reporting`, et `/anotherpath/subpath/financials`.

Note

À moins que vous ne choisissiez d'optimiser les performances de vos annuaires Amazon S3 (lorsque vous créez ou mettez à jour un serveur), l'utilisateur ou un administrateur doit créer les annuaires s'ils n'existent pas déjà. Éviter ce problème est une raison pour envisager d'optimiser les performances d'Amazon S3.

Pour AmazonEFS, vous avez toujours besoin de l'administrateur pour créer les mappages logiques ou le / répertoire.

```
[  
{"Entry": "/pics", "Target": "/bucket1/pics"},  
{"Entry": "/doc", "Target": "/bucket1/anotherpath/docs"},  
{"Entry": "/reporting", "Target": "/reportingbucket/Q1"},  
{"Entry": "/anotherpath/subpath/financials", "Target": "/reportingbucket/financials"}]
```

Note

Vous ne pouvez télécharger des fichiers que dans les dossiers spécifiques que vous mappez. Cela signifie que dans l'exemple précédent, vous ne pouvez pas télécharger vers `/anotherpath` des `anotherpath/subpath` répertoires ; uniquement `anotherpath/subpath/financials`. Vous ne pouvez pas non plus mapper directement ces tracés, car les tracés qui se chevauchent ne sont pas autorisés.

Supposons, par exemple, que vous créez les mappages suivants :

```
{  
  "Entry": "/pics",  
  "Target": "/mybucket/pics"  
},  
{  
  "Entry": "/doc",  
  "Target": "/mybucket/mydocs"  
},  
{  
  "Entry": "/temp",  
  "Target": "/mybucket"  
}
```

Vous ne pouvez télécharger des fichiers que dans ces compartiments. Lorsque vous vous connectez pour la première fois `sftp`, vous êtes déposé dans le répertoire racine, `/`. Si vous essayez de télécharger un fichier dans ce répertoire, le téléchargement échoue. Les commandes suivantes présentent un exemple de séquence :

```
sftp> pwd  
Remote working directory: /  
sftp> put file  
Uploading file to /file  
remote open("/file"): No such file or directory
```

Pour télécharger vers n'importe quel fichier `directory/sub-directory`, vous devez mapper explicitement le chemin vers le `sub-directory`.

Pour plus d'informations sur la configuration des répertoires logiques et `chroot` pour vos utilisateurs, y compris un AWS CloudFormation modèle que vous pouvez télécharger et utiliser, consultez [Simplifier votre AWS SFTP structure avec un `chroot` et des répertoires logiques](#) dans le blog sur le AWS stockage.

Exemple de configuration de répertoires logiques

Dans cet exemple, nous créons un utilisateur et lui attribuons deux répertoires logiques. La commande suivante crée un nouvel utilisateur (pour un serveur Transfer Family existant) avec des répertoires logiques `pics` et `doc`.

```
aws transfer create-user --user-name marymajor-logical --server-id s-11112222333344445
--role arn:aws:iam::1234abcd5678:role/marymajor-role --home-directory-type LOGICAL \
--home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/DOC-EXAMPLE-BUCKET1/
pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-BUCKET2/test/mydocs\"}]" \
--ssh-public-key-body file://~/.ssh/id_rsa.pub
```

S'il s'agit d'un utilisateur existant et que son répertoire personnel est de type `PATH`, vous pouvez le remplacer `LOGICAL` par une commande similaire à la précédente.

```
aws transfer update-user --user-name marymajor-logical \
--server-id s-11112222333344445 --role arn:aws:iam::1234abcd5678:role/marymajor-role \
--home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/pics\",
\"Target\":\"/DOC-EXAMPLE-BUCKET1/pics\"}, \
{\"Entry\":\"/doc\", \"Target\":\"/DOC-EXAMPLE-BUCKET2/test/mydocs\"}]"
```

Notez ce qui suit :

- Si `/DOC-EXAMPLE-BUCKET1/pics` les répertoires `/DOC-EXAMPLE-BUCKET2/test/mydocs` n'existent pas déjà, l'utilisateur (ou un administrateur) doit les créer.
- Lorsqu'elle **marymajor** se connecte au serveur et exécute la `ls -l` commande, elle voit ce qui suit :

```
drwxr--r--  1      -      -      0 Mar 17 15:42 doc
```

```
drwxr--r--  1      -      -      0 Mar 17 16:04 pics
```

- **marymajor** Impossible de créer des fichiers ou des répertoires à ce niveau. Cependant, dans `pics` et `doc`, elle peut ajouter des sous-répertoires.
- Les fichiers qu'elle ajoute `pics` et `doc` sont ajoutés aux chemins Amazon S3 `/DOC-EXAMPLE-BUCKET1/pics` et `/DOC-EXAMPLE-BUCKET2/test/mydocs` respectivement.
- Dans cet exemple, nous indiquons deux compartiments différents pour illustrer cette possibilité. Toutefois, vous pouvez utiliser le même compartiment pour plusieurs ou tous les répertoires logiques que vous spécifiez pour l'utilisateur.

Configuration de répertoires logiques pour Amazon EFS

Si votre serveur Transfer Family utilise AmazonEFS, le répertoire personnel de l'utilisateur doit être créé avec un accès en lecture et en écriture pour que l'utilisateur puisse travailler dans son répertoire de base logique. L'utilisateur ne peut pas créer ce répertoire lui-même, car il n'aurait pas les autorisations nécessaires pour `mkdir` accéder à son répertoire de base logique.

Si le répertoire personnel de l'utilisateur n'existe pas et que celui-ci exécute une `ls` commande, le système répond comme suit :

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Un utilisateur disposant d'un accès administratif au répertoire parent doit créer le répertoire de base logique de l'utilisateur.

AWS Lambda Réponse personnalisée

Vous pouvez utiliser des répertoires logiques dotés d'une fonction Lambda qui se connecte à votre fournisseur d'identité personnalisé. Pour ce faire, dans votre fonction Lambda, vous spécifiez les Target valeurs `HomeDirectoryType` as **LOGICAL**, `add Entry` et pour le `HomeDirectoryDetails` paramètre. Par exemple :

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{\"Entry\": \"\\\", \"Target\": \"\\\"/DOC-EXAMPLE-BUCKET/
theRealFolder\"}]\"
```

Le code suivant est un exemple de réponse réussie à un appel d'authentification Lambda personnalisé.

```
aws transfer test-identity-provider --server-id s-1234567890abcdef0 --user-name myuser
{
  "Url": "https://a1b2c3d4e5.execute-api.us-east-2.amazonaws.com/prod/servers/
s-1234567890abcdef0/users/myuser/config",
  "Message": "",
  "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/bob-usa-role\",
\"HomeDirectoryType\": \"LOGICAL\", \"HomeDirectoryDetails\": \"[{\\\"Entry\\\":\\\"/
myhome\\\",\\\"Target\\\":\\\"/DOC-EXAMPLE-BUCKET/theRealFolder\\\"]}\\\", \"PublicKeys\":
\\\"[ssh-rsa myrsapubkey]\\\"\",
  \"StatusCode\": 200
}
```

Note

La "Url" : ligne n'est renvoyée que si vous utilisez une méthode API Gateway comme fournisseur d'identité personnalisé.

AWS Transfer Family SFTPconnecteurs

AWS Transfer Family SFTPles connecteurs établissent une relation pour l'envoi de fichiers et de messages entre le stockage Amazon et un partenaire externe, en utilisant le SFTP protocole. Vous pouvez envoyer des fichiers depuis Amazon S3 vers une destination externe appartenant à un partenaire. Vous pouvez également utiliser un SFTP connecteur pour récupérer des fichiers depuis le SFTP serveur d'un partenaire.

Note

Actuellement, les SFTP connecteurs ne peuvent être utilisés que pour se connecter à des SFTP serveurs distants qui offrent un point de terminaison accessible à Internet.

Consultez la [AWS Transfer Family SFTPsection Connectors](#) pour une brève présentation des SFTP connecteurs Transfer Family.

Rubriques

- [Configuration des SFTP connecteurs](#)
- [Envoyer et récupérer des fichiers à l'aide d'un SFTP connecteur](#)
- [Gérer les SFTP connecteurs](#)

Configuration des SFTP connecteurs

Cette rubrique décrit comment créer des SFTP connecteurs, les algorithmes de sécurité qui leur sont associés, comment stocker un secret pour conserver les informations d'identification, les détails sur le formatage de la clé privée et les instructions pour tester vos connecteurs.

Rubriques

- [Création d'un SFTP connecteur](#)
- [SFTPAlgorithmes de connexion](#)
- [Stockez un secret à utiliser avec un SFTP connecteur](#)
- [Génération et SFTP formatage de la clé privée du connecteur](#)
- [Tester un SFTP connecteur](#)

Création d'un SFTP connecteur

Cette procédure explique comment créer des SFTP connecteurs à l'aide de la AWS Transfer Family console ou AWS CLI.

Console

Pour créer un SFTP connecteur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Connectors, puis Create connector.
3. Choisissez SFTPLe type de connecteur pour créer un SFTP connecteur, puis choisissez Next.

Transfer Family > Connectors > Create connector

Create connector [Info](#)

Create a connector that will be used to connect to your trading partner's server

Choose the connector type
Choose the protocol of the remote server to create a connector

☒ **SFTP**
Create a connector to connect to remote SFTP server

☐ **AS2**
Create a connector to connect to your trading partner's AS2 server

Cancel **Next**

4. Dans la section Configuration du connecteur, fournissez les informations suivantes :
 - Pour le URL, entrez le URL pour un SFTP serveur distant. Cela URL doit être formaté commesftp://*partner-SFTP-server-url*, par exemplesftp://AnyCompany.com.

 Note

Vous pouvez éventuellement fournir un numéro de port dans votre URL. Le format est `sftp://partner-SFTP-server-url:port-number`. Le numéro de port par défaut (lorsqu'aucun port n'est spécifié) est le port 22.

- Pour le rôle Access, choisissez le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) à utiliser.
- Assurez-vous que ce rôle fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande.
- Assurez-vous que ce rôle autorise `secretsmanager:GetSecretValue` accès au secret.

 Note

Dans la politique, vous devez spécifier ARN le secret. ARN Contient le nom du secret, mais y ajoute six caractères alphanumériques aléatoires. Un ARN pour un secret a le format suivant.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Assurez-vous que ce rôle contient une relation de confiance qui permet au connecteur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs. Pour plus de détails sur l'établissement d'une relation de confiance, voir [Étape 1 : Établir une relation d'approbation](#).

L'exemple suivant accorde les autorisations nécessaires pour accéder au **DOC-EXAMPLE-BUCKET** dans Amazon S3, et le secret spécifié est stocké dans Secrets Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
```

```

        "s3:GetBucketLocation"
    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
    ]
},
{
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/SecretName-6RandomCharacters"
}
]
}

```

Note

Pour le rôle d'accès, l'exemple accorde l'accès à un secret unique. Toutefois, vous pouvez utiliser un caractère générique, ce qui peut vous faire économiser du travail si vous souhaitez réutiliser le même IAM rôle pour plusieurs utilisateurs et secrets. Par exemple, l'instruction de ressource suivante accorde des autorisations pour tous les secrets dont le nom commence par `aws/transfer`.

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

Vous pouvez également stocker des secrets contenant vos SFTP informations d'identification dans un autre Compte AWS. Pour plus de détails sur l'activation de l'accès secret entre comptes, voir [Autorisations relatives aux AWS Secrets Manager secrets pour les utilisateurs d'un autre compte](#).

- (Facultatif) Pour le rôle de journalisation, choisissez le IAM rôle que le connecteur doit utiliser pour transférer des événements vers vos CloudWatch journaux. L'exemple de politique suivant répertorie les autorisations nécessaires pour consigner les événements des SFTP connecteurs.

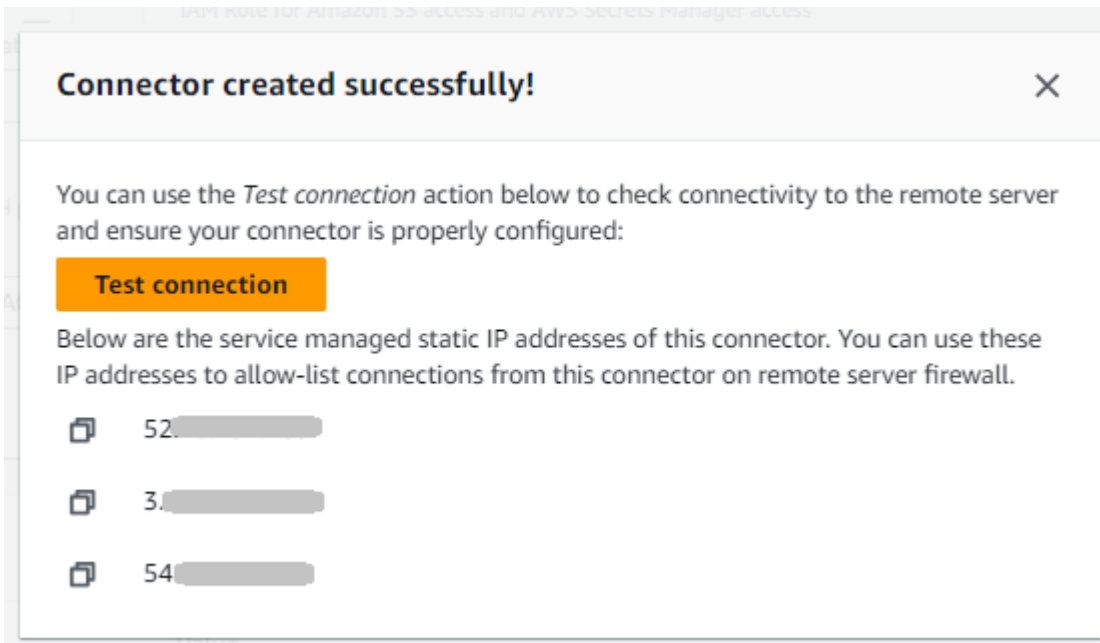
```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "SFTPConnectorPermissions",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    ]
  }]
}
```

5. Dans la section SFTPConfiguration, fournissez les informations suivantes :

- Pour les informations d'identification du Connector, dans la liste déroulante, choisissez le nom d'un secret AWS Secrets Manager contenant la clé privée ou le mot de passe de SFTP l'utilisateur. Vous devez créer un secret et le stocker d'une manière spécifique. Pour plus de détails, consultez [Stockez un secret à utiliser avec un SFTP connecteur](#).
- Clés d'hôte fiables : collez la partie publique de la clé d'hôte utilisée pour identifier le serveur externe. Vous pouvez ajouter plusieurs clés en choisissant Ajouter une clé d'hôte fiable pour ajouter une clé supplémentaire. Vous pouvez utiliser la ssh-keyscan

commande sur le SFTP serveur pour récupérer la clé nécessaire. Pour plus de détails sur le format et le type de clés d'hôte fiables prises en charge par Transfer Family, voir [SFTPConnectorConfig](#).

6. (Facultatif) Dans la section Balises, pour Clé et Valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur.
7. Après avoir confirmé tous vos paramètres, choisissez **Create connector** pour créer le SFTP connecteur. Si le connecteur est créé avec succès, un écran apparaît avec une liste des adresses IP statiques attribuées et un bouton **Tester la connexion**. Utilisez le bouton pour tester la configuration de votre nouveau connecteur.



La page Connecteurs apparaît, avec l'ID de votre nouveau SFTP connecteur ajouté à la liste. Pour consulter les détails de vos connecteurs, consultez [Afficher les détails SFTP du connecteur](#).

CLI

Vous utilisez le [create-connector](#) commande pour créer un connecteur. Pour utiliser cette commande afin de créer un SFTP connecteur, vous devez fournir les informations suivantes.

- Le URL pour un SFTP serveur distant. Cela URL doit être formaté comme `ftp://partner-SFTP-server-url`, par exemple `ftp://AnyCompany.com`.
- Le rôle d'accès. Choisissez le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) à utiliser.

- Assurez-vous que ce rôle fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande.
- Assurez-vous que ce rôle autorise `secretsmanager:GetSecretValue` accès au secret.

 Note

Dans la politique, vous devez spécifier ARN le secret. ARN Contient le nom du secret, mais y ajoute six caractères alphanumériques aléatoires. Un ARN pour un secret a le format suivant.

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- Assurez-vous que ce rôle contient une relation de confiance qui permet au connecteur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs. Pour plus de détails sur l'établissement d'une relation de confiance, voir [Étape 1 : Établir une relation d'approbation](#).

L'exemple suivant accorde les autorisations nécessaires pour accéder au *DOC-EXAMPLE-BUCKET* dans Amazon S3, et le secret spécifié est stocké dans Secrets Manager.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
```

```

        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
  },
  {
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/SecretName-6RandomCharacters"
  }
]
}

```

Note

Pour le rôle d'accès, l'exemple accorde l'accès à un secret unique. Toutefois, vous pouvez utiliser un caractère générique, ce qui peut vous faire économiser du travail si vous souhaitez réutiliser le même IAM rôle pour plusieurs utilisateurs et secrets. Par exemple, l'instruction de ressource suivante accorde des autorisations pour tous les secrets dont le nom commence par `aws/transfer/`.

```
"Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
```

Vous pouvez également stocker des secrets contenant vos SFTP informations d'identification dans un autre Compte AWS. Pour plus de détails sur l'activation de l'accès secret entre comptes, voir [Autorisations relatives aux AWS Secrets Manager secrets pour les utilisateurs d'un autre compte](#).

- (Facultatif) Choisissez le IAM rôle que le connecteur doit utiliser pour transférer des événements vers vos CloudWatch journaux. L'exemple de politique suivant répertorie les autorisations nécessaires pour consigner les événements des SFTP connecteurs.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "SFTPConnectorPermissions",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:CreateLogGroup",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    ]
  }]
}
```

- Fournissez les informations SFTP de configuration suivantes.
 - Le secret AWS Secrets Manager contenant ARN la clé privée ou le mot de passe de l'SFTPUtilisateur.
 - Partie publique de la clé d'hôte utilisée pour identifier le serveur externe. Vous pouvez fournir plusieurs clés d'hôte fiables si vous le souhaitez.

Le moyen le plus simple de fournir les SFTP informations est de les enregistrer dans un fichier. Par exemple, copiez le texte d'exemple suivant dans un fichier nommé `testSFTPConfig.json`.

```
// Listing for testSFTPConfig.json
{
  "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/transfer/example-username-key",
  "TrustedHostKeys": [
    "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
  ]
}
```


 Note

Il SecretId peut s'agir de l'intégralité ARN ou du nom du secret (*example-username-key* dans la liste précédente).

Exécutez ensuite la commande suivante pour créer le connecteur.

```
aws transfer create-connector --url "sftp://partner-SFTP-server-url" \  
--access-role your-IAM-role-for-bucket-access \  
--logging-role arn:aws:iam::your-account-id:role/service-role/  
AWSTransferLoggingAccess \  
--sftp-config file:///path/to/testSFTPConfig.json
```

SFTPalgorithmes de connexion

Lorsque vous créez un SFTP connecteur, les algorithmes de sécurité suivants sont attachés au connecteur.

Type	Algorithm
SSHchiffrer	aes256-gcm@openssh.com
	aes128-gcm@openssh.com
	aes256-ctr
	aes192-ctr
SSHméthode d'échange de clés (KEX)	curve25519-sha256
	curve25519-sha256@libssh.org
	diffie-hellman-group16-sha512
	diffie-hellman-group18-sha512
	diffie-hellman-group-exchange-sha256
SSH MAC	hmac-sha2-512-etm@openssh.com

Type	Algorithm
	hmac-sha2-256-etm@openssh.com
	hmac-sha2-512
	hmac-sha2-256
SSHclé d'hôte	ecdsa-sha2-nistp255
	ecdsa-sha2-nistp384
	ecdsa-sha2-nistp521
	rsa-sha2-512
	rsa-sha2-256

Stockez un secret à utiliser avec un SFTP connecteur

Vous pouvez utiliser Secrets Manager pour stocker les informations d'identification utilisateur de vos SFTP connecteurs. Lorsque vous créez votre secret, vous devez fournir un nom d'utilisateur. En outre, vous pouvez fournir un mot de passe, une clé privée ou les deux. Pour plus de détails, consultez [Quotas pour les SFTP connecteurs](#).

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](#).

Pour stocker les informations d'identification utilisateur dans le Gestionnaire des Secrets Manager d'un SFTP connecteur

1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Dans le volet de navigation de gauche, choisissez Secrets.
3. Sur la page Secrets, choisissez Enregistrer un nouveau secret.

4. Sur la page Choisir un type de secret, pour Type de secret, choisissez Autre type de secret.
5. Dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.
 - Clé — Entrée **Username**.
 - valeur — Entrez le nom de l'utilisateur autorisé à se connecter au serveur du partenaire.
6. Si vous souhaitez fournir un mot de passe, choisissez Ajouter une ligne, puis dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.

Choisissez Ajouter une ligne, puis dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.

- Clé — Entrée **Password**.
 - valeur — Entrez le mot de passe de l'utilisateur.
7. Si vous souhaitez fournir une clé privée, consultez [Génération et SFTP formatage de la clé privée du connecteur](#), qui décrit comment saisir des données de clé privée.

 Note

Les données de clé privée que vous entrez doivent correspondre à la clé publique enregistrée pour cet utilisateur sur le SFTP serveur distant.

8. Choisissez Suivant.
9. Sur la page Configurer le secret, entrez le nom et la description de votre secret. Nous vous recommandons d'utiliser le préfixe de **aws/transfer/** pour le nom. Par exemple, vous pourriez donner un nom à votre secret **aws/transfer/connector-1**.
10. Choisissez Next, puis acceptez les valeurs par défaut sur la page Configurer la rotation. Ensuite, sélectionnez Suivant.
11. Sur la page Révision, choisissez Store pour créer et stocker le secret.

Génération et SFTP formatage de la clé privée du connecteur

Les détails complets relatifs à la génération d'une paire de clés publique/privée sont décrits dans [Création de SSH clés sous macOS, Linux ou Unix](#)

Par exemple, pour générer une clé privée à utiliser avec des SFTP connecteurs, l'exemple de commande suivant produit le type de clé correct (remplacez *key_name* avec le nom de fichier réel de votre paire de clés) :

```
ssh-keygen -t rsa -b 4096 -m PEM -f key_name -N ""
```

Note

Lorsque vous créez votre paire de clés à utiliser avec des SFTP connecteurs, n'utilisez pas de phrase secrète. Un mot de passe vide est nécessaire pour que la SFTP configuration fonctionne correctement.

Cette commande crée une paire de RSA clés d'une taille de 4 096 bits. La clé est générée dans le PEM format existant, qui est requis par Transfer Family pour être utilisée avec le secret du SFTP connecteur. Les clés sont enregistrées dans *key_name* (clé privée) et *key_name*.pub (clé publique) dans le répertoire courant, c'est-à-dire le répertoire dans lequel vous exécutez la `ssh-keygen` commande.

Note

Transfer Family ne prend pas en charge le SSH format Open (-----BEGIN OPENSSH PRIVATE KEY-----) pour les clés utilisées pour votre SFTP connecteur. La clé doit être au PEM format existant (-----BEGIN RSA PRIVATE KEY-----ou-----BEGIN EC PRIVATE KEY-----). Vous pouvez utiliser l'`ssh-keygen`outil pour convertir votre clé en fournissant l'`-m PEM`option lorsque vous exécutez la commande.

Après avoir généré la clé, vous devez vous assurer que la clé privée est formatée avec des caractères de nouvelle ligne incorporés («\n») dans le format. JSON

Utilisez une commande pour convertir votre clé privée existante dans le bon format, c'est-à-dire avec des caractères de nouvelle ligne intégrés. JSON Nous fournissons ici des exemples pour `jq` Powershell. Vous pouvez utiliser n'importe quel outil ou commande pour convertir la clé privée au JSON format avec des caractères de nouvelle ligne incorporés.

`jq` command

Cet exemple utilise la `jq` commande, qui est téléchargeable depuis [Download jq](#).

```
jq -sR . path-to-private-key-file
```

Par exemple, si votre fichier de clé privée se trouve dans `~/ .ssh/my_private_key`, la commande est la suivante.

```
jq -sR . ~/.ssh/my_private_key
```

Cela affiche la clé dans le format correct (avec des caractères de nouvelle ligne intégrés) sur la sortie standard.

PowerShell

Si vous utilisez Windows, vous pouvez l'utiliser PowerShell pour convertir la clé au bon format. La commande Powershell suivante convertit la clé privée au format correct.

```
Get-Content -Raw path-to-private-key-file | ConvertTo-Json
```

Pour ajouter des données de clé privée au secret à utiliser avec des SFTP connecteurs

1. Dans la console Secrets Manager, lorsque vous stockez un autre type de secret, choisissez l'onglet Plaintext. Le texte doit être vide, avec uniquement une accolade d'ouverture et de fermeture, `{}`.
2. Collez votre nom d'utilisateur, les données de votre clé privée et/ou votre mot de passe en utilisant le format suivant. Pour les données de votre clé privée, collez le résultat de la commande que vous avez exécutée à l'étape 1.

```
{"Username": "SFTP-USER", "Password": "SFTP-USER-PASSWORD", "PrivateKey": "PASTE-PRIVATE-KEY-DATA-HERE"}
```

Key/value pairs [Info](#)

Key/value

Plaintext

1	{ "Username": "SFTP-USER", "Password": "SFTP-USER-PASSWORD", "PrivateKey": "PASTE-PRIVATE-KEY -DATA-HERE" }

Text

Line 1, Column 1

✖ Errors: 0

⚠ Warnings: 0

⚙

Si vous collez correctement les données de la clé privée, vous devriez voir ce qui suit lorsque vous sélectionnez l'onglet Clé/valeur. Notez que les données de la clé privée sont affichées line-by-line, plutôt que sous forme de chaîne de texte continue.

Secret value Info	
Retrieve and view the secret value.	
Key/value	Plaintext
Secret key	Secret value
Username	 SFTP-USER
Password	 SFTP-USER-PASSWORD
PrivateKey	 -----BEGIN RSA PRIVATE KEY----- MIIEpAIBAAKCAQEA... g... a... U... G... g... T... a... I... W... I... A... e... 5... 7... H... 1... By...

3. Continuez la procédure [Stockez un secret à utiliser avec un SFTP connecteur](#) à l'étape 8 et suivez cette procédure jusqu'à la fin.

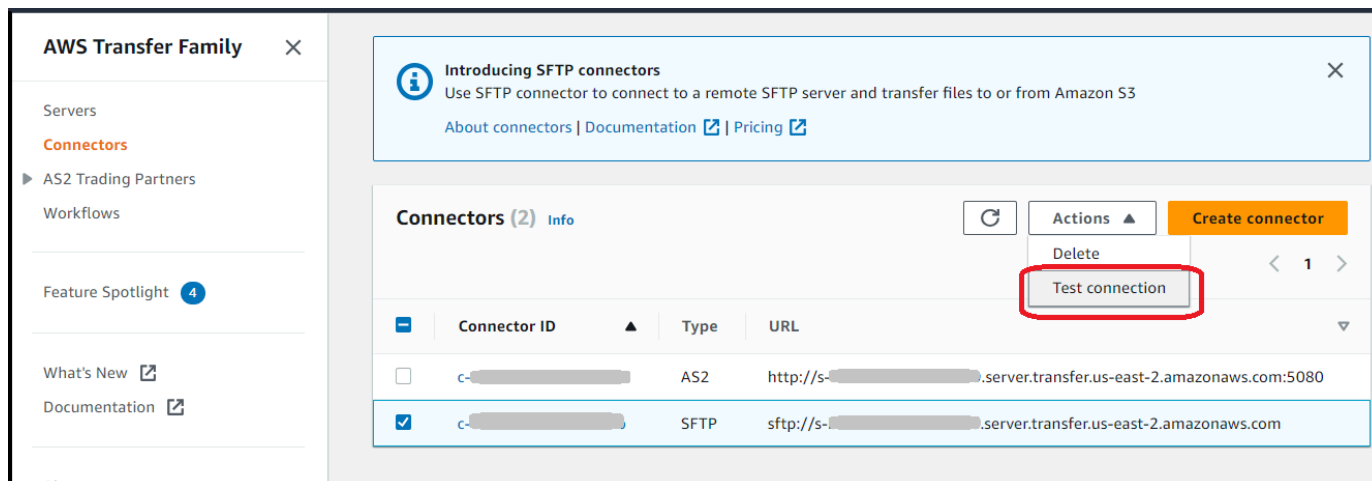
Tester un SFTP connecteur

Après avoir créé un SFTP connecteur, nous vous recommandons de le tester avant de tenter de transférer des fichiers à l'aide de votre nouveau connecteur.

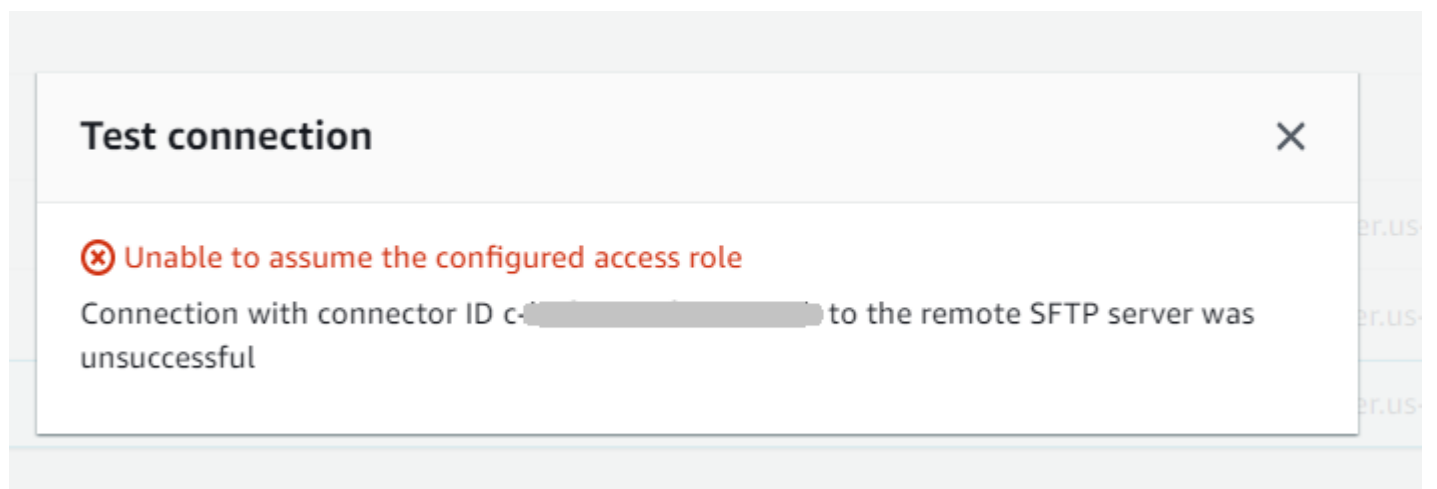
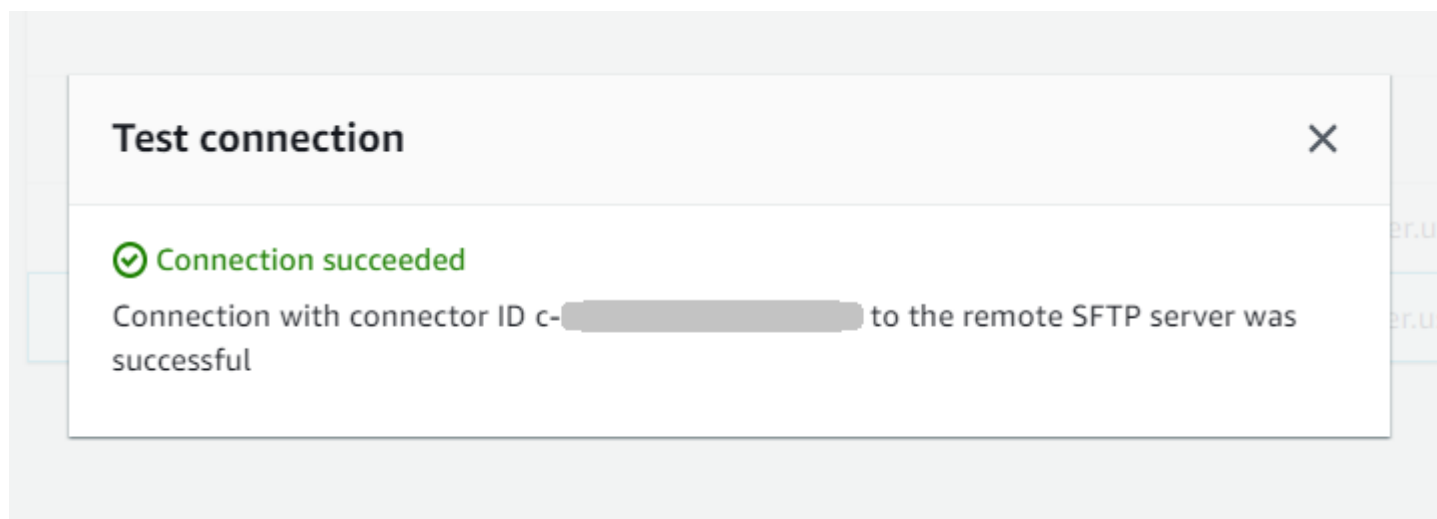
Pour tester un SFTP connecteur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Connectors, puis sélectionnez un connecteur.

3. Dans le menu Actions, choisissez Tester la connexion.



Le système renvoie un message indiquant si le test est réussi ou non. Si le test échoue, le système affiche un message d'erreur basé sur la raison de l'échec du test.



 Note

Pour API tester votre connecteur, consultez le [TestConnection](#) API documentation.

Envoyer et récupérer des fichiers à l'aide d'un SFTP connecteur

SFTP Les connecteurs étendent les capacités de AWS Transfer Family communication avec des serveurs distants à la fois dans le cloud et sur site. Vous pouvez intégrer les données générées et stockées dans des sources distantes à vos entrepôts de données AWS hébergés à des fins d'analyse, d'applications métier, de reporting et d'audit. Pour lancer un transfert de fichiers vers un SFTP serveur distant, vous utilisez [StartFileTransfer](#) API opération, qui utilise des SFTP connecteurs pour effectuer le transfert. Chaque `StartFileTransfer` demande peut contenir 10 chemins distincts.

Vous pouvez surveiller vos transferts de fichiers en consultant les journaux de votre serveur. L'activité du connecteur est enregistrée dans des flux de journaux au format `aws/transfer/connector-id`, par exemple, `aws/transfer/c-1234567890abcdef0`. Si vous ne voyez aucun journal pour votre connecteur, assurez-vous que vous avez spécifié un rôle de journalisation avec les autorisations appropriées pour votre connecteur.

Pour plus de détails sur la création de connecteurs, voir [Configuration des SFTP connecteurs](#).

Pour envoyer et récupérer des fichiers à l'aide d'un SFTP connecteur, vous devez utiliser la commande `start-file-transfer` AWS Command Line Interface (AWS CLI). Vous spécifiez les paramètres suivants, selon que vous envoyez des fichiers (transferts sortants) ou que vous recevez des fichiers (transferts entrants).

- Transferts sortants
 - `send-file-paths` contient de un à dix chemins de fichiers sources, pour les fichiers à transférer vers le SFTP serveur du partenaire.
 - `remote-directory-path` est le chemin distant vers lequel envoyer un fichier sur le SFTP serveur du client.
- Transferts entrants
 - `retrieve-file-paths` contient de un à dix chemins distants. Chaque chemin indique un emplacement pour le transfert des fichiers du SFTP serveur du partenaire vers votre serveur Transfer Family.

- `local-directory-path` est l'emplacement Amazon S3 (compartiment et préfixe facultatif) où vos fichiers sont stockés.

Pour envoyer des fichiers, vous devez spécifier les `remote-directory-path` paramètres `send-file-paths` et. Vous pouvez spécifier jusqu'à 10 fichiers pour le `send-file-paths` paramètre. L'exemple de commande suivant envoie les fichiers nommés `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` et `/DOC-EXAMPLE-SOURCE-BUCKET/file2.txt` situés dans le stockage Amazon S3 vers le `/tmp` répertoire du SFTP serveur de votre partenaire. Pour utiliser cet exemple de commande, remplacez le `DOC-EXAMPLE-SOURCE-BUCKET` par votre propre bucket.

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-SOURCE-BUCKET/
file1.txt /DOC-EXAMPLE-SOURCE-BUCKET/file2.txt \
  --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Pour recevoir des fichiers, vous devez spécifier les `local-directory-path` paramètres `retrieve-file-paths` et. L'exemple suivant récupère les fichiers `/my/remote/file1.txt` et les place `/my/remote/file2.txt` sur le SFTP serveur du partenaire à l'emplacement Amazon S3 `/DOC-EXAMPLE-BUCKET/prefix`. Pour utiliser cet exemple de commande, remplacez le `user input placeholders` par vos propres informations.

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt /my/
remote/file2.txt \
  --local-directory-path /DOC-EXAMPLE-BUCKET/prefix --connector-id c-2222BBBB3333CCCC4
--region us-east-2
```

Les exemples précédents spécifient des chemins absolus sur le SFTP serveur. Vous pouvez également utiliser des chemins relatifs, c'est-à-dire des chemins relatifs au répertoire personnel de SFTP l'utilisateur. Par exemple, si l'utilisateur SFTP est `marymajor` et que son répertoire personnel sur le SFTP serveur est `/users/marymajor/`, la commande suivante envoie `/DOC-EXAMPLE-SOURCE-BUCKET/file1.txt` à `/users/marymajor/test-connectors/file1.txt`

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-SOURCE-BUCKET/file1.txt
\
  --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

Gérer les SFTP connecteurs

Cette rubrique explique comment afficher et mettre à jour les SFTP connecteurs, et répertorie les quotas pertinents pour les SFTP connecteurs.

Rubriques

- [Mettre à jour les SFTP connecteurs](#)
- [Afficher les détails SFTP du connecteur](#)
- [Quotas pour les SFTP connecteurs](#)

Mettre à jour les SFTP connecteurs

Pour modifier les valeurs des paramètres existants pour vos connecteurs, vous pouvez exécuter la `update-connector` commande. La commande suivante met à jour le secret du connecteur *connector-id*, dans la région *region-id* vers *secret-ARN*. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
  --connector-id connector-id --region region-id
```

Afficher les détails SFTP du connecteur

Vous trouverez la liste des détails et des propriétés d'un SFTP connecteur dans la AWS Transfer Family console.

Pour afficher les détails du connecteur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le panneau de navigation de gauche, choisissez Connectors (Connecteurs).
3. Choisissez l'identifiant dans la colonne ID du connecteur pour voir la page de détails du connecteur sélectionné.

Vous pouvez modifier les propriétés du SFTP connecteur en choisissant Modifier sur la page de détails du connecteur.

[Transfer Family](#) > [Connectors](#) > c-[redacted]

C-[redacted] Delete

Connector configuration [Info](#) Edit

URL sftp://[redacted]	Access role [redacted]transfer-s3 ↗	Logging role [redacted]role ↗

SFTP configuration Edit

Connector credentials arn:aws:secretsmanager:us-[redacted] ↗	Trusted host keys 1. SHA256 [redacted]

Egress IP details [Info](#)

Service managed static IP addresses of this connector

↗	52.[redacted]
↗	3.[redacted]
↗	54.[redacted]

Tags (0) Manage tags

< 1 >

Key	Value

Note

Vous pouvez obtenir la plupart de ces informations, bien que dans un format différent, en exécutant la commande suivante AWS Command Line Interface (AWS CLI). Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws transfer describe-connector --connector-id your-connector-id
```

Pour plus d'informations, consultez [.DescribeConnector](#) dans la API référence.

Quotas pour les SFTP connecteurs

Les quotas suivants sont en place pour les SFTP connecteurs. Les quotas pour les AS2 connecteurs sont décrits dans [AS2quotas et limites](#). Pour demander l'augmentation d'un quota ajustable, consultez les [Service AWS quotas](#) dans le Références générales AWS.

SFTPquotas de connecteurs

Nom	Par défaut	Ajustable
Nombre maximal de transactions de connexion de test par seconde (TPS)	1 demande par seconde, par compte	Non
Maximum StartFile Transfer TPS	3 demandes par seconde, par compte	Oui
Taille de file d'attente maximale pour les transferts de fichiers en attente	1 000	Non
Taille maximale du fichier	50 Gibioctets (GiB)	Non
Durée de transfert maximale par fichier	6 heures	Non
Temps d'attente maximal pour les demandes par fichier	6 heures	Non
Durée minimale AccessRole ou durée LoggingRole de session	60 minutes	Non
Nombre maximal de transferts de fichiers simultanés	1 transfert de fichier simultané par connecteur	Non

Nom	Par défaut	Ajustable
Nombre maximum de demandes de transfert de fichiers par seconde et par compte	3	Oui
Nombre maximum de connecteurs par compte (les deux SFTP et les AS2 connecteurs contribuent à ce nombre)	100	Oui
Bande passante maximale pour les connecteurs par compte (les deux SFTP et les AS2 connecteurs contribuent à cette valeur)	50 MBps	Non

Pour stocker les informations d'identification des SFTP connecteurs, des quotas sont associés à chaque secret de Secrets Manager. Si vous utilisez le même secret pour stocker plusieurs types de clés, à des fins multiples, vous risquez de rencontrer ces quotas.

- Longueur totale d'un seul secret : 12 000 caractères
- Longueur maximale de la **Password** chaîne : 1024 caractères
- Longueur maximale de la **PrivateKey** chaîne : 8192 caractères
- Longueur maximale de la **Username** chaîne : 100 caractères

AWS Transfer Family pour AS2

La déclaration d'applicabilité 2 (AS2) est une spécification de transmission de fichiers RFC définie qui inclut de solides mécanismes de protection et de vérification des messages. Le AS2 protocole est essentiel pour les flux de travail soumis à des exigences de conformité qui reposent sur l'intégration de fonctionnalités de protection et de sécurité des données dans le protocole.

Note

AS2for Transfer Family est [certifié Drummond](#).

Les clients de secteurs tels que le commerce de détail, les sciences de la vie, la fabrication, les services financiers et les services publics qui dépendent AS2 des flux de travail de la chaîne d'approvisionnement, de la logistique et des paiements peuvent utiliser des AWS Transfer Family AS2 terminaux pour effectuer des transactions en toute sécurité avec leurs partenaires commerciaux. Les données traitées sont accessibles de manière native à des AWS fins de traitement, d'analyse et d'apprentissage automatique. Ces données sont également disponibles pour les intégrations avec les systèmes de planification des ressources d'entreprise (ERP) et de gestion de la relation client (CRM) qui s'exécutent sur AWS. Les clients peuvent ainsi exécuter leurs transactions business-to-business (B2B) à grande échelle AWS tout en maintenant les intégrations et la conformité des partenaires commerciaux existants. AS2

Si vous êtes un client de Transfer Family qui souhaite échanger des fichiers avec un partenaire disposant d'un serveur configuré AS2, la configuration implique de générer une paire de clés publique-privée pour le chiffrement et une autre pour signer et échanger les clés publiques avec le partenaire.

La protection d'une AS2 charge utile en transit implique généralement l'utilisation de la syntaxe des messages cryptographiques (CMS) et utilise généralement le chiffrement et une signature numérique pour assurer la protection des données et l'authentification des pairs. Une charge utile de réponse signée à un avis de disposition de message (MDN) permet de vérifier (non répudiation) qu'un message a été reçu et correctement déchiffré.

Le transport de ces CMS charges utiles et de ces MDN réponses est terminé. HTTP

 Note

HTTPSAS2 les points de terminaison du serveur ne sont actuellement pas pris en charge.
TLS la résiliation est actuellement à la charge du client.

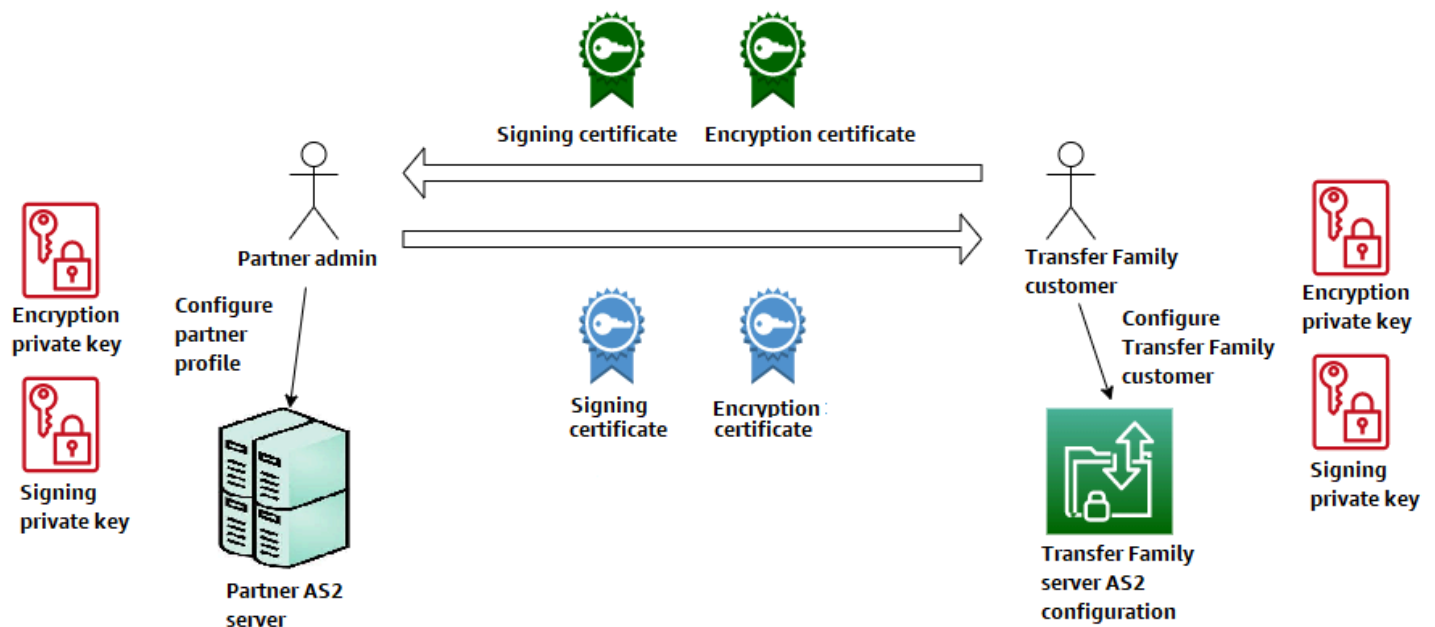
Pour une présentation détaillée de step-by-step la configuration d'une configuration de la déclaration d'applicabilité 2 (AS2), consultez le didacticiel. [Configuration d'une AS2 configuration](#)

Rubriques

- [AS2cas d'utilisation](#)
- [Configuration AS2](#)
- [Configuration des AS2 connecteurs](#)
- [Gérer les AS2 partenaires](#)
- [Envoyer et recevoir AS2 des messages](#)
- [Surveillance de l'utilisation de l'AS2](#)

AS2cas d'utilisation

Si vous êtes un AWS Transfer Family client qui souhaite échanger des fichiers avec un partenaire disposant d'un AS2 serveur configuré, la partie la plus complexe de la configuration consiste à générer une paire de clés publique-privée pour le chiffrement et une autre pour signer et échanger les clés publiques avec le partenaire.



Tenez compte des variantes suivantes à utiliser AWS Transfer Family avec AS2.

Note

Le partenaire commercial est le partenaire associé à ce profil de partenaire.
Toutes les mentions figurant MDN dans le tableau suivant sont supposées signées MDNs.

AS2 cas d'utilisation

Cas d'utilisation entrants uniquement

- Transférez AS2 des messages cryptés d'un partenaire commercial vers un serveur Transfer Family.

Dans ce cas, procédez comme suit :

1. Créez des profils pour votre partenaire commercial et pour vous-même.
2. Créez un serveur Transfer Family qui utilise le AS2 protocole.
3. Créez un accord et ajoutez-le à votre serveur.
4. Importez un certificat avec une clé privée et ajoutez-le à votre profil, puis importez la clé publique dans le profil de votre partenaire pour le chiffrer.
5. Une fois que vous avez obtenu ces éléments, envoyez la clé publique de votre certificat à votre partenaire commercial.

Votre partenaire peut désormais vous envoyer des messages chiffrés et vous pouvez les déchiffrer et les stocker dans votre compartiment Amazon S3.

- Transférez AS2 les messages chiffrés d'un partenaire commercial vers un serveur Transfer Family et ajoutez une signature.

Dans ce scénario, vous n'effectuez toujours que des transferts entrants, mais vous souhaitez maintenant que votre partenaire signe les messages qu'il envoie. Dans ce cas, importez la clé publique de signature du partenaire commercial (sous forme de certificat de signature ajouté au profil de votre partenaire).

- Transférez AS2 les messages chiffrés d'un partenaire commercial vers un serveur Transfer Family et ajoutez la signature et l'envoi d'une MDN réponse.

Dans ce scénario, vous n'effectuez toujours que des transferts entrants, mais désormais, en plus de recevoir des charges utiles signées, votre partenaire commercial souhaite recevoir une réponse signéeMDN.

1. Importez vos clés de signature publiques et privées (sous forme de certificat de signature sur votre profil).
2. Envoyez la clé de signature publique à votre partenaire commercial.

Cas d'utilisation uniquement en sortie

- Transférez AS2 des messages cryptés d'un serveur Transfer Family vers un partenaire commercial.

Ce cas est similaire au cas d'utilisation du transfert entrant uniquement, sauf qu'au lieu d'ajouter un accord à votre AS2 serveur, vous créez un connecteur. Dans ce cas, vous importez la clé publique de votre partenaire commercial dans son profil.

- Transférez AS2 des messages chiffrés d'un serveur Transfer Family vers un partenaire commercial et ajoutez une signature.

Vous n'effectuez toujours que des transferts sortants, mais votre partenaire commercial veut maintenant que vous signiez le message que vous lui envoyez.

1. Importez votre clé privée de signature (sous forme de certificat de signature ajouté à votre profil).
 2. Envoyez votre clé publique à votre partenaire commercial.
- Transférez AS2 des messages chiffrés d'un serveur Transfer Family vers un partenaire commercial, ajoutez une signature et envoyez une MDN réponse.

Vous n'effectuez toujours que des transferts sortants, mais désormais, en plus d'envoyer des charges utiles signées, vous souhaitez recevoir une MDN réponse signée de votre partenaire commercial.

1. Votre partenaire commercial vous envoie sa clé de signature publique.
2. Importez la clé publique de votre partenaire commercial (sous forme de certificat de signature ajouté à votre profil de partenaire).

Cas d'utilisation entrants et sortants

- Transférez AS2 des messages cryptés dans les deux sens entre un serveur Transfer Family et un partenaire commercial.

Dans ce cas, procédez comme suit :

1. Créez des profils pour votre partenaire commercial et pour vous-même.
2. Créez un serveur Transfer Family qui utilise le AS2 protocole.
3. Créez un accord et ajoutez-le à votre serveur.
4. Créez un connecteur.
5. Importez un certificat avec une clé privée et ajoutez-le à votre profil, puis importez la clé publique dans le profil de votre partenaire pour le chiffrer.
6. Recevez une clé publique de votre partenaire commercial et ajoutez-la à son profil à des fins de chiffrement.
7. Une fois que vous avez obtenu ces éléments, envoyez la clé publique de votre certificat à votre partenaire commercial.

Vous et votre partenaire commercial pouvez désormais échanger des messages cryptés, et vous pouvez tous les deux les déchiffrer. Vous pouvez stocker les messages que vous recevez dans votre compartiment Amazon S3, et votre partenaire peut déchiffrer et stocker les messages que vous lui envoyez.

- Transférez AS2 des messages chiffrés dans les deux sens entre un serveur Transfer Family et un partenaire commercial et ajoutez une signature.

Maintenant, vous et votre partenaire voulez des messages signés.

1. Importez votre clé privée de signature (sous forme de certificat de signature ajouté à votre profil).
 2. Envoyez votre clé publique à votre partenaire commercial.
 3. Importez la clé publique de signature de votre partenaire commercial et ajoutez-la à son profil.
- Transférez AS2 des messages chiffrés dans les deux sens entre un serveur Transfer Family et un partenaire commercial, ajoutez une signature et envoyez une MDN réponse.

Vous souhaitez maintenant échanger des charges utiles signées, et vous et votre partenaire commercial souhaitez obtenir MDN des réponses.

1. Votre partenaire commercial vous envoie sa clé de signature publique.
2. Importez la clé publique de votre partenaire commercial (sous forme de certificat de signature sur votre profil de partenaire).
3. Envoyez votre clé publique à votre partenaire commercial.

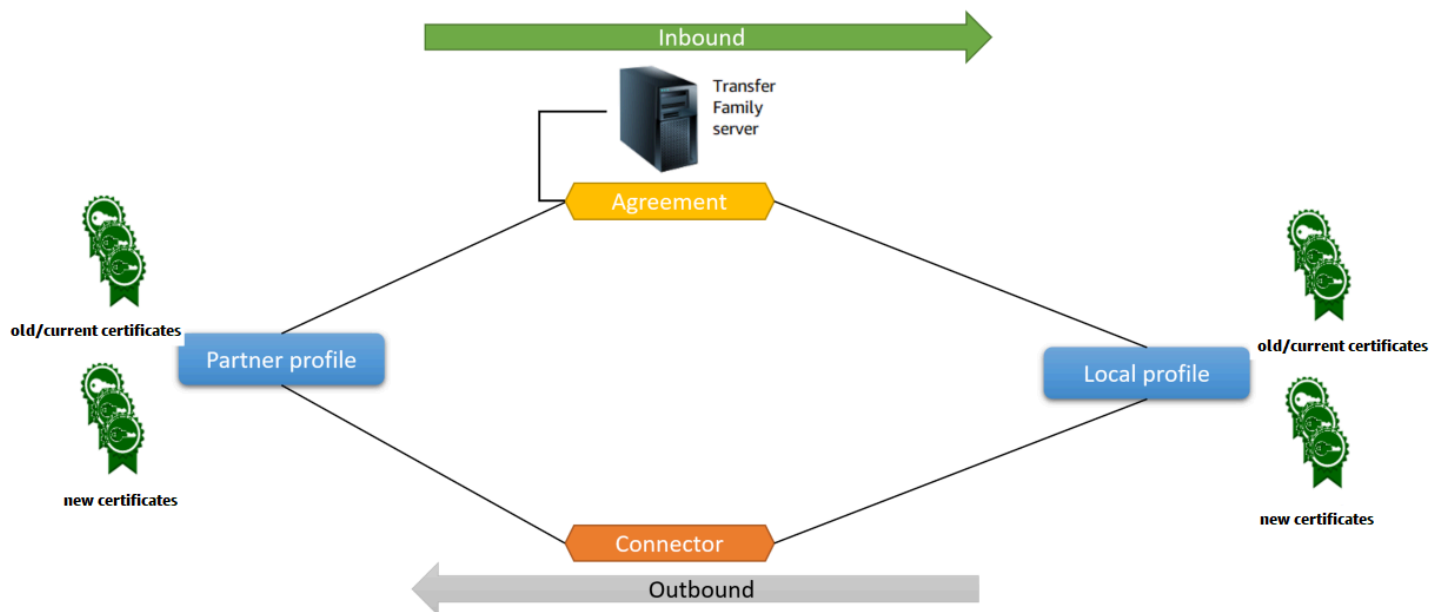
Configuration AS2

Pour créer un AS2 serveur activé, vous devez également spécifier les composants suivants :

- **Accords** — Les accords bilatéraux de partenaires commerciaux, ou partenariats, définissent la relation entre les deux parties qui échangent des messages (fichiers). Pour définir un accord, Transfer Family combine les informations relatives au serveur, au profil local, au profil du partenaire et au certificat. Transfer Family AS2 - les processus entrants utilisent des accords.
- **Certificats** — Les certificats à clé publique (X.509) sont utilisés dans les AS2 communications pour le chiffrement et la vérification des messages. Les certificats sont également utilisés pour les points de terminaison des connecteurs.
- **Profil locaux et profils de partenaires** — Un profil local définit l'organisation ou le « groupe » local (AS2compatible avec le serveur Transfer Family). De même, un profil de partenaire définit l'organisation partenaire distante, externe à Transfer Family.

Bien que cela ne soit pas obligatoire pour tous les serveurs AS2 compatibles, vous avez besoin d'un connecteur pour les transferts sortants. Un connecteur capture les paramètres d'une connexion sortante. Le connecteur est nécessaire pour envoyer des fichiers à un serveur externe, autre que le AWS serveur d'un client.

Le schéma suivant montre la relation entre les AS2 objets impliqués dans les processus entrants et sortants.



Pour un end-to-end exemple AS2 de configuration, voir [Configuration d'une AS2 configuration](#).

Rubriques

- [Création d'un AS2 serveur à l'aide de la console Transfer Family](#)
- [Utilisez un modèle pour créer un AS2 stack Transfer Family de démonstration](#)
- [AS2configurations et limites](#)
- [AS2fonctionnalités et capacités](#)

Création d'un AS2 serveur à l'aide de la console Transfer Family

Cette procédure explique comment créer un serveur AS2 compatible à l'aide de la console Transfer Family. Si vous souhaitez utiliser le à la AWS CLI place, consultez [the section called "Étape 2 : Création d'un serveur Transfer Family utilisant le AS2 protocole"](#).

Pour créer un AS2 serveur activé

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers, puis Create server.
3. Sur la page Choisir des protocoles, sélectionnez AS2(Déclaration d'applicabilité 2), puis cliquez sur Suivant.

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☒ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

[Cancel](#) [Next](#)

- Sur la page Choisir un fournisseur d'identité, sélectionnez Suivant.

Note

En effet AS2, vous ne pouvez pas choisir de fournisseur d'identité car l'authentification de base n'est pas prise en charge par le AS2 protocole. Au lieu de cela, vous contrôlez l'accès par le biais de groupes de sécurité du cloud privé virtuel (VPC).

- Sur la page Choisir un point de terminaison, procédez comme suit :

Choose an endpoint

Endpoint configuration [Info](#)

Endpoint type
Select whether the endpoint will be publicly accessible or hosted inside your VPC

☐ Publicly accessible
Accessible over the internet

☒ VPC hosted [Info](#)
Access controlled using Security Groups

Access [Info](#)

☒ Internal

☐ Internet Facing

VPC
Select a VPC ID



[Create a VPC](#) 

FIPS Enabled
Select whether the endpoint should comply with Federal Information Processing Standards (FIPS)

☐ FIPS Enabled endpoint

[Cancel](#) [Previous](#) [Next](#)

- a. Pour le type de point de terminaison, choisissez VPC hébergé pour héberger le point de terminaison de votre serveur. Pour plus d'informations sur la configuration de votre point de terminaison VPC hébergé, consultez [Création d'un serveur dans un cloud privé virtuel](#).

 Note

Les points de terminaison accessibles au public ne sont pas pris en charge par le AS2 protocole. Pour rendre votre VPC point de terminaison accessible via Internet, choisissez Internet Facing sous Accès, puis indiquez vos adresses IP élastiques.

- b. Pour Access, choisissez l'une des options suivantes :

- Interne : choisissez cette option pour fournir un accès depuis votre environnement VPC et celui des environnements VPC connectés, tels qu'un centre de données sur site par rapport AWS Direct Connect à ou. VPN
- Accès à Internet — Choisissez cette option pour fournir un accès via Internet et depuis votre VPC environnement VPC connecté, tel qu'un centre de données sur site au-dessus AWS Direct Connect de ou. VPN

Si vous choisissez Internet Facing, indiquez vos adresses IP élastiques lorsque vous y êtes invité.

- c. En VPCeffet, choisissez un existant VPC ou choisissez Créer VPC pour en créer un nouveauVPC.
- d. Pour FIPSEnabled, laissez la case FIPSEnabled endpoint décochée.

 Note

FIPSEs points de terminaison compatibles ne sont pas pris en charge par le AS2 protocole.

- e. Choisissez Suivant.
6. Sur la page Choisissez un domaine, choisissez Amazon S3 pour stocker et accéder à vos fichiers sous forme d'objets en utilisant le protocole sélectionné.

Choisissez Suivant.

7. Sur la page Configurer les détails supplémentaires, choisissez les paramètres dont vous avez besoin.

 Note

Si vous configurez d'autres protocoles en même tempsAS2, tous les paramètres de détail supplémentaires s'appliquent. Toutefois, pour le AS2 protocole, les seuls paramètres applicables sont ceux des sections de CloudWatch journalisation et de balises.

Même si la configuration d'un rôle de CloudWatch journalisation est facultative, nous vous recommandons vivement de le configurer afin que vous puissiez voir l'état de vos messages et résoudre les problèmes de configuration.

8. Sur la page Réviser et créer, passez en revue vos choix pour vous assurer qu'ils sont corrects.
- Si vous souhaitez modifier l'un de vos paramètres, choisissez Modifier à côté de l'étape que vous souhaitez modifier.

 Note

Si vous modifiez une étape, nous vous recommandons de passer en revue chaque étape après l'étape que vous avez choisi de modifier.

- Si aucune modification n'est apportée, choisissez Create server pour créer votre serveur. Vous êtes dirigé vers la page Servers (Serveurs), représentée ci-dessous, dans laquelle figure votre nouveau serveur.

Servers (1)							 Actions ▼ Add user Create server	
☐	Hostname ▲	Server ID ▼	State ▼	Service managed users ▼	Endpoint type ▼	Domain ▼	< 1 >	
☐	-	s-	Starting	-	VPC	Amazon S3		

Plusieurs minutes peuvent s'écouler avant que le statut de votre nouveau serveur passe à En ligne. À ce stade, votre serveur peut effectuer des opérations sur fichiers pour vos utilisateurs.

Utilisez un modèle pour créer un AS2 stack Transfer Family de démonstration

Nous fournissons un AWS CloudFormation modèle autonome pour créer rapidement un AS2 serveur Transfer Family compatible. Le modèle configure le serveur avec un point de VPC terminaison Amazon public, des certificats, des profils locaux et partenaires, un accord et un connecteur.

Avant d'utiliser ce modèle, prenez note des points suivants :

- Si vous créez une pile à partir de ce modèle, les AWS ressources utilisées vous seront facturées.
- Le modèle crée plusieurs certificats et les place pour les AWS Secrets Manager stocker en toute sécurité. Vous pouvez supprimer ces certificats de Secrets Manager si vous le souhaitez, car l'utilisation de ce service vous est facturée. La suppression de ces certificats dans Secrets Manager ne les supprime pas du serveur Transfer Family. Par conséquent, la fonctionnalité de la pile de démonstration n'est pas affectée. Toutefois, pour les certificats que vous allez utiliser

avec un AS2 serveur de production, vous pouvez utiliser Secrets Manager pour gérer et alterner régulièrement vos certificats stockés.

- Nous vous recommandons d'utiliser le modèle uniquement comme base, et principalement à des fins de démonstration. Si vous souhaitez utiliser cette pile de démonstration en production, nous vous recommandons de modifier le YAML code du modèle pour créer une pile plus robuste. Par exemple, créez des certificats au niveau de la production et créez une AWS Lambda fonction que vous pouvez utiliser en production.

Pour créer un AS2 serveur Transfer Family compatible à partir d'un modèle CloudFormation

1. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Dans le volet de navigation de gauche, choisissez Stacks (Piles).
3. Choisissez Créer une pile, puis choisissez Avec de nouvelles ressources (standard).
4. Dans la section Prérequis - Préparer le modèle, sélectionnez Le modèle est prêt.
5. Copiez ce lien, [modèle de AS2 démonstration](#), et collez-le dans le URL champ Amazon S3.
6. Choisissez Suivant.
7. Sur la page Spécifier les détails de la pile, nommez votre pile, puis spécifiez les paramètres suivants :
 - Sous AS2, entrez des valeurs pour l'AS2identifiant local et l'AS2identifiant du partenaire, ou acceptez les valeurs par défaut, `local` et `partner`, respectivement.
 - Sous Réseau, entrez une valeur pour l'adresse CIDR IP d'entrée du groupe de sécurité ou acceptez la valeur par défaut. `0.0.0.0/0`

 Note

Cette valeur, au CIDR format, indique quelles adresses IP sont autorisées pour le trafic entrant sur le AS2 serveur. La valeur par défaut autorise toutes les adresses IP.
`0.0.0.0/0`

- Sous Général, entrez une valeur pour le préfixe ou acceptez la valeur par défaut. `transfer-as2` Ce préfixe est placé avant tous les noms de ressources créés par la pile. Par exemple, si vous utilisez le préfixe par défaut, votre compartiment Amazon S3 est nommé `transfer-as2-TransferS3BucketName`.

8. Choisissez Suivant. Sur la page Configurer les options de pile, sélectionnez à nouveau Next.
9. Passez en revue les détails de la pile que vous créez, puis choisissez Create stack.

 Note

Au bas de la page, sous Capacités, vous devez reconnaître que des ressources AWS CloudFormation peuvent créer AWS Identity and Access Management (IAM).

Une fois la pile créée, vous pouvez envoyer un AS2 message de test du serveur partenaire à votre serveur Transfer Family local en utilisant le AWS Command Line Interface (AWS CLI). Un exemple de AWS CLI commande pour envoyer un message de test est créé avec toutes les autres ressources de la pile.

Pour utiliser cet exemple de commande, allez dans l'onglet Sorties de votre pile et copiez la `TransferExampleAs2Command`. Vous pouvez ensuite exécuter la commande à l'aide du AWS CLI. Si vous ne l'avez pas encore installé AWS CLI, consultez la section [Installation ou mise à jour de la AWS CLI dernière version du](#) Guide de l'AWS Command Line Interface utilisateur.

Le format de l'exemple de commande est le suivant :

```
aws s3api put-object --bucket TransferS3BucketName --key test.txt && aws transfer
start-file-transfer --region aws-region --connector-id TransferConnectorId --send-
file-paths /TransferS3BucketName/test.txt
```

 Note

Votre version de cette commande contient les valeurs réelles des *TransferConnectorId* ressources *TransferS3BucketName* et de votre pile.

Cet exemple de commande se compose de deux commandes distinctes qui sont enchaînées à l'aide de la `&&` chaîne.

La première commande crée un nouveau fichier texte vide dans votre compartiment :

```
aws s3api put-object --bucket TransferS3BucketName --key test.txt
```

Ensuite, la deuxième commande utilise le connecteur pour envoyer le fichier du profil du partenaire vers le profil local. Le serveur Transfer Family dispose d'un accord qui permet au profil local d'accepter les messages du profil du partenaire.

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId
--send-file-paths /TransferS3BucketName/test.txt
```

Après avoir exécuté la commande, vous pouvez accéder à votre compartiment Amazon S3 (*TransferS3BucketName*) et en consulter le contenu. Si la commande aboutit, vous devriez voir apparaître les objets suivants dans votre compartiment :

- `processed/`— Ce dossier contient un JSON fichier qui décrit le fichier transféré et la MDN réponse.
- `processing/`— Ce dossier contient temporairement des fichiers en cours de traitement, mais une fois le transfert terminé, ce dossier devrait être vide.
- *server-id*/— Ce dossier est nommé en fonction de votre identifiant de serveur Transfer Family. Il contient `from-partner` (ce dossier est nommé dynamiquement, en fonction de l'AS2identifiant du partenaire), qui contient lui-même `failed/processed/`, et `processing/` des dossiers. Le `/server-id/from-partner/processed/` dossier contient une copie du fichier texte transféré, ainsi que les MDN fichiers JSON et fichiers correspondants.
- `test.txt`— Cet objet est le fichier (vide) qui a été transféré.

AS2configurations et limites

Cette rubrique décrit les configurations, fonctionnalités et capacités prises en charge pour les transferts utilisant le protocole Applicability Statement 2 (AS2), y compris les chiffrements et les résumés acceptés. Cette section décrit également les limites et les problèmes connus relatifs aux AS2 transferts.

Rubriques

- [AS2configurations prises en charge](#)
- [AS2quotas et limites](#)

AS2configurations prises en charge

Signature, chiffrement, compression, MDN

Pour les transferts entrants et sortants, les éléments suivants sont obligatoires ou facultatifs :

- Chiffrement — Obligatoire (pour le HTTP transport, qui est le seul mode de transport actuellement pris en charge). Les messages non chiffrés ne sont acceptés que s'ils sont transmis par un proxy de TLS terminaison tel qu'un Application Load Balancer ALB () et X-Forwarded-Proto: https que l'en-tête est présent.
- Signature — Facultatif
- Compression — Facultatif (le seul algorithme de compression actuellement pris en charge est ZLIB)
- Avis de disposition des messages (MDN) — Facultatif

Chiffrements

Les chiffrements suivants sont pris en charge pour les transferts entrants et sortants :

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3 DES (pour la rétrocompatibilité uniquement)

Résumés

Les résumés suivants sont pris en charge :

- Signature entrante et MDN — SHA1, SHA256, SHA384 SHA512
- Signature sortante et MDN — SHA1, SHA256, SHA384 SHA512

MDN

Pour les MDN réponses, certains types sont pris en charge, comme suit :

- Transferts entrants : synchrones et asynchrones
- Transferts sortants : synchrones uniquement
- Protocole de transfert de courrier simple (SMTP) (e-mailMDN) — Non pris en charge

Les transports

- Transferts entrants : HTTP il s'agit du seul transport actuellement pris en charge, et vous devez le spécifier explicitement.

Note

Si vous devez l'utiliser HTTPS pour des transferts entrants, vous pouvez utiliser un Application Load Balancer ou un Network Load Balancer. TLS Ceci est décrit dans [Recevez AS2 des messages HTTPS](#).

- Transferts sortants : si vous fournissez un HTTPURL, vous devez également spécifier un algorithme de chiffrement. Si vous fournissez un HTTPSURL, vous avez la possibilité de spécifier NONE votre algorithme de chiffrement.

AS2quotas et limites

Cette section traite des quotas et des limites pour AS2

Rubriques

- [AS2quotas](#)
- [Quotas pour le traitement des secrets](#)
- [Limitations connues](#)

AS2quotas

Les quotas suivants sont en place pour les transferts de AS2 fichiers. Pour demander l'augmentation d'un quota ajustable, consultez les [Service AWS quotas](#) dans le Références générales AWS.

AS2quotas

Nom	Par défaut	Ajustable
AS2Demandes entrantes par serveur	25 par seconde	Non
AS2Demandes entrantes en cours par serveur	100	Non

Nom	Par défaut	Ajustable
Nombre maximum de fichiers par demande de transfert	10	Non
AS2Demandes sortantes en cours par connecteur	100	Non
Taille maximale du fichier (compressé ou non compressé)	50 MiB	Oui
Expiration du délai d'inactivité	350 secondes	Non
Nombre maximum de profils de partenaires par compte	1000 (jusqu'à 10 certificats par profil de partenaire : non ajustable)	Oui
Nombre maximum de certificats par compte	1 000	Oui
Nombre maximum de demandes de transfert de fichiers par seconde et par compte	3	Oui
Nombre maximum de connecteurs par compte (les deux SFTP et les AS2 connecteurs contribuent à ce nombre)	100	Oui
Bande passante maximale pour les connecteurs par compte (les deux SFTP et les AS2 connecteurs contribuent à cette valeur)	50 MBps	Non

Nom	Par défaut	Ajustable
Nombre maximum d'accords par serveur	100	Oui

Quotas pour le traitement des secrets

AWS Transfer Family passe des appels AWS Secrets Manager au nom des AS2 clients qui utilisent l'authentification de base. Secrets Manager passe également des appels à AWS KMS.

Note

Ces quotas ne sont pas spécifiques à votre utilisation des secrets pour Transfer Family : ils sont partagés entre tous les services de votre entreprise Compte AWS.

Pour Secrets Manager `GetSecretValue`, le quota applicable est le taux combiné de `DescribeSecret` et de `GetSecretValue` API demandes, comme décrit dans la section [AWS Secrets Manager Quotas](#).

Secrets Manager **GetSecretValue**

Nom	Valeur	Description
Taux <code>DescribeSecret</code> et <code>GetSecretValue</code> API demandes combinés	Chaque Région prise en charge : 10 000 par seconde	Le nombre maximum de transactions par seconde pour <code>DescribeSecret</code> et pour les <code>GetSecretValue</code> API demandes combinées.

Pour AWS KMS, les quotas suivants s'appliquent à `Decrypt`. Pour plus de détails, voir [Demander des quotas pour chaque AWS KMS API opération](#)

AWS KMS **Decrypt**

Nom du quota	Valeur par défaut (requêtes par seconde)
Taux de demandes d'opérations cryptographiques (symétriques)	Ces quotas partagés varient en fonction de la AWS KMS clé utilisée dans la demande

Nom du quota	Valeur par défaut (requêtes par seconde)
	Région AWS et du type de clé. Chaque quota est calculé séparément. • 5 500 (partagées) • 10 000 (partagées) dans les régions suivantes : • USA Est (Ohio), us-east-2 • Asie-Pacifique (Singapour), ap-southeast-1 • Asie-Pacifique (Sydney), ap-southeast-2 • Asie-Pacifique (Tokyo), ap-northeast-1 • Europe (Francfort), eu-central-1 • Europe (Londres), eu-west-2 • 50 000 (partagées) dans les régions suivantes : • USA Est (Virginie du Nord), us-east-1 • USA Ouest (Oregon), us-west-2 • Europe (Irlande), eu-west-1
Quotas de demandes de magasin de clés personnalisé  Note Ce quota ne s'applique que si vous utilisez un magasin de clés externe.	Les quotas de demandes de stockage de clés personnalisés sont calculés séparément pour chaque magasin de clés personnalisé. • 1 800 (partagés) pour chaque magasin de AWS CloudHSM clés • 1 800 (partagées) pour chaque magasin de clés externes

Limitations connues

- Le mode TCP keep-alive côté serveur n'est pas pris en charge. La connexion expire après 350 secondes d'inactivité, sauf si le client envoie des paquets de maintien en vie.
- Pour qu'un accord actif soit accepté par le service et apparaisse dans les CloudWatch journaux Amazon, les messages doivent contenir des AS2 en-têtes valides.

- [Le serveur qui reçoit des messages de AWS Transfer Family for AS2 doit prendre en charge l'attribut de protection de l'algorithme Cryptographic Message Syntax \(CMS\) pour valider les signatures des messages, tel que défini dans RFC 6211.](#) Cet attribut n'est pas pris en charge dans certains anciens produits IBM Sterling.
- Un message dupliqué IDs entraîne un message traité/Avertissement : document dupliqué.
- La longueur de la clé pour les AS2 certificats doit être d'au moins 2 048 bits et d'au plus 4 096 bits.
- Lors de l'envoi de AS2 messages ou de manière asynchrone MDNs au HTTPS point de terminaison d'un partenaire commercial, les messages ou les messages MDNs doivent utiliser un SSL certificat valide signé par une autorité de certification (CA) reconnue publiquement. Les certificats auto-signés ne sont actuellement pas pris en charge.
- Le point de terminaison doit prendre en charge le protocole TLS version 1.2 et un algorithme cryptographique autorisé par la politique de sécurité (comme décrit dans [Politiques de sécurité pour AWS Transfer Family](#)).
- Mutual TLS (mTLS) n'est pas pris en charge actuellement.
- Les pièces jointes multiples et les messages d'échange de certificats (CEM) de AS2 la version 1.2 ne sont pas pris en charge actuellement.
- L'authentification de base n'est actuellement prise en charge que pour les messages sortants.

AS2 fonctionnalités et capacités

Les tableaux suivants répertorient les fonctionnalités et capacités disponibles pour les ressources Transfer Family qui les utilisent AS2.

AS2 fonctionnalités

Transfer Family propose les fonctionnalités suivantes pour AS2.

Fonctionnalité	Soutenu par AWS Transfer Family
Certification Drummond	Oui
AWS CloudFormation soutien	Oui
CloudWatch Métriques Amazon	Oui
SHA-2 algorithmes cryptographiques	Oui

Fonctionnalité	Soutenu par AWS Transfer Family
Support pour Amazon S3	Oui
Support pour Amazon EFS	Non
Messages planifiés	Oui ¹
AWS Transfer Family Flux de travail gérés	Non
Messagerie d'échange de certificats (CEM)	Non
TLSMutuel (mTLS)	Non

1. Messages planifiés sortants disponibles via les [AWS Lambda fonctions de planification à l'aide d'Amazon EventBridge](#)

AS2capacités d'envoi et de réception

Le tableau suivant fournit une liste des fonctionnalités d' AWS Transfer Family AS2envoi et de réception.

Capacité	Entrant : réception avec le serveur	Sortant : envoi avec connecteur
TLSTransport crypté (HTTPS)	Oui ¹	Oui
Non lié au TLS transport (HTTP)	Oui	Oui ²
Synchrone MDN	Oui	Oui
Compression des messages	Oui	Oui
Asynchrone MDN	Oui	Non
Adresse IP statique	Oui	Oui
Apportez votre propre adresse IP	Oui	Non

Capacité	Entrant : réception avec le serveur	Sortant : envoi avec connecteur
Pièces jointes multiples	Non	Non
Authentification de base	Non	Oui
AS2Redémarrer	Ne s'applique pas	Non
Objet personnalisé par message	Ne s'applique pas	Non

1. Transport TLS crypté entrant disponible avec Network Load NLB Balancer ()
2. TLS Transport non sortant disponible uniquement lorsque le chiffrement est activé

Configuration des AS2 connecteurs

L'objectif d'un connecteur est d'établir une relation entre les partenaires commerciaux pour les transferts sortants, en envoyant des AS2 fichiers depuis un serveur Transfer Family vers une destination externe appartenant au partenaire. Pour le connecteur, vous spécifiez la partie locale, le partenaire distant et leurs certificats (en créant des profils locaux et partenaires). Une fois le connecteur en place, vous pouvez transférer des informations à vos partenaires commerciaux.

Note

La taille du message reçu par un partenaire commercial ne correspond pas à la taille de l'objet dans Amazon S3. Cette différence est due au fait que le AS2 message enveloppe le fichier dans une enveloppe avant de l'envoyer. La taille du fichier peut donc augmenter, même si le fichier est envoyé avec compression. Par conséquent, assurez-vous que la taille maximale du fichier du partenaire commercial est supérieure à celle du fichier que vous envoyez.

Déclaration d'applicabilité 2 (AS2) Les connecteurs établissent une relation entre les partenaires commerciaux pour les transferts sortants. Pour plus d'informations sur les AS2 connecteurs, consultez [Configuration des AS2 connecteurs](#).

Création d'un AS2 connecteur

Cette procédure explique comment créer des AS2 connecteurs à l'aide de la AWS Transfer Family console. Si vous souhaitez utiliser le à la AWS CLI place, consultez [the section called “Étape 6 : Créez un lien entre vous et votre partenaire”](#).

Pour créer un AS2 connecteur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Connectors, puis Create connector.
3. Dans la section Configuration du connecteur, spécifiez les informations suivantes :

- URL— Entrez le URL pour les connexions sortantes.
- Rôle d'accès : choisissez le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) à utiliser. Assurez-vous que ce rôle fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande. Assurez-vous également que le rôle fournit un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer `StartFileTransfer`.

Note

Si vous utilisez l'authentification de base pour votre connecteur, le rôle d'accès nécessite `secretsmanager:GetSecretValue` autorisation d'accès au secret. Si le secret est chiffré à l'aide d'une clé gérée par le client au lieu de la Clé gérée par AWS clé d'entrée AWS Secrets Manager, le rôle doit également disposer de `kms:Decrypt` autorisation pour cette clé. Si vous nommez votre secret avec le préfixe `aws/transfer/`, vous pouvez ajouter l'autorisation nécessaire avec un caractère générique (*), comme indiqué dans [Exemple d'autorisation pour créer des secrets](#).

- Rôle de journalisation (facultatif) — Choisissez le IAM rôle que le connecteur doit utiliser pour transférer des événements vers vos CloudWatch journaux.
4. Dans la section AS2 de configuration, choisissez les profils local et partenaire, les algorithmes de chiffrement et de signature, et indiquez si vous souhaitez compresser les informations transférées. Notez ce qui suit :

- Pour l'algorithme de chiffrement, ne le choisissez DES_EDE3_CBC que si vous devez prendre en charge un ancien client qui en a besoin, car il s'agit d'un algorithme de chiffrement faible.
 - L'objet est utilisé comme attribut d'header HTTP dans les AS2 messages envoyés avec le connecteur.
 - Si vous choisissez de créer un connecteur sans algorithme de chiffrement, vous devez HTTPS le spécifier comme protocole.
5. Dans la section MDN de configuration, spécifiez les informations suivantes :
- Demande MDN — Vous avez la possibilité de demander à votre partenaire commercial de vous envoyer un message MDN après avoir reçu votre message avec succès AS2.
 - Signé MDN — Vous avez la possibilité d'exiger qu'il MDNs soit signé. Cette option n'est disponible que si vous avez sélectionné Demande MDN.
6. Dans la section Authentification de base, spécifiez les informations suivantes.
- Pour envoyer des informations d'identification ainsi que des messages sortants, sélectionnez Activer l'authentification de base. Si vous ne souhaitez pas envoyer d'informations d'identification avec les messages sortants, laissez la case Activer l'authentification de base désactivée.
 - Si vous utilisez l'authentification, choisissez ou créez un secret.
 - Pour créer un nouveau secret, choisissez Créer un nouveau secret, puis entrez un nom d'utilisateur et un mot de passe. Ces informations d'identification doivent correspondre à l'utilisateur qui se connecte au point de terminaison du partenaire.

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ Create a new secret

☐ Choose an existing secret

Username

Password

 Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

- Pour utiliser un secret existant, choisissez Choisir un secret existant, puis choisissez un secret dans le menu déroulant. Pour en savoir plus sur la création d'un secret correctement formaté dans Secrets Manager, consultez [Activer l'authentification de base pour les AS2 connecteurs](#).

[illegible]

7. Après avoir confirmé tous vos paramètres, choisissez **Create connector** pour créer le connecteur.

La page Connecteurs apparaît, avec l'ID de votre nouveau connecteur ajouté à la liste. Pour consulter les détails de vos connecteurs, consultez [Afficher les détails AS2 du connecteur](#).

AS2algorithmes de connexion

Lorsque vous créez un AS2 connecteur, les algorithmes de sécurité suivants sont attachés au connecteur.

Type	Algorithm
TLSCiffre	TLS_ ECDHE __ ECDSA WITH _ AES GCM _128__ SHA256

Type	Algorithm
	TLS_ECDHE __ RSA WITH _ AES GCM _128__ SHA256
	TLS_ECDHE __ ECDSA WITH _ AES CBC _128__ SHA256
	TLS_ECDHE __ RSA WITH _ AES CBC _128_ _ SHA256
	TLS_ECDHE __ ECDSA WITH _ AES GCM _256__ SHA384
	TLS_ECDHE __ RSA WITH _ AES GCM _256__ SHA384
	TLS_ECDHE __ ECDSA WITH _ AES CBC _256__ SHA384
	TLS_ECDHE __ RSA WITH _ AES CBC _256_ _ SHA384

Authentification de base pour les AS2 connecteurs

Lorsque vous créez ou mettez à jour un serveur Transfer Family qui utilise le AS2 protocole, vous pouvez ajouter l'authentification de base pour les messages sortants. Pour ce faire, ajoutez des informations d'authentification à un connecteur.

Note

L'authentification de base n'est disponible que si vous utilisez HTTPS.

Pour utiliser l'authentification pour votre connecteur, sélectionnez Activer l'authentification de base dans la section Authentification de base. Après avoir activé l'authentification de base, vous pouvez choisir de créer un nouveau secret ou d'utiliser un secret existant. Dans les deux cas, les informations d'identification contenues dans le secret sont envoyées avec les messages sortants qui

utilisent ce connecteur. Les informations d'identification doivent correspondre à celles de l'utilisateur qui tente de se connecter au point de terminaison distant du partenaire commercial.

La capture d'écran suivante montre l'option Activer l'authentification de base sélectionnée et la sélection Créer un nouveau secret. Après avoir fait ces choix, vous pouvez saisir un nom d'utilisateur et un mot de passe pour le secret.

The screenshot shows the 'Basic authentication' configuration page. At the top, there is a header 'Basic authentication' with an 'Info' link. Below this, there is a checkbox labeled 'Enable Basic authentication - optional' which is checked. A note below the checkbox says 'Select this option to authenticate with your trading partner's host using username and password credentials.' Underneath, there is a section 'Basic authentication credentials' with an 'Info' link. A note says 'Choose the username and password credentials that will be used to authenticate with your trading partner's host.' There are two radio buttons: 'Create a new secret' (selected) and 'Choose an existing secret'. Below these are two text input fields: 'Username' with a placeholder 'Enter a username' and 'Password' with a placeholder 'Enter a password'. At the bottom, there is a light blue box with an information icon and text: 'Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.'

La capture d'écran suivante montre l'option Activer l'authentification de base sélectionnée et la sélection d'un secret existant. Votre secret doit être au bon format, comme décrit dans [Activer l'authentification de base pour les AS2 connecteurs](#).

[illegible]

Activer l'authentification de base pour les AS2 connecteurs

Lorsque vous activez l'authentification de base pour les AS2 connecteurs, vous pouvez soit créer un nouveau secret dans la console Transfer Family, soit utiliser un secret que vous avez créé dans AWS Secrets Manager. Dans les deux cas, votre secret est enregistré dans Secrets Manager.

Rubriques

- Créez un nouveau secret dans la console
- Utilisation d'un secret existant
- Créez un secret dans AWS Secrets Manager

Créez un nouveau secret dans la console

Lorsque vous créez un connecteur dans la console, vous pouvez créer un nouveau secret.

Pour créer un nouveau secret, choisissez Créer un nouveau secret, puis entrez un nom d'utilisateur et un mot de passe. Ces informations d'identification doivent correspondre à l'utilisateur qui se connecte au point de terminaison du partenaire.

Basic authentication [Info](#)

☒ **Enable Basic authentication - optional**
Select this option to authenticate with your trading partner's host using username and password credentials.

Basic authentication credentials [Info](#)
Choose the username and password credentials that will be used to authenticate with your trading partner's host.

☒ **Create a new secret**

☐ Choose an existing secret

Username

Password

 Update the access role associated with your connector to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

Note

Lorsque vous créez un nouveau secret dans la console, le nom du secret suit cette convention de dénomination : `/aws/transfer/connector-id`, où **connector-id** est l'ID du connecteur que vous créez. Pensez-y lorsque vous essayez de localiser le secret AWS Secrets Manager.

Utilisation d'un secret existant

Lorsque vous créez un connecteur dans la console, vous pouvez spécifier un secret existant.

Pour utiliser un secret existant, choisissez Choisir un secret existant, puis choisissez un secret dans le menu déroulant. Pour en savoir plus sur la création d'un secret correctement formaté dans Secrets Manager, consultez [Créez un secret dans AWS Secrets Manager](#).

[illegible]

Créez un secret dans AWS Secrets Manager

La procédure suivante explique comment créer un secret approprié à utiliser avec votre AS2 connecteur.

 Note

L'authentification de base n'est disponible que si vous utilisez HTTPS.

Pour stocker les informations d'identification de l'utilisateur dans Secrets Manager pour l'authentification AS2 de base

1. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
2. Dans le volet de navigation de gauche, choisissez Secrets.
3. Sur la page Secrets, choisissez Enregistrer un nouveau secret.
4. Sur la page Choisir un type de secret, pour Type de secret, choisissez Autre type de secret.
5. Dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.

- Clé — Entrée **Username**.

- valeur — Entrez le nom de l'utilisateur autorisé à se connecter au serveur du partenaire.

6. Si vous souhaitez fournir un mot de passe, choisissez Ajouter une ligne, puis dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.

Choisissez Ajouter une ligne, puis dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.

- Clé — Entrée **Password**.

- valeur — Entrez le mot de passe de l'utilisateur.

7. Si vous souhaitez fournir une clé privée, choisissez Ajouter une ligne, puis dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.

- Clé — Entrée **PrivateKey**.

- valeur — Entrez une clé privée pour l'utilisateur. Cette valeur doit être stockée au SSH format Open et doit correspondre à la clé publique enregistrée pour cet utilisateur sur le serveur distant.

8. Choisissez Suivant.
9. Sur la page Configurer le secret, entrez le nom et la description de votre secret. Nous vous recommandons d'utiliser le préfixe de **aws/transfer/** pour le nom. Par exemple, vous pourriez donner un nom à votre secret **aws/transfer/connector-1**.
10. Choisissez Next, puis acceptez les valeurs par défaut sur la page Configurer la rotation. Ensuite, sélectionnez Suivant.
11. Sur la page Révision, choisissez Store pour créer et stocker le secret.

Après avoir créé le secret, vous pouvez le choisir lorsque vous créez un connecteur (voir [Configuration des AS2 connecteurs](#)). À l'étape où vous activez l'authentification de base, choisissez le secret dans la liste déroulante des secrets disponibles.

Afficher les détails AS2 du connecteur

Vous trouverez la liste des détails et des propriétés d'un AS2 AWS Transfer Family connecteur dans la AWS Transfer Family console. Les propriétés d'un AS2 connecteur incluent ses rôlesURL, ses profilsMDNs, ses balises et ses indicateurs de surveillance.

Il s'agit de la procédure permettant de visualiser les détails du connecteur.

Pour afficher les détails du connecteur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le panneau de navigation de gauche, choisissez Connectors (Connecteurs).
3. Choisissez l'identifiant dans la colonne ID du connecteur pour voir la page de détails du connecteur sélectionné.

Vous pouvez modifier les propriétés du AS2 connecteur sur la page de détails du connecteur en choisissant Modifier.

The screenshot displays the AWS Transfer Family console interface for a specific connector. The breadcrumb navigation at the top shows 'Transfer Family > Connectors > c-'. The connector ID 'c-' is visible in the top left, and a 'Delete' button is in the top right.

Connector configuration (Edit button):

- URL: http://
- Access role: [role name]
- Logging role: [role name]

Communication settings (Info button):

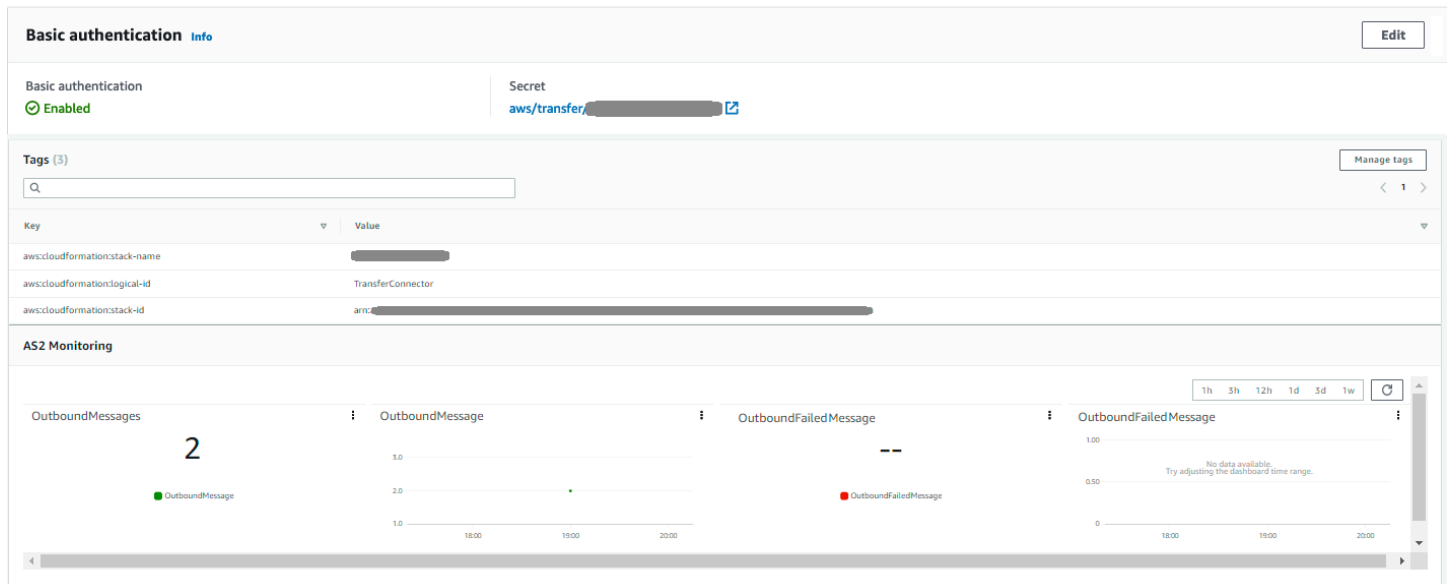
- AS2-From header: partner-test
- AS2-To header: local-test

AS2 configuration (Info button, Edit button):

- Local profile: partner-test
- Partner profile: local-test
- Compression: Disabled
- Message Subject: View
- Encryption algorithm: AES256_CBC
- Signing algorithm: SHA256

MDN configuration (Info button, Edit button):

- Request MDN: Enabled
- Signed MDN: Default to message signing algorithm: SHA256
- Synchronization: Enabled



Note

Vous pouvez obtenir la plupart de ces informations, bien que dans un format différent, en exécutant la AWS CLI commande suivante AWS Command Line Interface (:

```
aws transfer describe-connector --connector-id your-connector-id
```

Pour plus d'informations, consultez [.DescribeConnector](#) dans la API référence.

Gérer les AS2 partenaires

Cette rubrique explique comment gérer les AS2 certificats, les profils et les accords.

AS2Certificats d'importation

Le AS2 processus Transfer Family utilise des clés de certificat pour le chiffrement et la signature des informations transférées. Les partenaires peuvent utiliser la même clé dans les deux cas, ou une clé distincte pour chacune d'entre elles. Si vous disposez de clés de chiffrement communes conservées sous séquestre par un tiers de confiance afin que les données puissent être déchiffrées en cas de sinistre ou de faille de sécurité, nous vous recommandons de disposer de clés de signature distinctes. En utilisant des clés de signature distinctes (que vous ne transférez pas), vous ne compromettez pas les fonctionnalités de non-répudiation de vos signatures numériques.

 Note

La longueur de la clé pour les AS2 certificats doit être d'au moins 2 048 bits et d'au plus 4 096 bits.

Les points suivants détaillent la manière dont les AS2 certificats sont utilisés au cours du processus.

- Entrant AS2
 - Le partenaire commercial envoie sa clé publique pour le certificat de signature, et cette clé est importée dans le profil du partenaire.
 - La partie locale envoie la clé publique pour ses certificats de chiffrement et de signature. Le partenaire importe ensuite la ou les clés privées. La partie locale peut envoyer des clés de certificat distinctes pour la signature et le chiffrement, ou choisir d'utiliser la même clé dans les deux cas.
- Sortant AS2
 - Le partenaire envoie la clé publique pour son certificat de chiffrement, et cette clé est importée dans le profil du partenaire.
 - La partie locale envoie la clé publique du certificat à signer et importe la clé privée du certificat à signer.

Pour plus de détails sur la création de certificats, consultez [the section called “Étape 1 : créer des certificats pour AS2”](#).

Cette procédure explique comment importer des certificats à l'aide de la console Transfer Family. Si vous souhaitez utiliser le à la AWS CLI place, consultez [the section called “Étape 3 : Importer des certificats en tant que ressources de certificats Transfer Family”](#).

Pour spécifier un AS2 certificat activé

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, sous Partenaires AS2 commerciaux, sélectionnez Certificats.
3. Sélectionnez Importer un certificat.

4. Dans la section Description du certificat, entrez un nom facilement identifiable pour le certificat. Assurez-vous de pouvoir identifier l'objectif du certificat grâce à sa description. Choisissez également le rôle du certificat.
5. Dans la section Contenu du certificat, fournissez un certificat public d'un partenaire commercial ou les clés publiques et privées d'un certificat local.
6. Dans la section Utilisation du certificat, choisissez l'objectif de ce certificat. Il peut être utilisé pour le chiffrement, la signature ou les deux.

 Note

Si vous choisissez le chiffement et la signature pour l'utilisation, Transfer Family crée deux certificats identiques (chacun ayant son propre identifiant) : l'un avec une valeur d'utilisation de ENCRYPTION et l'autre avec une valeur d'utilisation de SIGNING.

7. Renseignez la section Contenu du certificat avec les informations appropriées.
 - Si vous choisissez Certificat auto-signé, vous ne fournissez pas la chaîne de certificats.
 - Collez le contenu du certificat.
 - S'il ne s'agit pas d'un certificat auto-signé, fournissez la chaîne de certificats.
 - S'il s'agit d'un certificat local, collez sa clé privée.
8. Choisissez Importer le certificat pour terminer le processus et enregistrer les détails du certificat importé.

AS2rotation des certificats

Souvent, les certificats sont valides pour une période de six mois à un an. Vous avez peut-être configuré des profils que vous souhaitez conserver plus longtemps. Pour faciliter cela, Transfer Family propose une rotation des certificats. Vous pouvez spécifier plusieurs certificats pour un profil, ce qui vous permet de continuer à utiliser le profil pendant plusieurs années. Transfer Family utilise des certificats pour la signature (facultatif) et le chiffement (obligatoire). Vous pouvez spécifier un seul certificat pour les deux objectifs, si vous le souhaitez.

La rotation des certificats consiste à remplacer un ancien certificat expirant par un certificat plus récent. La transition est progressive afin d'éviter de perturber les transferts lorsqu'un partenaire de l'accord n'a pas encore configuré de nouveau certificat pour les transferts sortants ou pourrait envoyer des charges utiles signées ou chiffrées avec un ancien certificat alors qu'un certificat plus

récent pourrait également être utilisé. La période intermédiaire pendant laquelle les anciens et les nouveaux certificats sont valides est appelée période de grâce.

Les certificats X.509 ont `Not Before` et `Not After` datent. Toutefois, il est possible que ces paramètres ne fournissent pas un contrôle suffisant aux administrateurs. Transfer Family fournit `Active Date` et `Inactive Date` paramètres permettant de contrôler quel certificat est utilisé pour les charges utiles sortantes et lequel est accepté pour les charges utiles entrantes.

La sélection des certificats sortants utilise la valeur maximale antérieure à la date du transfert en tant que `Inactive Date`. Les processus entrants acceptent les certificats compris entre `Active Date` et `Inactive Date`. `Not Before` et `Not After`

Le tableau suivant décrit une méthode possible pour configurer deux certificats pour un même profil.

Deux certificats en rotation

Nom	NOT BEFORE (contrôlé par l'autorité de certification)	ACTIVE DATE (défini par Transfer Family)	INACTIVE DATE (défini par Transfer Family)	NOT AFTER (défini par l'autorité de certification)
Cert1 (ancien certificat)	2019-11-01	01/01/2020	31 décembre 2020	01/01/2021
Cert2 (certificat plus récent)	2020-11-01	2020-06-01	01-06-2021	01/01/2025

Notez ce qui suit :

- Lorsque vous spécifiez un `Active Date` et `Inactive Date` pour un certificat, la plage doit être comprise entre `Not Before` et `Not After`.
- Nous vous recommandons de configurer plusieurs certificats pour chaque profil, en vous assurant que la plage de dates d'activité de tous les certificats combinés couvre la durée pendant laquelle vous souhaitez utiliser le profil.
- Nous vous recommandons de spécifier un délai de grâce entre le moment où votre ancien certificat devient inactif et le moment où votre nouveau certificat devient actif. Dans l'exemple précédent, le premier certificat ne devient inactif qu'au 31 décembre 2020, tandis que le second devient actif le 01/06/2020, offrant une période de grâce de 6 mois. Pendant la période allant du 01/06/2020 au 31/12/2020, les deux certificats sont actifs.

Création de AS2 profils

Utilisez cette procédure pour créer des profils locaux et partenaires. Cette procédure explique comment créer des AS2 profils à l'aide de la console Transfer Family. Si vous souhaitez utiliser le à la AWS CLI place, consultez [the section called “Étape 4 : Créez des profils pour vous et votre partenaire commercial”](#).

Pour créer un AS2 profil

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, sous Partenaires AS2 commerciaux, sélectionnez Profils, puis Créer un profil.
3. Dans la section Configuration du profil, entrez l'AS2ID du profil. Cette valeur est utilisée pour les HTTP en-têtes AS2 spécifiques au protocole as2-from et as2-to pour identifier le partenariat commercial, qui détermine les certificats à utiliser, etc.
4. Dans la section Type de profil, sélectionnez Profil local ou Profil partenaire.
5. Dans la section Certificats, choisissez un ou plusieurs certificats dans le menu déroulant.

Note

Si vous souhaitez importer un certificat qui ne figure pas dans le menu déroulant, sélectionnez Importer un nouveau certificat. Cela ouvre une nouvelle fenêtre de navigateur sur l'écran Importer le certificat. Pour la procédure d'importation de certificats, voir [AS2Certificats d'importation](#).

6. (Facultatif) Dans la section Tags, spécifiez une ou plusieurs paires clé-valeur pour aider à identifier ce profil.
7. Choisissez Créer un profil pour terminer le processus et enregistrer le nouveau profil.

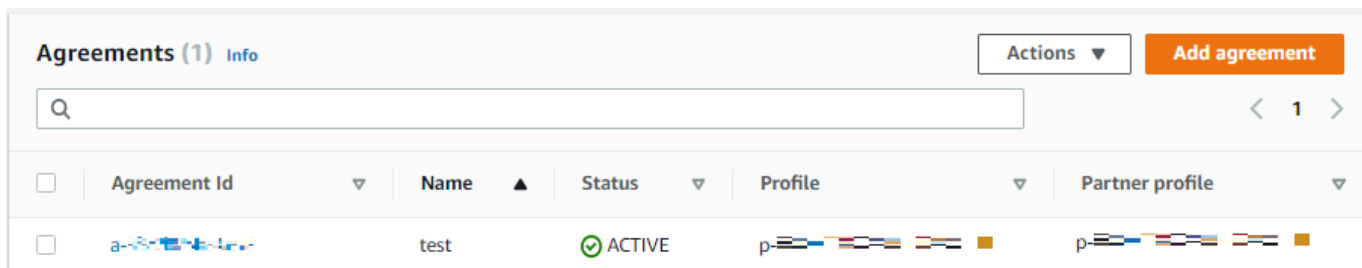
Créez des AS2 accords

Les accords sont associés aux serveurs Transfer Family. Ils précisent les détails pour les partenaires commerciaux qui utilisent le AS2 protocole pour échanger des messages ou des fichiers à l'aide de Transfer Family, pour les transferts entrants, c'est-à-dire l'envoi de AS2 fichiers depuis une source externe appartenant au partenaire vers un serveur Transfer Family.

Cette procédure explique comment créer des AS2 accords à l'aide de la console Transfer Family. Si vous souhaitez utiliser le à la AWS CLI place, consultez [the section called “Étape 5 : Créez un accord entre vous et votre partenaire”](#).

Pour créer un accord pour un serveur Transfer Family

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers, puis choisissez un serveur qui utilise le AS2 protocole.
3. Sur la page des détails du serveur, faites défiler la page vers le bas jusqu'à la section Accords.



4. Choisissez Ajouter un accord.
5. Renseignez les paramètres de l'accord comme suit :
 - a. Dans la section Configuration de l'accord, entrez un nom descriptif. Assurez-vous de pouvoir identifier le but de l'accord par son nom. Définissez également le statut de l'accord : actif (sélectionné par défaut) ou inactif.
 - b. Dans la section Configuration des communications, choisissez un profil local et un profil partenaire.
 - c. Dans la section Configuration du dossier de boîte de réception, choisissez un compartiment Amazon S3 pour stocker les fichiers entrants et un IAM rôle pouvant accéder au compartiment. Vous pouvez éventuellement saisir un préfixe (dossier) à utiliser pour stocker les fichiers dans le compartiment.

Par exemple, si vous entrez **DOC-EXAMPLE-BUCKET** votre bucket et **incoming** votre préfixe, vos fichiers entrants sont enregistrés **/DOC-EXAMPLE-BUCKET/incoming** dans le dossier.
 - d. (Facultatif) Ajoutez des balises dans la section Tags.
 - e. Après avoir saisi toutes les informations relatives à l'accord, choisissez Créer un accord.

Le nouvel accord apparaît dans la section Accords de la page de détails du serveur.

Envoyer et recevoir AS2 des messages

Cette section décrit les processus d'envoi et de réception de AS2 messages. Il fournit également des détails sur les noms de fichiers et les emplacements associés AS2 aux messages.

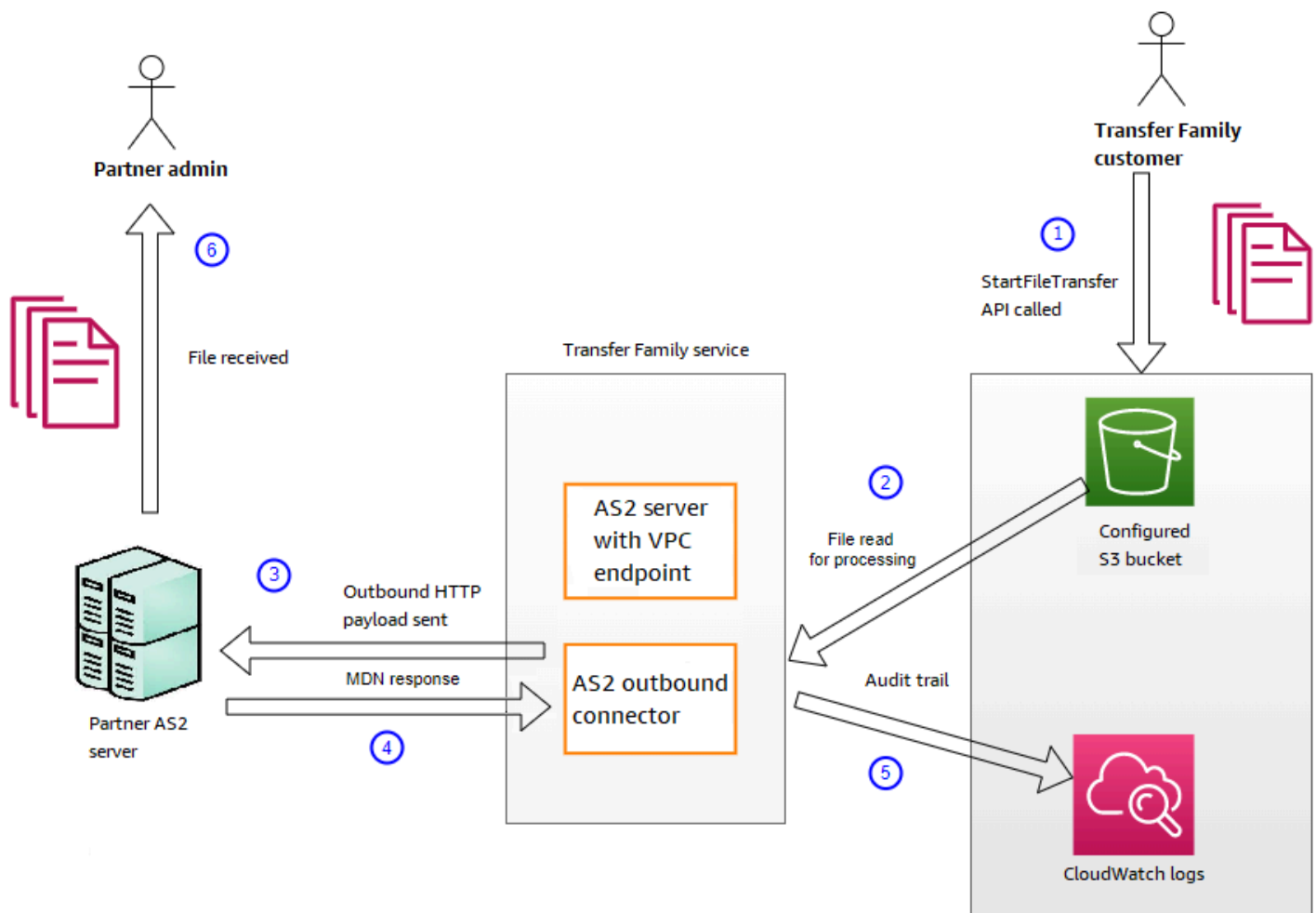
Rubriques

- [Processus d'envoi de AS2 message](#)
- [Processus de réception des AS2 messages](#)
- [Envoi et réception de AS2 messages via HTTPS](#)
- [Transférer des fichiers à l'aide d'un AS2 connecteur](#)
- [Noms et emplacements des fichiers](#)
- [Codes d'état](#)
- [JSONFichiers d'exemple](#)

Processus d'envoi de AS2 message

Le processus sortant est défini comme un message ou un fichier envoyé depuis AWS un client ou un service externe. La séquence des messages sortants est la suivante :

1. Un administrateur appelle la commande `start-file-transfer` AWS Command Line Interface (AWS CLI) ou `StartFileTransferAPI` opération. Cette opération fait référence à une `connector` configuration.
2. Transfer Family détecte une nouvelle demande de fichier et localise le fichier. Le fichier est compressé, signé et chiffré.
3. Un HTTP client de transfert exécute une HTTP POST demande pour transmettre la charge utile au AS2 serveur du partenaire.
4. Le processus renvoie la MDN réponse signée, en ligne avec la HTTP réponse (`synchronousMDN`).
5. Au fur et à mesure que le fichier passe d'une étape de transmission à l'autre, le processus fournit au client la réception de la MDN réponse et les détails du traitement.
6. Le AS2 serveur distant met le fichier déchiffré et vérifié à la disposition de l'administrateur partenaire.



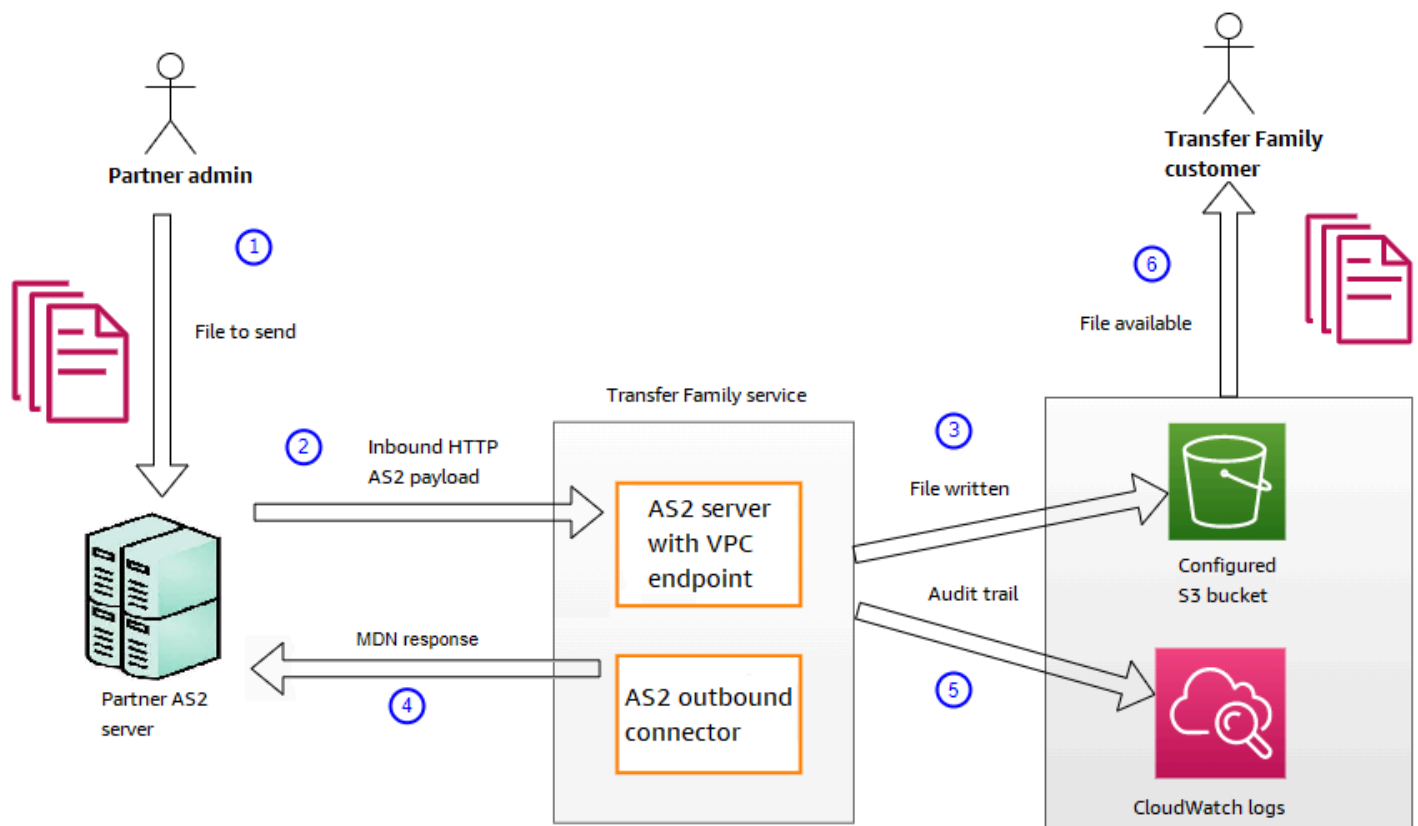
AS2le traitement prend en charge de nombreux protocoles RFC 4130, en mettant l'accent sur les cas d'utilisation courants et sur l'intégration avec les implémentations de serveurs AS2 compatibles existantes. Pour plus de détails sur les configurations prises en charge, consultez [AS2configurations prises en charge](#).

Processus de réception des AS2 messages

Le processus entrant est défini comme un message ou un fichier transféré vers votre AWS Transfer Family serveur. La séquence des messages entrants est la suivante :

1. Un administrateur ou un processus automatisé lance un transfert de AS2 fichiers sur le AS2 serveur distant du partenaire.
2. Le AS2 serveur distant du partenaire signe et chiffre le contenu du fichier, puis envoie une HTTP POST demande à un point de terminaison AS2 entrant hébergé sur Transfer Family.

3. À l'aide des valeurs configurées pour le serveur, les partenaires, les certificats et le contrat, Transfer Family déchiffre et vérifie la charge utile. AS2 Le contenu du fichier est stocké dans le magasin de fichiers Amazon S3 configuré.
4. La MDN réponse signée est renvoyée soit en ligne avec la HTTP réponse, soit de manière asynchrone par le biais d'une HTTP POST demande séparée envoyée au serveur d'origine.
5. Une piste d'audit contenant les détails de l'échange est écrite pour Amazon CloudWatch .
6. Le fichier déchiffré est disponible dans un dossier nommé. `inbox/processed`



Envoi et réception de AS2 messages via HTTPS

Cette section décrit comment configurer un serveur Transfer Family qui utilise le AS2 protocole pour envoyer et recevoir des messages HTTPS.

Envoyer AS2 des messages HTTPS

Pour envoyer AS2 des messages en utilisant HTTPS, créez un connecteur contenant les informations suivantes :

- Pour l'URL, spécifiez un HTTPS URL
- Pour l'algorithme de chiffrement, spécifiez NONE.
- Fournissez les valeurs restantes pour le connecteur, comme décrit dans [Configuration des AS2 connecteurs](#).

Recevez AS2 des messages HTTPS

AWS Transfer Family AS2 les serveurs fournissent actuellement uniquement le HTTP transport via le port 5080. Cependant, vous pouvez vous connecter TLS à un équilibreur de charge situé devant le point de VPC terminaison de votre serveur Transfer Family en utilisant le port et le certificat de votre choix. Avec cette approche, vous pouvez utiliser les AS2 messages entrants HTTPS.

Prérequis

- VPC Il doit se trouver sur le même serveur Région AWS que celui de votre Transfer Family.
- Les sous-réseaux de votre serveur VPC doivent se trouver dans les zones de disponibilité dans lesquelles vous souhaitez utiliser votre serveur.

Note

Chaque serveur Transfer Family peut prendre en charge jusqu'à trois zones de disponibilité.

- Allouez jusqu'à trois adresses IP élastiques dans la même région que votre serveur. Vous pouvez également choisir d'apporter votre propre plage d'adresses IP (BYOIP).

Note

Le nombre d'adresses IP élastiques doit correspondre au nombre de zones de disponibilité que vous utilisez avec les points de terminaison de votre serveur.

Configurez votre Network Load Balancer

Configurez un Network Load Balancer NLB () connecté à Internet dans votre VPC

Pour créer un Network Load Balancer et définir le VPC point de terminaison du serveur comme cible de l'équilibreur de charge

1. Ouvrez la console Amazon Elastic Compute Cloud à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers, puis Create load Balancer.
3. Sous Network Load Balancer, choisissez Créer.
4. Dans la section Configuration de base, entrez les informations suivantes :
 - Dans Nom, entrez un nom descriptif pour l'équilibreur de charge.
 - Pour Méthodes, choisissez Accessible sur Internet.
 - Pour IP address type (Type d'adresse IP), choisissez IPv4.
5. Dans la section Cartographie du réseau, entrez les informations suivantes :
 - Pour VPC, choisissez le cloud privé virtuel (VPC) que vous avez créé.
 - Sous Mappages, choisissez les zones de disponibilité associées aux sous-réseaux publics disponibles dans les mêmes zones que celles VPC que vous utilisez avec les points de terminaison de votre serveur.
 - Pour l'IPv4adresse de chaque sous-réseau, choisissez l'une des adresses IP élastiques que vous avez allouées.
6. Dans la section Écouteurs et routage, entrez les informations suivantes :
 - Pour Protocol (Protocole), choisissez TLS.
 - Pour Port, entrez **5080**.
 - Pour Action par défaut, choisissez Créer un groupe cible. Pour en savoir plus sur la création d'un nouveau groupe cible, consultez [Pour créer un groupe cible](#).

Après avoir créé un groupe cible, entrez son nom dans le champ Action par défaut.

7. Dans la section Paramètres de l'écouteur sécurisé, choisissez votre certificat dans la zone DefaultSSL/TLScertificate.
8. Choisissez Créer un équilibreur de charge pour créer votreNLB.
9. (Facultatif, mais recommandé) Activez les journaux d'accès au Network Load Balancer afin de conserver une piste d'audit complète, comme décrit dans la section [Journaux d'accès de votre Network](#) Load Balancer.

Nous recommandons cette étape car la TLS connexion est interrompue auNLB. Par conséquent, l'adresse IP source reflétée dans vos groupes de AS2 CloudWatch log Transfer Family est l'adresse IP privée NLB de votre partenaire commercial, et non l'adresse IP externe de votre partenaire commercial.

Après avoir configuré l'équilibreur de charge, les clients communiquent avec celui-ci via l'écouteur de port personnalisé. L'équilibreur de charge communique ensuite avec le serveur via le port 5080.

Pour créer un groupe cible

1. Après avoir choisi Créer un groupe cible dans la procédure précédente, vous êtes redirigé vers la page Spécifier les détails du groupe pour un nouveau groupe cible.
2. Dans la section Configuration de base, entrez les informations suivantes.
 - Pour Choisir un type de cible, choisissez les adresses IP.
 - Pour Nom du groupe cible, saisissez un nom pour le groupe cible.
 - Pour Protocol (Protocole), choisissez TCP.
 - Pour Port, entrez **5080**.
 - Pour IP address type (Type d'adresse IP), choisissez IPv4.
 - Pour VPC, choisissez celui VPC que vous avez créé pour votre AS2 serveur Transfer Family.
3. Dans la section Health checks, choisissez TCPIe protocole Health check.
4. Choisissez Suivant.
5. Sur la page Enregistrer les cibles, entrez les informations suivantes :
 - Pour Network, vérifiez que celui VPC que vous avez créé pour votre AS2 serveur Transfer Family est spécifié.
 - Pour IPv4l'adresse, entrez l'IPv4adresse privée des points de terminaison de votre AS2 serveur Transfer Family.

Si vous avez plusieurs points de terminaison pour votre serveur, choisissez Ajouter une IPv4 adresse pour ajouter une autre ligne permettant de saisir une autre IPv4 adresse. Répétez ce processus jusqu'à ce que vous ayez saisi les adresses IP privées de tous les points de terminaison de votre serveur.

- Assurez-vous que Ports est réglé sur**5080**.

- Choisissez Inclure comme en attente ci-dessous pour ajouter vos entrées à la section Objectifs de révision.
6. Dans la section Vérifier les cibles, passez en revue vos cibles IP.
 7. Choisissez Créer un groupe cible, puis revenez à la procédure précédente pour créer votre groupe cible NLB et entrez le nouveau groupe cible à l'endroit indiqué.

Tester l'accès au serveur depuis une adresse IP élastique

Connectez-vous au serveur via le port personnalisé en utilisant une adresse IP élastique ou le DNS nom du Network Load Balancer.

Important

Gérez l'accès à votre serveur à partir des adresses IP des clients en utilisant les [listes de contrôle d'accès réseau \(réseauACLs\)](#) pour les sous-réseaux configurés sur l'équilibreur de charge. Les ACL autorisations réseau sont définies au niveau du sous-réseau, de sorte que les règles s'appliquent à toutes les ressources qui utilisent le sous-réseau. Vous ne pouvez pas contrôler l'accès depuis les adresses IP des clients à l'aide de groupes de sécurité, car le type de cible de l'équilibreur de charge est défini sur les adresses IP plutôt que sur les instances. Par conséquent, l'équilibreur de charge ne conserve pas les adresses IP sources. Si les [vérifications de santé du Network Load Balancer](#) échouent, cela signifie que l'équilibreur de charge ne peut pas se connecter au point de terminaison du serveur. Pour résoudre ce problème, vérifiez les points suivants :

- Vérifiez que le [groupe de sécurité associé au point de terminaison](#) du serveur autorise les connexions entrantes provenant des sous-réseaux configurés sur l'équilibreur de charge. L'équilibreur de charge doit pouvoir se connecter au point de terminaison du serveur via le port 5080.
- Vérifiez que l'état du serveur est en ligne.

Transférer des fichiers à l'aide d'un AS2 connecteur

AS2 les connecteurs établissent une relation entre les partenaires commerciaux pour les transferts de AS2 messages d'un serveur Transfer Family vers une destination externe appartenant au partenaire.

Vous pouvez utiliser Transfer Family pour envoyer AS2 des messages en faisant référence à l'ID du connecteur et aux chemins d'accès aux fichiers, comme illustré dans la commande suivante `start-file-transfer` AWS Command Line Interface (AWS CLI) :

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \  
--send-file-paths "/DOC-EXAMPLE-SOURCE-BUCKET/myfile1.txt" "/DOC-EXAMPLE-SOURCE-BUCKET/  
myfile2.txt"
```

Pour obtenir les détails de vos connecteurs, exécutez la commande suivante :

```
aws transfer list-connectors
```

La `list-connectors` commande renvoie le connecteur IDs et Amazon Resource Names (ARNs) pour vos connecteurs. URLs

Pour renvoyer les propriétés d'un connecteur spécifique, exécutez la commande suivante avec l'ID que vous souhaitez utiliser :

```
aws transfer describe-connector --connector-id your-connector-id
```

La `describe-connector` commande renvoie toutes les propriétés du connecteur, notamment ses rôles, ses profilsURL, ses notifications de disposition des messages (MDNs), ses balises et ses mesures de surveillance.

Vous pouvez vérifier que le partenaire a bien reçu les fichiers en consultant les MDN fichiers JSON et. Ces fichiers sont nommés conformément aux conventions décrites dans [Noms et emplacements des fichiers](#). Si vous avez configuré un rôle de journalisation lors de la création du connecteur, vous pouvez également vérifier l'état des AS2 messages dans vos CloudWatch journaux.

Pour consulter les détails du AS2 connecteur, voir [Afficher les détails AS2 du connecteur](#). Pour plus d'informations sur la création de AS2 connecteurs, consultez [Configuration des AS2 connecteurs](#).

Noms et emplacements des fichiers

Cette section décrit les conventions de dénomination des fichiers pour AS2 les transferts.

Pour les transferts de fichiers entrants, tenez compte des points suivants :

- Vous spécifiez le répertoire de base dans un accord. Le répertoire de base est le nom du compartiment Amazon S3 associé à un préfixe, le cas échéant. Par exemple, /DOC-EXAMPLE-BUCKET/AS2-folder.
- Si un fichier entrant est traité avec succès, le fichier (et le JSON fichier correspondant) est enregistré /processed dans le dossier. Par exemple, /DOC-EXAMPLE-BUCKET/AS2-folder/processed.

Le JSON fichier contient les champs suivants :

- agreement-id
 - as2-from
 - as2-to
 - as2-message-id
 - transfer-id
 - client-ip
 - connector-id
 - failure-message
 - file-path
 - message-subject
 - mdn-message-id
 - mdn-subject
 - requester-file-name
 - requester-content-type
 - server-id
 - status-code
 - failure-code
 - transfer-size
- Si un fichier entrant ne peut pas être traité correctement, le fichier (et le JSON fichier correspondant) est enregistré /failed dans le dossier. Par exemple, /DOC-EXAMPLE-BUCKET/AS2-folder/failed.
 - Le fichier transféré est stocké dans le processed dossier sous le nom *original_filename.messageId.original_extension*. C'est-à-dire que l'ID du message pour le transfert est ajouté au nom du fichier, avant son extension d'origine.

- Un JSON fichier est créé et enregistré sous le nom `original_filename.messageId.original_extension.json`. Outre l'ID du message ajouté, la chaîne `.json` est ajoutée au nom du fichier transféré.
- Un fichier d'avis de disposition des messages (MDN) est créé et enregistré sous le nom `original_filename.messageId.original_extension.mdn`. Outre l'ID du message ajouté, la chaîne `.mdn` est ajoutée au nom du fichier transféré.
- Si un fichier entrant est nommé `ExampleFileInS3Payload.dat`, les fichiers suivants sont créés :
 - Fichier —
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - JSON –
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`
 - MDN –
`ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.`

Pour les transferts sortants, le nom est similaire, à la différence qu'il n'y a aucun fichier de message entrant et que l'ID de transfert du message transféré est également ajouté au nom du fichier. L'ID de transfert est renvoyé par l'`StartFileTransferAPI` opération (ou lorsqu'un autre processus ou script appelle cette opération).

- `transfer-id` s'agit d'un identifiant associé à un transfert de fichier. Toutes les demandes faisant partie d'un `StartFileTransfer` appel partagent un `transfer-id`.
- Le répertoire de base est le même que le chemin que vous utilisez pour le fichier source. En d'autres termes, le répertoire de base est le chemin que vous spécifiez dans l'`StartFileTransferAPI` opération ou la `start-file-transfer` AWS CLI commande. Par exemple :

```
aws transfer start-file-transfer --send-file-paths /DOC-EXAMPLE-BUCKET/AS2-folder/
file-to-send.txt
```

Si vous exécutez cette commande MDN et que JSON les fichiers sont enregistrés dans `/DOC-EXAMPLE-BUCKET/AS2-folder/processed` (pour les transferts réussis) ou `/DOC-EXAMPLE-BUCKET/AS2-folder/failed` (pour les transferts infructueux).

- Un JSON fichier est créé et enregistré sous le nom `original_filename.transferId.messageId.original_extension.json`.

- Un MDN fichier est créé et enregistré sous le nom `original_filename.transferId.messageId.original_extension.mdn`.
- Si un fichier sortant est nommé `ExampleFileOutTestOutboundSyncMdn.dat`, les fichiers suivants sont créés :
 - JSON – `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.json`
 - MDN – `ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.mdn`

Vous pouvez également consulter les CloudWatch journaux pour consulter les détails de vos transferts, y compris ceux qui ont échoué.

Codes d'état

Le tableau suivant répertorie tous les codes de statut qui peuvent être enregistrés dans les CloudWatch journaux lorsque vous ou votre partenaire envoyez un AS2 message. Les différentes étapes de traitement des messages s'appliquent à différents types de messages et sont destinées uniquement à la surveillance. Les FAILED états COMPLETED et représentent l'étape finale du traitement et sont visibles dans JSON les fichiers.

Code	Description	Le traitement est terminé ?
PROCESSING	Le message est en cours de conversion dans son format final. Par exemple, les étapes de décompression et de déchiffrement ont toutes deux ce statut.	Non
MDN_TRANSMIT	Le traitement des messages consiste à envoyer une MDN réponse.	Non
MDN_RECEIVE	Le traitement des messages reçoit une MDN réponse.	Non

Code	Description	Le traitement est terminé ?
COMPLETED	Le traitement des messages s'est terminé avec succès. Cet état inclut l'envoi MDN d'un message entrant ou pour MDN vérifier les messages sortants.	Oui
FAILED	Le traitement du message a échoué. Pour obtenir la liste des codes d'erreur, consultez Codes d'erreur AS2 .	Oui

JSONFichiers d'exemple

Cette section répertorie des exemples de JSON fichiers pour les transferts entrants et sortants, y compris des exemples de fichiers pour les transferts réussis et les transferts qui échouent.

Exemple de fichier sortant transféré avec succès :

```
{
  "requester-content-type": "application/octet-stream",
  "message-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
  "file-path": "/DOC-EXAMPLE-BUCKET/as2testcell10000/openAs2/TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
  "timestamp": "2022-07-11T06:30:10.791274Z"
}
```

Exemple de fichier sortant transféré sans succès :

```
{
  "failure-code": "HTTP_ERROR_RESPONSE_FROM_PARTNER",
  "status-code": "FAILED",
  "requester-content-type": "application/octet-stream",
  "subject": "Test run from Id da86e74d6e57464aae1a55b8596bad0a to partner
9f8474d7714e476e8a46ce8c93a48c6c",
  "transfer-size": 3198,
  "requester-file-name": "openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "as2-message-id": "9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned
status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
  "connector-id": "c-056e15cc851f4b2e9",
  "file-path": "/testbucket-4c1tq6ohjt9y/as2IntegCell10002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "timestamp": "2022-07-11T21:17:24.802378Z"
}
```

Exemple de fichier entrant transféré avec succès :

```
{
  "requester-content-type": "application/EDI-X12",
  "subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat sent from MyCompany
to PartnerA",
  "client-ip": "10.0.109.105",
  "requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfC0.dat",
  "as2-from": "MyCompany_OID",
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 1050,
  "mdn-subject": "Message Disposition Notification",
  "as2-message-id": "OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID",
  "as2-to": "PartnerA_OID",
  "agreement-id": "a-f5c5cbea5f7741988",
  "file-path": "processed/openAs2TestInboundAsyncMdn-
necco-5Ab6bTfC0.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID.dat",
  "server-id": "s-5f7422b04c2447ef9",
  "timestamp": "2022-07-11T23:36:36.105030Z"
}
```

Exemple de fichier entrant transféré sans succès :

```
{
  "failure-code": "INVALID_REQUEST",
  "status-code": "FAILED",
  "subject": "Sending a request from InboundHttpClientTests",
  "client-ip": "10.0.117.27",
  "as2-message-id": "testFailedLogs-TestRunConfig-Default-inbound-direct-
integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "as2-to": "0beff6af56c548f28b0e78841dce44f9",
  "failure-message": "Unsupported date format: 2022/123/456T",
  "agreement-id": "a-0ceec8ca0a3348d6a",
  "as2-from": "ab91a398aed0422d9dd1362710213880",
  "file-path": "failed/01187f15-523c-43ac-9fd6-51b5ad2b08f3.testFailedLogs-
TestRunConfig-Default-inbound-direct-integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "server-id": "s-0582af12e44540b9b",
  "timestamp": "2022-07-11T06:30:03.662939Z"
}
```

Surveillance de l'utilisation de l'AS2

Vous pouvez surveiller l'activité AS2 à l'aide d'Amazon CloudWatch et AWS CloudTrail. Pour consulter d'autres statistiques du serveur Transfer Family, voir [Amazon CloudWatch Logging pour AWS Transfer Family](#)

Métriques AS2

Métrique	Description
InboundMessage	Nombre total de messages AS2 reçus avec succès d'un partenaire commercial. Unités : nombre Période : 5 minutes
InboundFailedMessage	Nombre total de messages AS2 reçus sans succès d'un partenaire commercial. En d'autres termes, un partenaire commercial a envoyé un message, mais le serveur Transfer Family n'a pas réussi à le traiter.

Métrique	Description
	Unités : nombre
	Période : 5 minutes
OutboundMessage	Nombre total de messages AS2 envoyés avec succès depuis le serveur Transfer Family à un partenaire commercial. Unités : nombre Durée : 5 minutes
OutboundFailedMessage	Nombre total de messages AS2 envoyés sans succès à un partenaire commercial. En d'autres termes, ils ont été envoyés depuis le serveur Transfer Family, mais n'ont pas été reçus avec succès par le partenaire commercial. Unités : nombre Période : 5 minutes

Codes d'état AS2

Le tableau suivant répertorie tous les codes d'état qui peuvent être enregistrés dans les CloudWatch journaux lorsque vous ou votre partenaire envoyez un message AS2. Les différentes étapes de traitement des messages s'appliquent à différents types de messages et sont destinées uniquement à la surveillance. Les états COMPLETED et FAILED représentent l'étape finale du traitement et sont visibles dans les fichiers JSON.

Code	Description	Le traitement est terminé ?
EN TRAITEMENT	Le message est en cours de conversion dans son format final. Par exemple, les étapes de décompression et de	Non

Code	Description	Le traitement est terminé ?
	déchiffrement ont toutes deux ce statut.	
MDN_TRANSMIT	Le traitement des messages envoie une réponse MDN.	Non
MDN_RECEIVE	Le traitement des messages reçoit une réponse MDN.	Non
TERMINÉ	Le traitement des messages s'est terminé avec succès. Cet état inclut l'envoi d'un MDN pour un message entrant ou pour la vérification MDN des messages sortants.	Oui
ÉCHEC	Le traitement du message a échoué. Pour obtenir la liste des codes d'erreur, consultez Codes d'erreur AS2 .	Oui

Codes d'erreur AS2

Le tableau suivant répertorie et décrit les codes d'erreur que vous pouvez recevoir lors des transferts de fichiers AS2.

Codes d'erreur AS2

Code	Erreur	Description et résolution
ACCESS_DENIED	- Accès refusé. Vérifiez si votre rôle d'accès dispose des autorisations nécessaires. - Chemin de fichier non valide <i>send-file-path</i>	Se produit lors du traitement d'une StartFileTransfer demande dont l'une des requêtes SendFilePaths n'est pas valide ou est mal formée. En d'autres termes, le chemin ne contient pas le

Code	Erreur	Description et résolution
	Impossible d'obtenir les informations d'identification avec ErrorCode : code <i>d'erreur</i>	nom du compartiment Amazon S3 ou contient des caractères non valides. Cela se produit également si Transfer Family n'assume pas le rôle d'accès ou de journalisation. Assurez-vous que le chemin contient un nom de compartiment et un nom de clé Amazon S3 valides.
AGREEMENT_NOT_FOUND	Aucun accord n'a été trouvé.	Soit l'accord n'a pas été trouvé, soit il est associé à un profil inactif. Mettez à jour l'accord au sein du serveur Transfer Family pour inclure les profils actifs.
CONNECTOR_NOT_FOUND	Le connecteur ou la configuration associée est introuvable.	Soit le connecteur n'a pas été trouvé, soit il est associé à un profil inactif. Mettez à jour le connecteur pour inclure les profils actifs.

Code	Erreur	Description et résolution
CREDENTIALS_RETRIEVAL_FAILED	1. Secret introuvable dans Secrets Manager. 2. Impossible d'accéder à Secrets Manager. 3. Impossible de déchiffrer le secret dans Secrets Manager. 4. Impossible d'obtenir la valeur secrète en raison de la limitation.	Pour l'authentification AS2 Basic, le secret doit être correctement formaté. Les résolutions suivantes correspondent aux erreurs répertoriées dans la colonne précédente. 1. Assurez-vous que l'identifiant secret est correct. 2. Assurez-vous que le rôle d'accès dispose des autorisations appropriées pour lire le secret. Le rôle d'accès doit fournir un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la <code>StartFileTransfer</code> demande. Assurez-vous également que le rôle fournit un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer avec <code>StartFileTransfer</code>. 3. Si une clé gérée par le client est utilisée pour le secret, assurez-vous que le rôle d'accès dispose d'autorisations pour la clé AWS Key Management Service (AWS KMS).

Code	Erreur	Description et résolution
		4. Pour les quotas applicables, voir Quotas pour le traitement des secrets .
DECOMPRESSION_FAILED	Impossible de décompresser le message.	Soit le fichier envoyé est endommagé, soit l'algorithme de compression n'est pas valide. Renvoyez le message et vérifiez que la compression ZLIB est utilisée, ou renvoyez le message sans que la compression soit activée.
DECRYPT_FAILED	Impossible de déchiffrer l'ID du <i>message</i> . Assurez-vous que le partenaire dispose de la bonne clé de chiffrement publique.	Le déchiffrement a échoué. Vérifiez que le partenaire a envoyé une charge utile à l'aide d'un certificat valide et que le chiffrement a été effectué à l'aide d'un algorithme de chiffrement valide.
DECRYPT_FAILED_INVALID_SMIME_FORMAT	Impossible d'analyser le composant MIMEpart enveloppé.	La charge utile MIME est soit corrompue, soit dans un format SMIME non pris en charge. L'expéditeur doit s'assurer que le format qu'il utilise est pris en charge, puis renvoyer la charge utile.

Code	Erreur	Description et résolution
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	Aucune clé de déchiffrement correspondante n'a été trouvée.	Aucun certificat correspondant au message n'a été attribué au profil du partenaire, ou les certificats correspondant au message sont maintenant expirés ou ne sont plus valides. Vous devez mettre à jour le profil du partenaire et vous assurer qu'il contient un certificat valide.
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	<i>Décryptage de la charge utile SMIME demandé à l'aide d'un algorithme non pris en charge avec l'ID : Encryption-ID.</i>	L'expéditeur distant a envoyé une charge utile AS2 avec un algorithme de chiffrement non pris en charge. L'expéditeur doit choisir un algorithme de chiffrement pris en charge par AWS Transfer Family.
DUPLICATE_MESSAGE	Étape dupliquée ou traitée deux fois.	La charge utile comporte une étape de traitement dupliquée. Par exemple, il existe deux étapes de chiffrement. Renvoyez le message en une seule étape pour la signature, la compression et le chiffrement.

Code	Erreur	Description et résolution
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	Aucun certificat de chiffrement public valide n'a été trouvé dans le profil : <i>Local-Profile-ID</i>	Transfer Family tente de chiffrer un message sortant, mais aucun certificat de chiffrement n'a été trouvé pour le profil local. Options de résolution : • Assurez-vous que le profil local est associé à un certificat et à une clé privée pour le chiffrement. • Assurez-vous que le certificat de chiffrement est actuellement actif.
ENCRYPTION_FAILED	Impossible de chiffrer le nom du <i>fichier</i> .	Le fichier à envoyer n'est pas disponible pour le chiffrement. Vérifiez que le fichier se trouve à l'emplacement AS2 attendu et qu'il AWS Transfer Family est autorisé à le lire.
FILE_SIZE_TOO_LARGE	La taille du fichier est trop importante.	Cela se produit lors de l'envoi ou de la réception d'un fichier dont la taille dépasse la limite de taille de fichier.

Code	Erreur	Description et résolution
HTTP_ERROR_RESPONSE_FROM_PARTNER	<i>Partner-URL a renvoyé le statut 400 pour le message avec ID= Message-ID.</i>	La communication avec le serveur AS2 du partenaire a renvoyé un code de réponse HTTP inattendu. Le partenaire pourra peut-être fournir davantage de diagnostics à partir des journaux de son serveur AS2.
INSUFFICIENT_MESSAGE_SECURITY_UNENCRYPTED	Le chiffrement est obligatoire.	Le partenaire a envoyé un message non crypté à Transfer Family, qui n'est pas pris en charge. L'expéditeur doit utiliser une charge utile cryptée.
INVALID_ENDPOINT_PROTOCOL	Seuls les protocoles HTTP et HTTPS sont pris en charge.	Vous devez spécifier HTTP ou HTTPS comme protocole dans la configuration de votre connecteur AS2.

Code	Erreur	Description et résolution
INVALID_REQUEST	1. Il y a un problème avec un en-tête de message. 2. Impossible d'analyser le code JSON secret. Le code JSON secret ne correspondait pas au format attendu. 3. Le secret doit être une chaîne JSON. 4. Le nom d'utilisateur ne doit pas contenir de deux-points. Le nom d'utilisateur ne doit pas contenir de caractères de contrôle. Le nom d'utilisateur ne doit contenir que des caractères ASCII. Le mot de passe ne doit pas contenir de caractères de contrôle. Le mot de passe ne doit contenir que des caractères ASCII.	Cette erreur a plusieurs causes. Les résolutions suivantes correspondent aux erreurs répertoriées dans la colonne précédente. 1. Vérifiez les <code>as2-to</code> champs <code>as2-from</code> et. Assurez-vous que l'ID du message d'origine est correct pour le format MDN. Assurez-vous également qu'aucun en-tête AS2 n'est absent du format de l'ID du message. 2. Assurez-vous que la valeur secrète correspond au format documenté, comme décrit dans Activer l'authentification de base pour les AS2 connecteurs. 3. Assurez-vous que le secret est fourni sous forme de chaîne et non sous forme binaire. 4. Apportez les corrections nécessaires au nom d'utilisateur ou au mot de passe.

Code	Erreur	Description et résolution
INVALID_URL_FORMAT	Format d'URL non valide : <i>URL</i>	Cela se produit lorsque vous envoyez un message sortant à l'aide d'un connecteur configuré avec une URL mal formée. Assurez-vous que le connecteur est configuré avec une URL HTTP ou HTTPS valide.
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	Ne s'applique pas	Le destinataire ne peut pas authentifier l'expéditeur. Le partenaire commercial renvoie un MDN à Transfer Family avec le modificateur de disposition Error : authentication-failed.
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	Ne s'applique pas	Cela se produit lorsque le récepteur ne peut pas décompresser le contenu du message. Le partenaire commercial renvoie un MDN à Transfer Family avec le modificateur de disposition Error : decompression-failed.
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	Ne s'applique pas	Le destinataire ne peut pas déchiffrer le contenu du message. Le partenaire commercial renvoie un MDN à Transfer Family avec le modificateur de disposition Error : authentication-failed.

Code	Erreur	Description et résolution
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	Ne s'applique pas	Le destinataire s'attend à ce que le message soit signé ou chiffré, mais ce n'est pas le cas. Le partenaire commercial renvoie un MDN à Transfer Family avec le modificateur de disposition Error : insufficient-message-security. Activez la signature et/ou le chiffrement sur le connecteur pour répondre aux attentes du partenaire commercial.
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	Ne s'applique pas	Le récepteur ne peut pas vérifier l'intégrité du contenu. Le partenaire commercial renvoie un MDN à Transfer Family avec le modificateur de disposition Error : integrity-check-failed.
PATH_NOT_FOUND	Impossible de créer le chemin de <i>fichier du répertoire</i> . Le chemin parent n'a pas pu être trouvé.	Transfer Family tente de créer un répertoire dans le compartiment Amazon S3 du client, mais celui-ci est introuvable. Assurez-vous que chaque chemin mentionné dans la <code>StartFileTransfer</code> commande contient le nom d'un compartiment existant.

Code	Erreur	Description et résolution
SEND_FILE_NOT_FOUND	Le chemin du <i>fichier est introuvable</i> .	Transfer Family ne trouve pas le fichier lors de l'opération d'envoi de fichier. Vérifiez que le répertoire de base et le chemin configurés sont valides et que Transfer Family dispose des autorisations de lecture pour le fichier.
SERVER_NOT_FOUND	Impossible de trouver le serveur associé au message.	Transfer Family n'a pas pu trouver le serveur lors de la réception d'un message. Cela peut se produire si le serveur est supprimé pendant le traitement d'un message entrant.
SERVER_NOT_ONLINE	L' <i>ID du serveur</i> n'est pas en ligne.	Le serveur Transfer Family est hors ligne. Démarrez le serveur afin qu'il puisse recevoir et traiter les messages.
SIGNING_FAILED	Impossible de signer le fichier.	Le fichier à envoyer n'est pas disponible pour signature ou la signature n'a pas pu être effectuée. Vérifiez que le fichier se trouve à l'emplacement AS2 attendu et qu'il AWS Transfer Family est autorisé à le lire.

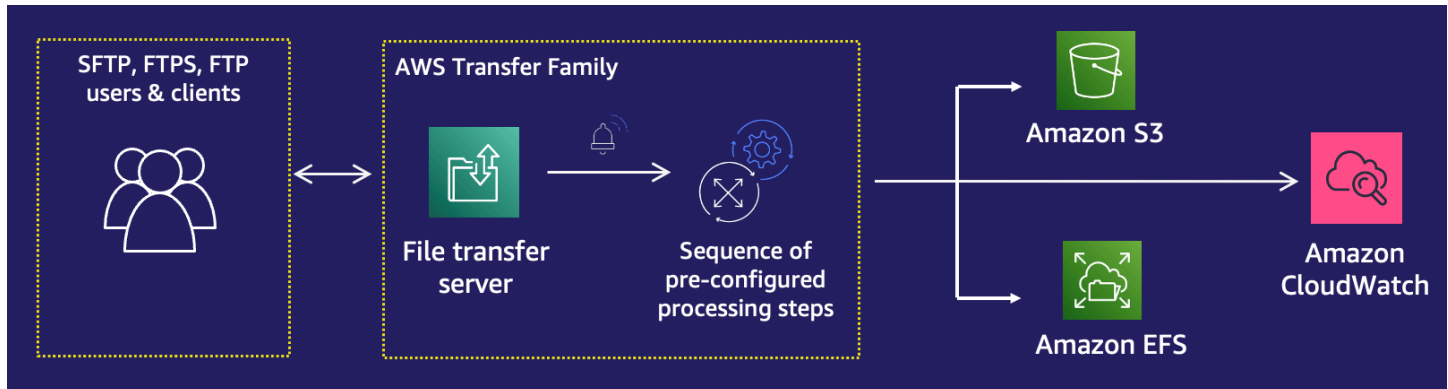
Code	Erreur	Description et résolution
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	Aucun certificat n'a été trouvé pour le profil : <i>Local-Profile-ID</i> .	Tentative de signature d'un message sortant, mais aucun certificat de signature n'a été trouvé pour le profil local. Options de résolution : - Assurez-vous que le profil local est associé à un certificat et à une clé privée pour la signature. - Assurez-vous que le certificat de signature est actuellement actif.
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	Impossible de convertir le nom d'hôte en adresses IP.	Transfer Family n'est pas en mesure d'effectuer la résolution du DNS en adresse IP sur le serveur DNS public configuré dans le connecteur AS2. Mettez à jour le connecteur pour qu'il pointe vers une URL de partenaire valide.
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	Le délai de connexion au point de terminaison a expiré.	Transfer Family ne peut pas établir de connexion socket avec le serveur AS2 configuré du partenaire. Vérifiez que le serveur AS2 du partenaire est disponible à l'adresse IP configurée.

Code	Erreur	Description et résolution
UNABLE_TO_RESOLVE_HOSTNAME	Impossible de résoudre le nom d' <i>hôte</i> .	Le serveur Transfer Family n'a pas pu résoudre le nom d'hôte du partenaire en utilisant un serveur DNS public. Vérifiez que l'hôte configuré est enregistré et que l'enregistrement DNS a eu le temps de publier.
VERIFICATION_FAILED	La vérification de signature a échoué pour l' <i>ID du message</i> AS2 ou un code MIC ne correspond pas.	Vérifiez que le certificat de signature de l'expéditeur correspond aux certificats de signature du profil distant. Vérifiez également que les algorithmes MIC sont compatibles avec AWS Transfer Family.

Code	Erreur	Description et résolution
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	- Aucun certificat public correspondant à la signature du message n'a été trouvé dans le profil : <i>Partner-Profile-ID</i> . - Impossible d'obtenir des certificats pour un profil inexistant : <i>Partner-Profile-ID</i> . - Aucun certificat valide n'a été trouvé dans le profil : <i>Partner-Profile-ID</i> .	AWS Transfer Family tente de vérifier la signature d'un message reçu, mais aucun certificat de signature correspondant n'est trouvé pour le profil du partenaire. Options de résolution : - Assurez-vous qu'un certificat de signature est joint au profil du partenaire. - Assurez-vous que le certificat est actuellement actif. - Assurez-vous que le certificat est le bon certificat de signature pour le partenaire.

AWS Transfer Family flux de travail gérés

AWS Transfer Family prend en charge les flux de travail gérés pour le traitement des fichiers. Avec les flux de travail gérés, vous pouvez lancer un flux de travail après le transfert d'un fichier SFTP/FTPS, ou FTP. Grâce à cette fonctionnalité, vous pouvez répondre de manière sûre et rentable à vos exigences de conformité pour les échanges de fichiers business-to-business (B2B) en coordonnant toutes les étapes nécessaires au traitement des fichiers. En outre, vous bénéficiez de l'end-to-end audit et de la visibilité.



En orchestrant les tâches de traitement de fichiers, les flux de travail gérés vous aident à prétraiter les données avant qu'elles ne soient consommées par vos applications en aval. Ces tâches de traitement de fichiers peuvent inclure :

- Déplacement de fichiers vers des dossiers spécifiques à l'utilisateur.
- Décryptage de fichiers dans le cadre d'un flux de travail.
- Marquage de fichiers.
- Exécution d'un traitement personnalisé en créant et en associant une AWS Lambda fonction à un flux de travail.
- Envoi de notifications lorsqu'un fichier a été transféré avec succès. (Pour un article de blog détaillant ce cas d'utilisation, voir [Personnaliser les notifications de livraison de fichiers à l'aide de flux de travail AWS Transfer Family gérés.](#))

Pour répliquer et standardiser rapidement les tâches courantes de traitement des fichiers après le téléchargement dans plusieurs unités commerciales de votre organisation, vous pouvez déployer des flux de travail en utilisant l'infrastructure en tant que code (iAc). Vous pouvez spécifier un flux de travail géré à lancer sur les fichiers téléchargés dans leur intégralité. Vous pouvez également spécifier un flux de travail géré différent à lancer sur les fichiers qui ne sont que partiellement

téléchargés en raison d'une déconnexion prématurée de session. La gestion intégrée des exceptions vous permet de réagir rapidement aux résultats du traitement des fichiers, tout en vous permettant de contrôler la manière de gérer les défaillances. En outre, chaque étape du flux de travail produit des journaux détaillés, que vous pouvez auditer pour tracer le lignage des données.

Pour commencer, effectuez les tâches suivantes :

1. Configurez votre flux de travail pour qu'il contienne des actions de prétraitement, telles que la copie, le balisage et d'autres étapes en fonction de vos besoins. Consultez [Création d'un flux de travail](#) pour plus de détails.
2. Configurez un rôle d'exécution que Transfer Family utilise pour exécuter le flux de travail. Consultez [IAMpolitiques relatives aux flux de travail](#) pour plus de détails.
3. Associez le flux de travail à un serveur, de sorte qu'à l'arrivée du fichier, les actions spécifiées dans ce flux de travail soient évaluées et initiées en temps réel. Consultez [Configuration et exécution d'un flux de travail](#) pour plus de détails.

Informations connexes

- Pour surveiller l'exécution de vos flux de travail, consultez [Utilisation CloudWatch des métriques pour Transfer Family](#).
- Pour obtenir des journaux d'exécution détaillés et des informations de dépannage, consultez [Résoudre les erreurs liées au flux de travail à l'aide d'Amazon CloudWatch](#).
- Vous pouvez participer à un atelier au cours duquel vous pouvez créer une solution de transfert de fichiers. Cette solution s'appuie sur les FTPS points de terminaison gérés SFTP et sur Amazon Cognito et DynamoDB AWS Transfer Family pour la gestion des utilisateurs. Vous pouvez consulter les détails de cet atelier [ici](#).
- Consultez [AWS Transfer Family Managed Workflows](#) pour une brève introduction aux flux de travail Transfer Family.

Rubriques

- [Création d'un flux de travail](#)
- [Utiliser des étapes prédéfinies](#)
- [Utiliser des étapes de traitement de fichiers personnalisées](#)
- [IAMpolitiques relatives aux flux de travail](#)
- [Gestion des exceptions pour un flux de travail](#)

- [Surveiller l'exécution du flux de](#)
- [Création d'un flux de travail à partir d'un modèle](#)
- [Supprimer un flux de travail d'un serveur Transfer Family](#)
- [Restrictions et limites des flux de travail gérés](#)

Pour obtenir de l'aide supplémentaire pour démarrer avec les flux de travail gérés, consultez les ressources suivantes :

- AWS Transfer Family vidéo de démonstration [des flux de travail gérés](#)
- Article de blog sur la [création d'une plateforme de transfert de fichiers native pour le cloud à l'aide AWS Transfer Family de workflows](#)

Création d'un flux de travail

Vous pouvez créer un flux de travail géré à l'aide du AWS Management Console, comme décrit dans cette rubrique. Pour faciliter au maximum le processus de création du flux de travail, des panneaux d'aide contextuels sont disponibles pour la plupart des sections de la console.

Un flux de travail comporte deux types d'étapes :

- Étapes nominales — Les étapes nominales sont des étapes de traitement de fichiers que vous souhaitez appliquer aux fichiers entrants. Si vous sélectionnez plusieurs étapes nominales, chaque étape est traitée selon une séquence linéaire.
- Étapes de gestion des exceptions — Les gestionnaires d'exceptions sont des étapes de traitement de fichiers qui AWS Transfer Family s'exécutent en cas d'échec d'une étape nominale ou d'erreur de validation.

Création d'un flux de travail

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, sélectionnez Workflows.
3. Sur la page Flux de travail, choisissez Créer un flux de travail.
4. Sur la page Créer un flux de travail, entrez une description. Cette description apparaît sur la page Workflows.

5. Dans la section Étapes nominales, choisissez Ajouter une étape. Ajoutez une ou plusieurs étapes.
 - a. Choisissez un type d'étape parmi les options disponibles. Pour plus d'informations sur les différents types d'étapes, consultez [the section called “Utiliser des étapes prédéfinies”](#).
 - b. Choisissez Next, puis configurez les paramètres de l'étape.
 - c. Choisissez Next, puis passez en revue les détails de l'étape.
 - d. Choisissez Créer une étape pour ajouter l'étape et continuer.
 - e. Continuez à ajouter des étapes selon vos besoins. Le nombre maximal d'étapes d'un flux de travail est de 8.
 - f. Après avoir ajouté toutes les étapes nominales nécessaires, faites défiler la page vers le bas jusqu'à la section Gestionnaires d'exceptions — facultatif, puis choisissez Ajouter une étape.

 Note

Pour être informé des défaillances en temps réel, nous vous recommandons de configurer des gestionnaires d'exceptions et des étapes à exécuter en cas d'échec de votre flux de travail.

6. Pour configurer les gestionnaires d'exceptions, ajoutez des étapes de la même manière que celle décrite précédemment. Si un fichier entraîne le lancement d'une exception par une étape, vos gestionnaires d'exceptions sont invoqués un par un.
7. (Facultatif) Faites défiler la page jusqu'à la section Balises et ajoutez des balises pour votre flux de travail.
8. Passez en revue la configuration, puis choisissez Créer un flux de travail.

 Important

Une fois que vous avez créé un flux de travail, vous ne pouvez pas le modifier. Veillez donc à examiner attentivement la configuration.

Configuration et exécution d'un flux de travail

Avant de pouvoir exécuter un flux de travail, vous devez l'associer à un serveur Transfer Family.

Pour configurer Transfer Family afin d'exécuter un flux de travail sur les fichiers téléchargés

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers.
 - Pour ajouter le flux de travail à un serveur existant, choisissez le serveur que vous souhaitez utiliser pour votre flux de travail.
 - Vous pouvez également créer un nouveau serveur et y ajouter le flux de travail. Pour de plus amples informations, veuillez consulter [Configuration d'un point SFTP de FTPS terminaison ou d'FTPun serveur](#).
3. Sur la page de détails du serveur, faites défiler la page vers le bas jusqu'à la section Détails supplémentaires, puis choisissez Modifier.

 Note

Par défaut, aucun flux de travail n'est associé aux serveurs. Vous utilisez la section Détails supplémentaires pour associer un flux de travail au serveur sélectionné.

4. Sur la page Modifier les informations supplémentaires, dans la section Flux de travail gérés, sélectionnez un flux de travail à exécuter sur tous les téléchargements.

 Note

Si vous n'avez pas encore de flux de travail, choisissez Créer un nouveau flux de travail pour en créer un.

- a. Choisissez l'ID de flux de travail à utiliser.
- b. Choisissez un rôle d'exécution. C'est le rôle que Transfer Family assume lors de l'exécution des étapes du flux de travail. Pour de plus amples informations, veuillez consulter [IAMpolitiques relatives aux flux de travail](#). Choisissez Save (Enregistrer).

Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w-

Create a new Workflow

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w-

Create a new Workflow

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

Note

Si vous ne souhaitez plus qu'un flux de travail soit associé au serveur, vous pouvez supprimer l'association. Pour plus de détails, consultez [Supprimer un flux de travail d'un serveur Transfer Family](#).

Pour exécuter un flux de travail

Pour exécuter un flux de travail, vous devez télécharger un fichier sur un serveur Transfer Family que vous avez configuré avec un flux de travail associé.

Note

Chaque fois que vous supprimez un flux de travail d'un serveur et que vous le remplacez par un nouveau, ou que vous mettez à jour la configuration du serveur (ce qui a un impact sur le rôle d'exécution d'un flux de travail), vous devez attendre environ 10 minutes avant d'exécuter le nouveau flux de travail. Le serveur Transfer Family met en cache les détails du flux de travail et met 10 minutes au serveur pour actualiser son cache.

En outre, vous devez vous déconnecter de toutes les SFTP sessions actives, puis vous reconnecter après la période d'attente de 10 minutes pour voir les modifications.

Exemple

```
# Execute a workflow
> sftp bob@s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com

Connected to s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com.
sftp> put doc1.pdf
Uploading doc1.pdf to /DOC-EXAMPLE-BUCKET/home/users/bob/doc1.pdf
doc1.pdf                                     100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

Une fois que votre fichier a été chargé, l'action définie est exécutée sur votre fichier. Par exemple, si votre flux de travail contient une étape de copie, le fichier est copié à l'emplacement que vous avez défini à cette étape. Vous pouvez utiliser Amazon CloudWatch Logs pour suivre les étapes exécutées et leur statut d'exécution.

Afficher les détails du flux de travail

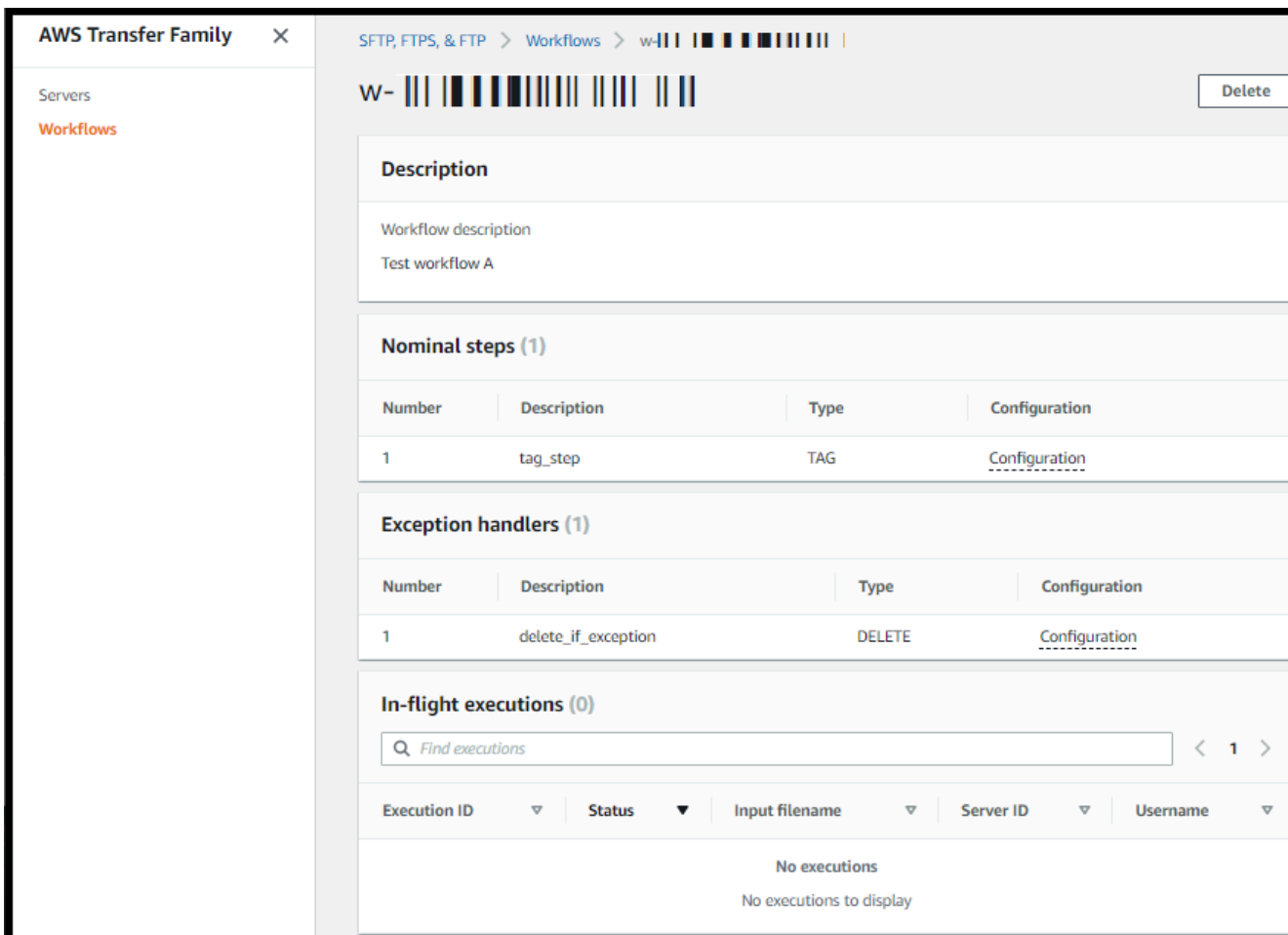
Vous pouvez consulter les détails relatifs aux flux de travail créés précédemment ou aux exécutions de flux de travail. Pour afficher ces informations, vous pouvez utiliser la console ou le AWS Command Line Interface (AWS CLI).

Console

Afficher les détails du flux de travail

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, sélectionnez Workflows.
3. Sur la page Flux de travail, choisissez un flux de travail.

La page des détails du flux de travail s'ouvre.



CLI

Pour afficher les détails du flux de travail, utilisez la `describe-workflow` CLI commande, comme indiqué dans l'exemple suivant. Remplacez l'ID du flux `w-1234567890abcdef0` de travail par votre propre valeur. Pour plus d'informations, voir [describe-workflow](#) dans la référence des AWS CLI commandes.

```
# View Workflow details
> aws transfer describe-workflow --workflow-id w-1234567890abcdef0
{
  "Workflow": {
    "Arn": "arn:aws:transfer:us-east-1:111122223333:workflow/w-1234567890abcdef0",
    "WorkflowId": "w-1234567890abcdef0",
    "Name": "Copy file to shared_files",
    "Steps": [
      {
```

```
        "Type": "COPY",
        "CopyStepDetails": {
          "Name": "Copy to shared",
          "FileLocation": {
            "S3FileLocation": {
              "Bucket": "DOC-EXAMPLE-BUCKET",
              "Key": "home/shared_files/"
            }
          }
        }
      ],
      "OnException": {}
    }
  }
```

Si votre flux de travail a été créé dans le cadre d'une AWS CloudFormation pile, vous pouvez le gérer à l'aide de la AWS CloudFormation console (<https://console.aws.amazon.com/cloudformation>).

Transfer Family > Workflows > workflow-stack-name

Workflow Stack Name

Delete

This workflow belongs to the AWS CloudFormation stack **WorkflowStack**. [Manage this stack](#) on the CloudFormation console.

Description

Workflow description

-

Nominal steps (1) Info

Number	Description	Type	Configuration
1	tagFileForArchive	TAG	Details

Exception handlers (0) Info

Number	Description	Type	Configuration

Utiliser des étapes prédéfinies

Lorsque vous créez un flux de travail, vous pouvez choisir d'ajouter l'une des étapes prédéfinies suivantes décrites dans cette rubrique. Vous pouvez également choisir d'ajouter vos propres étapes de traitement de fichiers personnalisées. Pour de plus amples informations, veuillez consulter [the section called “Utiliser des étapes de traitement de fichiers personnalisées”](#).

Rubriques

- [Copier le fichier](#)
- [Déchiffrer le fichier](#)
- [Fichier de balises](#)
- [Supprimer le fichier](#)
- [Variables nommées pour les flux de travail](#)
- [Exemple de balise et de flux de travail de suppression](#)

Copier le fichier

Une étape de copie de fichier crée une copie du fichier chargé dans un nouvel emplacement Amazon S3. Actuellement, vous ne pouvez utiliser une étape de copie de fichier qu'avec Amazon S3.

L'étape de copie de fichier suivante permet de copier les fichiers dans test le dossier du compartiment de file-test destination.

Si l'étape de copie du fichier n'est pas la première étape de votre flux de travail, vous pouvez spécifier l'emplacement du fichier. En spécifiant l'emplacement du fichier, vous pouvez copier soit le fichier utilisé à l'étape précédente, soit le fichier d'origine qui a été chargé. Vous pouvez utiliser cette fonctionnalité pour créer plusieurs copies du fichier original tout en conservant le fichier source intact pour l'archivage des fichiers et la conservation des dossiers. Pour obtenir un exemple, consultez [Exemple de balise et de flux de travail de suppression](#).

Configure copy parameters

Step name

File location

Select the file location to use as an input for this step

☒ Copy the file created from previous step to a new location

Input file is selected from the previous step's output

☐ Copy the original source file to a new location

Originally uploaded file

Destination bucket name

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

☐ Overwrite existing

Fournissez le compartiment et les informations clés

Vous devez fournir le nom du compartiment et une clé pour la destination de l'étape de copie du fichier. La clé peut être un nom de chemin ou un nom de fichier. Le fait que la clé soit traitée comme un nom de chemin ou comme un nom de fichier dépend de la fin de la clé par la barre oblique (/).

Si le dernier caractère est /, votre fichier est copié dans le dossier et son nom ne change pas. Si le dernier caractère est alphanumérique, le fichier téléchargé est renommé avec la valeur clé. Dans

ce cas, si un fichier portant ce nom existe déjà, le comportement dépend du paramètre du champ Remplacer existant.

- Si l'option Remplacer l'existant est sélectionnée, le fichier existant est remplacé par le fichier en cours de traitement.
- Si l'option Remplacer l'existant n'est pas sélectionnée, rien ne se passe et le traitement du flux de travail s'arrête.

Tip

Si des écritures simultanées sont exécutées sur le même chemin de fichier, cela peut entraîner un comportement inattendu lors du remplacement de fichiers.

Par exemple, si votre valeur clé est `test/`, les fichiers que vous avez téléchargés sont copiés `test` dans le dossier. Si votre valeur clé est `test/today`, (et que l'option Remplacer les fichiers existants est sélectionnée), chaque fichier que vous téléchargez est copié `today` dans un fichier nommé dans le `test` dossier, et chaque fichier suivant remplace le précédent.

Note

Amazon S3 prend en charge les compartiments et les objets. Il n'y a aucune hiérarchie. Cependant, vous pouvez utiliser des préfixes et des délimiteurs dans les noms de clés d'objets pour indiquer une hiérarchie et organiser vos données de la même manière que les dossiers.

Utiliser une variable nommée dans une étape de copie de fichier

Lors d'une étape de copie de fichier, vous pouvez utiliser une variable pour copier dynamiquement vos fichiers dans des dossiers spécifiques à l'utilisateur. Actuellement, vous pouvez utiliser `${transfer:UserName}` ou `${transfer:UploadDate}` en tant que variable pour copier des fichiers vers un emplacement de destination pour l'utilisateur donné qui télécharge les fichiers, ou en fonction de la date actuelle.

Dans l'exemple suivant, si l'utilisateur `richard-roe` télécharge un fichier, celui-ci est copié dans le `file-test2/richard-roe/processed/` dossier. Si l'utilisateur `mary-major` télécharge un fichier, celui-ci est copié dans le `file-test2/mary-major/processed/` dossier.

Configure parameters

Configure copy parameters

Step name

dynamic-copy

Destination bucket name

file-test2 ▼

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UserName}/processed`

☐ Overwrite existing

De même, vous pouvez l'utiliser `${transfer:UploadDate}` comme variable pour copier des fichiers vers un emplacement de destination nommé d'après la date actuelle. Dans l'exemple suivant, si vous définissez la destination `${transfer:UploadDate}/processed` sur le 1er février 2022, les fichiers téléchargés sont copiés dans le `file-test2/2022-02-01/processed/` dossier.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

file-test2

Destination key prefix

If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.

`${transfer:UploadDate}/processed`

☐ Overwrite existing

Vous pouvez également utiliser ces deux variables ensemble, en combinant leurs fonctionnalités. Par exemple :

- Vous pouvez définir le préfixe de la clé de destination sur **folder/\${transfer:UserName}/\${transfer:UploadDate}/**, ce qui créerait des dossiers imbriqués, par exemple. folder/marymajor/2023-01-05/
- Vous pouvez définir le préfixe de la clé de destination sur **folder/\${transfer:UserName}-\${transfer:UploadDate}/**, pour concaténer les deux variables, par exemple. folder/marymajor-2023-01-05/

IA M autorisations pour l'étape de copie

Pour qu'une étape de copie réussisse, assurez-vous que le rôle d'exécution de votre flux de travail contient les autorisations suivantes.

```
{  
    "Sid": "ListBucket",
```

```
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::destination-bucket-name"
    ],
  },
  {
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
  }
}
```

Note

L'`s3:ListBucket` autorisation n'est nécessaire que si vous ne sélectionnez pas Remplacer l'existant. Cette autorisation vérifie dans votre compartiment si un fichier portant le même nom existe déjà. Si vous avez sélectionné Remplacer l'existant, le flux de travail n'a pas besoin de vérifier la présence du fichier et peut simplement l'écrire.

Si vos fichiers Amazon S3 comportent des balises, vous devez ajouter une ou deux autorisations à votre IAM politique.

- Ajoutez `s3:GetObjectTagging` un fichier Amazon S3 qui n'est pas versionné.
- Ajoutez `s3:GetObjectVersionTagging` un fichier Amazon S3 versionné.

Déchiffrer le fichier

Le blog sur le AWS stockage contient un article qui décrit comment crypter et déchiffrer des fichiers, crypter et [déchiffrer des fichiers avec et](#). PGP AWS Transfer Family

Utilisez PGP le déchiffrement dans votre flux de travail

Transfer Family dispose d'un support intégré pour le déchiffrement de Pretty Good Privacy (PGP). Vous pouvez utiliser le PGP déchiffrement sur les fichiers chargés sur SFTP Amazon Simple Storage

Service (Amazon S3) ou FTP Amazon Elastic File System (Amazon)FTPS, ou sur Amazon Elastic File System (Amazon). EFS

Pour utiliser PGP le déchiffrement, vous devez créer et stocker les clés PGP privées qui seront utilisées pour le déchiffrement de vos fichiers. Vos utilisateurs peuvent ensuite chiffrer les fichiers à l'aide des clés de PGP chiffrement correspondantes avant de les télécharger sur votre serveur Transfer Family. Après avoir reçu les fichiers chiffrés, vous pouvez les déchiffrer dans votre flux de travail. Pour voir un didacticiel détaillé, consultez [Configuration d'un flux de travail géré pour le déchiffrement d'un fichier](#).

Pour utiliser le PGP déchiffrement dans votre flux de travail

1. Identifiez un serveur Transfer Family pour héberger votre flux de travail ou créez-en un nouveau. Vous devez disposer de l'ID du serveur avant de pouvoir stocker vos PGP clés AWS Secrets Manager avec le nom secret correct.
2. Enregistrez votre PGP clé AWS Secrets Manager sous le nom secret requis. Pour plus de détails, consultez [Gérer les clés PGP](#). Les flux de travail peuvent localiser automatiquement la bonne PGP clé à utiliser pour le déchiffrement en fonction du nom du secret dans Secrets Manager.

 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](#).

3. Chiffrez un fichier à l'aide de votre paire de PGP clés. (Pour obtenir la liste des clients pris en charge, voir [PGPClients pris en charge](#).) Si vous utilisez la ligne de commande, exécutez la commande suivante. Pour utiliser cette commande, remplacez-la *username@example.com* par l'adresse e-mail que vous avez utilisée pour créer la paire de PGP clés. *testfile.txt* Remplacez-le par le nom du fichier que vous souhaitez chiffrer.

```
gpg -e -r username@example.com testfile.txt
```

4. Téléchargez le fichier crypté sur votre serveur Transfer Family.
5. Configurez une étape de déchiffrement dans votre flux de travail. Pour de plus amples informations, veuillez consulter [Ajouter une étape de déchiffrement](#).

Ajouter une étape de déchiffrement

Une étape de déchiffrement déchiffre un fichier chiffré qui a été chargé sur Amazon S3 ou Amazon dans le EFS cadre de votre flux de travail. Pour plus de détails sur la configuration du déchiffrement, consultez [Utilisez PGP le déchiffrement dans votre flux de travail](#).

Lorsque vous créez votre étape de déchiffrement pour un flux de travail, vous devez spécifier la destination des fichiers déchiffrés. Vous devez également indiquer si vous souhaitez remplacer les fichiers existants si un fichier existe déjà à l'emplacement de destination. Vous pouvez surveiller les résultats du flux de déchiffrement et obtenir des journaux d'audit pour chaque fichier en temps réel à l'aide d'Amazon CloudWatch Logs.

Une fois que vous avez choisi le type de fichier de déchiffrement pour votre étape, la page Configurer les paramètres apparaît. Renseignez les valeurs de la section Configurer les paramètres de PGP déchiffrement.

Les options disponibles sont les suivantes :

- Nom de l'étape : entrez un nom descriptif pour l'étape.
- Emplacement du fichier — En spécifiant l'emplacement du fichier, vous pouvez déchiffrer soit le fichier utilisé à l'étape précédente, soit le fichier d'origine qui a été chargé.

Note

Ce paramètre n'est pas disponible s'il s'agit de la première étape du flux de travail.

- Destination des fichiers déchiffrés : choisissez un compartiment Amazon S3 ou un système de EFS fichiers Amazon comme destination du fichier déchiffré.
 - Si vous choisissez Amazon S3, vous devez fournir un nom de compartiment de destination et un préfixe de clé de destination. Pour paramétrer le préfixe de clé de destination par nom d'utilisateur, **`${transfer:UserName}`** entrez le préfixe de clé de destination. De même, pour paramétrer le préfixe de clé de destination par date de téléchargement, **`${Transfer:UploadDate}`** entrez le préfixe de clé de destination.
 - Si vous choisissez AmazonEFS, vous devez fournir un système de fichiers et un chemin de destination.

 Note

L'option de stockage que vous choisissez ici doit correspondre au système de stockage utilisé par le serveur Transfer Family auquel ce flux de travail est associé. Dans le cas contraire, vous recevrez un message d'erreur lorsque vous tenterez d'exécuter ce flux de travail.

- Remplacer un fichier existant : si vous chargez un fichier et qu'un fichier portant le même nom de fichier existe déjà à destination, le comportement dépend de la définition de ce paramètre :
 - Si l'option Remplacer l'existant est sélectionnée, le fichier existant est remplacé par le fichier en cours de traitement.
 - Si l'option Remplacer l'existant n'est pas sélectionnée, rien ne se passe et le traitement du flux de travail s'arrête.

 Tip

Si des écritures simultanées sont exécutées sur le même chemin de fichier, cela peut entraîner un comportement inattendu lors du remplacement de fichiers.

La capture d'écran suivante montre un exemple des options que vous pouvez choisir pour l'étape de déchiffrement du fichier.

Step 1

[Choose step type](#)

Step 2

Configure parameters

Step 3

Review and create

Configure parameters

Configure PGP decryption parameters

Store your PGP private key(s) and passphrase(s) in AWS Secrets Manager. [Learn more](#)

 Refer to the [AWS Transfer Family pricing page](#) for pricing details. 

Step name

File location

Select the file location to use as an input for this step

- ☒ **Apply on the file created from the previous step**
Input file is selected from the previous step's output
- ☐ **Apply on the original file**
Originally uploaded file

Destination for decrypted files

Choose an S3 bucket or an EFS file system for storing decrypted files.

- ☒ **Amazon S3**
Store your decrypted files as Amazon S3 objects
- ☐ **Amazon EFS**
Store your decrypted files in an EFS file system

Destination bucket name

Destination key prefix

If you are decrypting files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize the destination prefix by username or upload date respectively.

- ☐ **Overwrite existing**
Overwrite if a file with the same file name already exists at the destination.

IAM autorisations pour l'étape de déchiffrement

Pour qu'une étape de déchiffrement réussisse, assurez-vous que le rôle d'exécution de votre flux de travail contient les autorisations suivantes.

```
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::destination-bucket-name"
    ]
},
{
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
},
{
    "Sid": "Decrypt",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue",
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/"
}
*"
```

Note

L'`s3:ListBucket` autorisation n'est nécessaire que si vous ne sélectionnez pas Remplacer l'existant. Cette autorisation vérifie dans votre compartiment si un fichier portant le même nom existe déjà. Si vous avez sélectionné Remplacer l'existant, le flux de travail n'a pas besoin de vérifier la présence du fichier et peut simplement l'écrire.

Si vos fichiers Amazon S3 comportent des balises, vous devez ajouter une ou deux autorisations à votre IAM politique.

- Ajoutez `s3:GetObjectTagging` un fichier Amazon S3 qui n'est pas versionné.
- Ajoutez `s3:GetObjectVersionTagging` un fichier Amazon S3 versionné.

Fichier de balises

Pour étiqueter les fichiers entrants en vue d'un traitement ultérieur, utilisez une étape de balise. Entrez la valeur de la balise que vous souhaitez attribuer aux fichiers entrants. Actuellement, l'opération de balise n'est prise en charge que si vous utilisez Amazon S3 pour le stockage de votre serveur Transfer Family.

L'exemple d'étape de balise suivant affecte `scan_outcome` et `clean` en tant que clé et valeur de balise, respectivement.

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

Pour qu'une étape de balise réussisse, assurez-vous que le rôle d'exécution de votre flux de travail contient les autorisations suivantes.


```
{
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ]
}
```

Note

Si votre flux de travail contient une étape de balise qui s'exécute avant une étape de copie ou de déchiffrement, vous devez ajouter une ou deux autorisations à votre IAM politique.

- Ajoutez `s3:GetObjectTagging` un fichier Amazon S3 qui n'est pas versionné.
- Ajoutez `s3:GetObjectVersionTagging` un fichier Amazon S3 versionné.

Supprimer le fichier

Pour supprimer un fichier traité d'une étape précédente du flux de travail ou pour supprimer le fichier initialement chargé, utilisez une étape de suppression de fichier.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

Pour qu'une étape de suppression réussisse, assurez-vous que le rôle d'exécution de votre flux de travail contient les autorisations suivantes.

```
{
    "Sid": "Delete",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObjectVersion",
        "s3:DeleteObject"
    ],
    "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
* "
}
```

Variables nommées pour les flux de travail

Pour les étapes de copie et de déchiffrement, vous pouvez utiliser une variable pour effectuer des actions de manière dynamique. Actuellement, AWS Transfer Family prend en charge les variables nommées suivantes.

- `${transfer:UserName}` À utiliser pour copier ou déchiffrer des fichiers vers une destination en fonction de l'utilisateur qui télécharge les fichiers.
- `${transfer:UploadDate}` À utiliser pour copier ou déchiffrer des fichiers vers un emplacement de destination en fonction de la date actuelle.

Exemple de balise et de flux de travail de suppression

L'exemple suivant illustre un flux de travail qui balise les fichiers entrants devant être traités par une application en aval, telle qu'une plateforme d'analyse de données. Après avoir balisé le fichier entrant, le flux de travail supprime le fichier initialement chargé pour économiser sur les coûts de stockage.

Console

Exemple de processus de balisage et de déplacement

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, sélectionnez Workflows.
3. Sur la page Flux de travail, choisissez Créer un flux de travail.

4. Sur la page Créer un flux de travail, entrez une description. Cette description apparaît sur la page Workflows.
5. Ajoutez la première étape (copie).
 - a. Dans la section Étapes nominales, choisissez Ajouter une étape.
 - b. Choisissez Copier le fichier, puis Next.
 - c. Entrez le nom de l'étape, puis sélectionnez un compartiment de destination et un préfixe de clé.

Step 1
Choose step type

Step 2
Configure parameters

Step 3
Review and create

Configure parameters

Configure copy parameters

Step name
copy-step-first-step

Destination bucket name
example-bucket ▼

Destination key prefix
If you are copying files into a folder, specify / at the end of the prefix name. Use `${transfer:UserName}` or `${transfer:UploadDate}` to parametrize destination prefix by username or upload date respectively.
test/

☐ Overwrite existing

- d. Choisissez Next, puis passez en revue les détails de l'étape.
 - e. Choisissez Créer une étape pour ajouter l'étape et continuer.
6. Ajoutez la deuxième étape (tag).
 - a. Dans la section Étapes nominales, choisissez Ajouter une étape.
 - b. Choisissez Tag file, puis Next.
 - c. Entrez le nom de l'étape.
 - d. Pour Emplacement du fichier, sélectionnez Marquer le fichier créé à l'étape précédente.
 - e. Saisissez une Key (Clé) et une Value (Valeur).

Configure tag parameters

Step name
tag scan

File location
Select the file location to use as an input for this step

☒ Tag the file created from previous step
Input file is selected from the previous step's output

☐ Tag the original source file
Originally uploaded file

Tags

Key	Value
scan_outcome	clean

Remove tag

Add tag

- f. Choisissez Next, puis passez en revue les détails de l'étape.
 - g. Choisissez Créer une étape pour ajouter l'étape et continuer.
7. Ajoutez la troisième étape (supprimer).
- a. Dans la section Étapes nominales, choisissez Ajouter une étape.
 - b. Choisissez Supprimer le fichier, puis Suivant.

Configure delete parameters

Step name
delete original file

File location
Select the file location to use as an input for this step

☐ Delete the file created from previous step
Input file is selected from the previous step's output

☒ Delete the original source file
Originally uploaded file

- c. Entrez le nom de l'étape.

- d. Pour Emplacement du fichier, sélectionnez Supprimer le fichier source d'origine.
 - e. Choisissez Next, puis passez en revue les détails de l'étape.
 - f. Choisissez Créer une étape pour ajouter l'étape et continuer.
8. Vérifiez la configuration du flux de travail, puis choisissez Créer un flux de travail.

CLI

Exemple de processus de balisage et de déplacement

1. Enregistrez le code suivant dans un fichier ; par exemple, `tagAndMoveWorkflow.json`. Remplacez chaque *user input placeholder* par vos propres informations.

```
[
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "DOC-EXAMPLE-BUCKET",
          "Key": "test/"
        }
      }
    }
  },
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "demo"
        }
      ],
      "SourceFileLocation": "${previous.file}"
    }
  },
  {
    "Type": "DELETE",
    "DeleteStepDetails": {
```

```
        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
```

La première étape consiste à copier le fichier chargé vers un nouvel emplacement Amazon S3. La deuxième étape ajoute une balise (paire clé-valeur) au fichier (`previous.file`) qui a été copié vers le nouvel emplacement. Enfin, la troisième étape supprime le fichier d'origine (`original.file`).

2. Créez un flux de travail à partir du fichier enregistré. Remplacez chaque *user input placeholder* par vos propres informations.

```
aws transfer create-workflow --description "short-description" --steps
file://path-to-file --region region-ID
```

Par exemple :

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
file://tagAndMoveWorkflow.json --region us-east-1
```

 Note

Pour plus de détails sur l'utilisation de fichiers pour charger des paramètres, consultez [Comment charger des paramètres à partir d'un fichier](#).

3. Mettez à jour un serveur existant.

 Note

Cette étape suppose que vous possédez déjà un serveur Transfer Family et que vous souhaitez y associer un flux de travail. Si ce n'est pas le cas, voyez [Configuration d'un point SFTP de FTPS terminaison ou d'FTPun serveur](#). Remplacez chaque *user input placeholder* par vos propres informations.

```
aws transfer update-server --server-id server-ID --region region-ID
```

```
--workflow-details '{"OnUpload":[{"WorkflowId": "workflow-ID", "ExecutionRole": "execution-role-ARN"}]}'
```

Par exemple :

```
aws transfer update-server --server-id s-1234567890abcdef0 --region us-east-2  
--workflow-details '{"OnUpload":[{"WorkflowId": "w-  
abcdef01234567890", "ExecutionRole": "arn:aws:iam::111111111111:role/nikki-wolf-  
execution-role"}]}'
```

Utiliser des étapes de traitement de fichiers personnalisées

En utilisant une étape de traitement de fichiers personnalisée, vous pouvez apporter votre propre logique de traitement de fichiers en utilisant AWS Lambda. À l'arrivée du fichier, un serveur Transfer Family invoque une fonction Lambda qui contient une logique de traitement de fichiers personnalisée, telle que le chiffrement de fichiers, la recherche de logiciels malveillants ou la recherche de types de fichiers incorrects. Dans l'exemple suivant, la AWS Lambda fonction cible est utilisée pour traiter le fichier de sortie de l'étape précédente.

Configure custom parameters

Step name
custom file processing step

File location
Select the file location to use as an input for this step

☒ Apply custom processing to the file created from previous step
Input file is selected from the previous step's output

☐ Apply custom processing to the original source file
Originally uploaded file

Target
am:aws:lambda:us-east-2:1234567... ▼

Timeout (seconds)
60

Note

Pour obtenir un exemple de fonction Lambda, veuillez consulter [Exemple de fonction Lambda pour une étape de flux de travail personnalisée](#). Pour des exemples d'événements (y compris l'emplacement des fichiers transmis au Lambda), voir. [Exemples d'événements envoyés à une adresse AWS Lambda lors du chargement d'un fichier](#)

Avec une étape de flux de travail personnalisée, vous devez configurer la fonction Lambda pour appeler l'[SendWorkflowStepState](#) API opération. `SendWorkflowStepState` indique à l'exécution du flux de travail que l'étape s'est terminée avec un statut de réussite ou d'échec. L'état de l'`SendWorkflowStepState` API opération appelle une étape du gestionnaire d'exceptions ou une étape nominale dans la séquence linéaire, en fonction du résultat de la fonction Lambda.

Si la fonction Lambda échoue ou expire, l'étape échoue et cela apparaît `StepErrored` dans vos CloudWatch journaux. Si la fonction Lambda fait partie de l'étape nominale et que la fonction répond `SendWorkflowStepState` avec `Status="FAILURE"` ou expire, le flux continue avec les étapes du gestionnaire d'exceptions. Dans ce cas, le flux de travail ne continue pas à exécuter les étapes nominales restantes (le cas échéant). Pour en savoir plus, consultez [Gestion des exceptions pour un flux de travail](#).

Lorsque vous appelez l'`SendWorkflowStepState` API opération, vous devez envoyer les paramètres suivants :

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

Vous pouvez extraire le `ExecutionIdToken`, et `WorkflowId` de l'événement d'entrée transmis lors de l'exécution de la fonction Lambda (des exemples sont présentés dans les sections suivantes). La `Status` valeur peut être `SUCCESS` soit `FAILURE`.

Pour pouvoir appeler l'`SendWorkflowStepState` API opération depuis votre fonction Lambda, vous devez utiliser une version de celle-ci publiée après l' AWS SDK introduction de [Managed Workflows](#).

Utilisation consécutive de plusieurs fonctions Lambda

Lorsque vous utilisez plusieurs étapes personnalisées l'une après l'autre, l'option Emplacement du fichier fonctionne différemment que si vous n'utilisez qu'une seule étape personnalisée. Transfer Family ne prend pas en charge le transfert du fichier traité par Lambda pour qu'il soit réutilisé comme entrée de l'étape suivante. Ainsi, si plusieurs étapes personnalisées sont toutes configurées pour utiliser `previous.fileoption`, elles utilisent toutes le même emplacement de fichier (l'emplacement du fichier d'entrée pour la première étape personnalisée).

Note

Le `previous.file` paramètre fonctionne également différemment si vous avez une étape prédéfinie (marquer, copier, déchiffrer ou supprimer) après une étape personnalisée. Si l'étape prédéfinie est configurée pour utiliser le `previous.file` paramètre, elle utilise le même fichier d'entrée que celui utilisé par l'étape personnalisée. Le fichier traité à partir de l'étape personnalisée n'est pas transmis à l'étape prédéfinie.

Accès à un fichier après un traitement personnalisé

Si vous utilisez Amazon S3 comme espace de stockage, et si votre flux de travail inclut une étape personnalisée qui exécute des actions sur le fichier initialement chargé, les étapes suivantes ne peuvent pas accéder à ce fichier traité. En d'autres termes, aucune étape postérieure à l'étape personnalisée ne peut faire référence au fichier mis à jour à partir de la sortie de l'étape personnalisée.

Supposons, par exemple, que votre flux de travail comporte les trois étapes suivantes.

- Étape 1 — Téléchargez un fichier nommé `example-file.txt`.
- Étape 2 — Invoquez une fonction Lambda qui change d'une manière ou d'une `example-file.txt` autre.
- Étape 3 — Essayez d'effectuer un traitement supplémentaire sur la version mise à jour de `example-file.txt`.

Si vous configurez `sourceFileLocation` à l'étape 3 `${original.file}`, l'étape 3 utilise l'emplacement du fichier d'origine à partir du moment où le serveur a chargé le fichier vers le

stockage à l'étape 1. Si vous utilisez `${previous.file}` pour l'étape 3, l'étape 3 réutilise l'emplacement du fichier que l'étape 2 a utilisé comme entrée.

Par conséquent, l'étape 3 provoque une erreur. Par exemple, si l'étape 3 tente de copier la mise à jour `example-file.txt`, le message d'erreur suivant s'affiche :

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "NOT_FOUND",
    "errorMessage": "ETag constraint not met (Service: null; Status Code: 412; Error Code: null; Request ID: null; S3 Extended Request ID: null; Proxy: null)",
    "stepType": "COPY",
    "stepName": "CopyFile"
  },
}
```

Cette erreur se produit car l'étape personnalisée modifie la balise d'entité (ETag) pour `example-file.txt` qu'elle ne corresponde pas au fichier d'origine.

Note

Ce comportement ne se produit pas si vous utilisez Amazon EFS car Amazon EFS n'utilise pas de balises d'entité pour identifier les fichiers.

Exemples d'événements envoyés à une adresse AWS Lambda lors du chargement d'un fichier

Les exemples suivants montrent les événements qui sont envoyés AWS Lambda lorsque le téléchargement d'un fichier est terminé. Un exemple utilise un serveur Transfer Family où le domaine est configuré avec Amazon S3. L'autre exemple utilise un serveur Transfer Family où le domaine utilise AmazonEFS.

Custom step that uses an Amazon S3 domain

```
{
  "token": "MzI0Nzc4ZDktMGRmMi00MjFhLTgxMjUtYWZmZmRmODNkYjc0",
  "serviceMetadata": {
    "executionDetails": {
```

```

        "workflowId": "w-1234567890example",
        "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
    },
    "transferDetails": {
        "sessionId": "36688ff5d2deda8c",
        "userName": "myuser",
        "serverId": "s-example1234567890"
    }
},
"fileLocation": {
    "domain": "S3",
    "bucket": "DOC-EXAMPLE-BUCKET",
    "key": "path/to/mykey",
    "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
    "versionId": null
}
}

```

Custom step that uses an Amazon EFS domain

```

{
    "token": "MTg0N2Y3N2UtNWl5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
    "serviceMetadata": {
        "executionDetails": {
            "workflowId": "w-1234567890example",
            "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
        },
        "transferDetails": {
            "sessionId": "36688ff5d2deda8c",
            "userName": "myuser",
            "serverId": "s-example1234567890"
        }
    },
    "fileLocation": {
        "domain": "EFS",
        "fileSystemId": "fs-1234567",
        "path": "/path/to/myfile"
    }
}

```

Exemple de fonction Lambda pour une étape de flux de travail personnalisée

La fonction Lambda suivante extrait les informations relatives à l'état d'exécution, puis appelle l'[SendWorkflowStepState](#) API pour renvoyer le statut au flux de travail de l'étape SUCCESS, soit. FAILURE Avant que votre fonction n'appelle l'[SendWorkflowStepState](#) API, vous pouvez configurer Lambda pour qu'il exécute une action en fonction de votre logique de flux de travail.

```
import json
import boto3

transfer = boto3.client('transfer')

def lambda_handler(event, context):
    print(json.dumps(event))

    # call the SendWorkflowStepState API to notify the workflow about the step's
    # SUCCESS or FAILURE status
    response = transfer.send_workflow_step_state(
        WorkflowId=event['serviceMetadata']['executionDetails']['workflowId'],
        ExecutionId=event['serviceMetadata']['executionDetails']['executionId'],
        Token=event['token'],
        Status='SUCCESS|FAILURE'
    )

    print(json.dumps(response))

    return {
        'statusCode': 200,
        'body': json.dumps(response)
    }
```

IAuthorisations pour une étape personnalisée

Pour permettre à une étape qui appelle un Lambda de réussir, assurez-vous que le rôle d'exécution de votre flux de travail contient les autorisations suivantes.

```
{
    "Sid": "Custom",
    "Effect": "Allow",
```

```

    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": [
        "arn:aws:lambda:region:account-id:function:function-name"
    ]
}

```

IAM politiques relatives aux flux de travail

Lorsque vous ajoutez un flux de travail à un serveur, vous devez sélectionner un rôle d'exécution. Le serveur utilise ce rôle lorsqu'il exécute le flux de travail. Si le rôle ne dispose pas des autorisations appropriées, il AWS Transfer Family ne peut pas exécuter le flux de travail.

Cette section décrit un ensemble possible d'autorisations AWS Identity and Access Management (IAM) que vous pouvez utiliser pour exécuter un flux de travail. D'autres exemples sont décrits plus loin dans cette rubrique.

Note

Si vos fichiers Amazon S3 comportent des balises, vous devez ajouter une ou deux autorisations à votre IAM politique.

- Ajoutez `s3:GetObjectTagging` un fichier Amazon S3 qui n'est pas versionné.
- Ajoutez `s3:GetObjectVersionTagging` un fichier Amazon S3 versionné.

Pour créer un rôle d'exécution pour votre flux de travail

1. Créez un nouveau IAM rôle et ajoutez-y `AWSTransferFullAccess` la politique AWS gérée. Pour plus d'informations sur la création d'un nouveau IAM rôle, consultez [the section called “Création d'un IAM rôle et d'une politique”](#).
2. Créez une autre politique avec les autorisations suivantes et associez-la à votre rôle. Remplacez chaque *user input placeholder* par vos propres informations.

```

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

```

```

        "Sid": "ConsoleAccess",
        "Effect": "Allow",
        "Action": "s3:GetBucketLocation",
        "Resource": "*"
    },
    {
        "Sid": "ListObjectsInBucket",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        ]
    },
    {
        "Sid": "AllObjectActions",
        "Effect": "Allow",
        "Action": "s3:*Object",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ]
    },
    {
        "Sid": "GetObjectVersion",
        "Effect": "Allow",
        "Action": "s3:GetObjectVersion",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ]
    },
    {
        "Sid": "Custom",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:region:account-id:function:function-name"
        ]
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",

```

```

        "s3:PutObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ]
    }
  ]
}

```

3. Enregistrez ce rôle et spécifiez-le comme rôle d'exécution lorsque vous ajoutez un flux de travail à un serveur.

Note

Lorsque vous créez des IAM rôles, il est AWS recommandé de restreindre l'accès à vos ressources autant que possible pour votre flux de travail.

Relations de confiance en matière de flux

Les rôles d'exécution du flux de travail nécessitent également une relation de confiance avec `transfer.amazonaws.com`. Pour établir une relation de confiance pour AWS Transfer Family, voir [Étape 1 : Établir une relation d'approbation](#).

Pendant que vous établissez votre relation de confiance, vous pouvez également prendre des mesures pour éviter le problème de confusion des adjoints. Pour une description de ce problème, ainsi que des exemples permettant de l'éviter, reportez-vous à [the section called "Prévention du problème de l'adjoint confus entre services"](#).

Exemple de rôle d'exécution : déchiffrer, copier et étiqueter

Si vos flux de travail incluent des étapes de balisage, de copie et de déchiffrement, vous pouvez appliquer la politique suivante IAM. Remplacez chaque *user input placeholder* par vos propres informations.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyRead",
      "Effect": "Allow",

```

```

    "Action": [
      "s3:GetObject",
      "s3:GetObjectTagging",
      "s3:GetObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::source-bucket-name/*"
  },
  {
    "Sid": "CopyWrite",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*"
  },
  {
    "Sid": "CopyList",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
      "arn:aws:s3:::source-bucket-name",
      "arn:aws:s3:::destination-bucket-name"
    ]
  },
  {
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
      "s3:PutObjectTagging",
      "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::destination-bucket-name/*",
    "Condition": {
      "StringEquals": {
        "s3:RequestObjectTag/Archive": "yes"
      }
    }
  },
  {
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [

```



```

        "arn:aws:s3:::destination-bucket-name"
    ],
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObjectVersion",
            "s3:DeleteObject",
            "s3:GetObjectVersion"
        ],
        "Resource": "arn:aws:s3:::destination-bucket-name/*"
    },
    {
        "Sid": "Decrypt",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/"
    }
]
}

```

Exemple de rôle d'exécution : Exécuter la fonction et supprimer

Dans cet exemple, vous avez un flux de travail qui appelle une AWS Lambda fonction. Si le flux de travail supprime le fichier chargé et comporte une étape de gestion des exceptions pour agir en cas d'échec de l'exécution du flux de travail à l'étape précédente, appliquez la politique suivante IAM.

Remplacez chaque *user input placeholder* par vos propres informations.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Delete",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ]
        }
    ]
}

```

```
    ],
    "Resource": "arn:aws:s3:::bucket-name"
  },
  {
    "Sid": "Custom",
    "Effect": "Allow",
    "Action": [
      "lambda:InvokeFunction"
    ],
    "Resource": [
      "arn:aws:lambda:region:account-id:function:function-name"
    ]
  }
]
```

Gestion des exceptions pour un flux de travail

Si des erreurs se produisent lors de l'exécution d'un flux de travail, les étapes de gestion des exceptions que vous avez spécifiées sont exécutées. Vous spécifiez les étapes de gestion des erreurs pour un flux de travail de la même manière que vous spécifiez les étapes nominales pour le flux de travail. Supposons, par exemple, que vous ayez configuré un traitement personnalisé par étapes nominales pour valider les fichiers entrants. Si la validation du fichier échoue, une étape de gestion des exceptions peut envoyer un e-mail à l'administrateur.

L'exemple de flux de travail suivant contient deux étapes :

- Une étape nominale qui vérifie si le fichier téléchargé est au CSV format
- Une étape de gestion des exceptions qui envoie un e-mail au cas où le fichier téléchargé n'est pas au CSV format et que l'étape nominale échoue

Pour lancer l'étape de gestion des exceptions, la AWS Lambda fonction de l'étape nominale doit répondre par `Status="FAILURE"` Pour plus d'informations sur la gestion des erreurs dans les flux de travail, consultez [the section called “Utiliser des étapes de traitement de fichiers personnalisées”](#).

w-1234567890abcdef0 Delete			
Description			
Workflow description			
Check for CSV files			
Nominal steps (1) Info			
Number	Description	Type	Configuration
1	is-CSV	CUSTOM	Details
Exception handlers (1) Info			
Number	Description	Type	Configuration
1	send-email	CUSTOM	Details

Surveiller l'exécution du flux de

Amazon CloudWatch surveille vos AWS ressources et les applications que vous exécutez AWS Cloud en temps réel. Vous pouvez utiliser Amazon CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer pour vos flux de travail. Vous pouvez consulter les statistiques du flux de travail et les journaux consolidés à l'aide d'Amazon CloudWatch.

CloudWatch journalisation pour un flux de travail

CloudWatch fournit un audit et une journalisation consolidés de la progression et des résultats du flux de travail.

Afficher les CloudWatch journaux Amazon pour les flux de travail

1. Ouvrez la CloudWatch console Amazon à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le volet de navigation de gauche, choisissez Logs, puis Log groups.
3. Sur la page Groupes de journaux, dans la barre de navigation, choisissez la région appropriée pour votre AWS Transfer Family serveur.
4. Choisissez le groupe de journaux correspondant à votre serveur.

Par exemple, si l'ID de votre serveur est `-1234567890abcdef0`, votre groupe de journaux l'est `/aws/transfer/s-1234567890abcdef0`.

5. Sur la page des détails du groupe de journaux de votre serveur, les flux de journaux les plus récents sont affichés. Il existe deux flux de log pour l'utilisateur que vous explorez :
 - Un pour chaque session Secure Shell (SSH) File Transfer Protocol (SFTP).
 - Un pour le flux de travail en cours d'exécution pour votre serveur. Le format du flux de journal pour le flux de travail est `username.workflowID.uniqueStreamSuffix`.

Par exemple, si votre utilisateur l'est `mary-major`, vous disposez des flux de journaux suivants :

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

 Note

Les identifiants alphanumériques à 16 chiffres répertoriés dans cet exemple sont fictifs. Les valeurs que vous voyez sur Amazon CloudWatch sont différentes.

La page Enregistrer les événements de `mary-major-usa-east.1234567890abcdef0` affiche les détails de chaque session utilisateur, et le flux de `mary.w-abcdef01234567890.021345abcdef6789` journal contient les détails du flux de travail.

Voici un exemple de flux de journal pour `mary.w-abcdef01234567890.021345abcdef6789`, basé sur un flux de travail (`w-abcdef01234567890`) contenant une étape de copie.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "DOC-EXAMPLE-BUCKET",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  }
}
```

```

    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepStarted",
    "details": {
      "input": {
        "fileLocation": {
          "backingStore": "S3",
          "bucket": "DOC-EXAMPLE-BUCKET",
          "key": "mary/workflowSteps2.json",
          "versionId": "version-id",
          "etag": "etag-id"
        }
      },
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  },
  {
    "type": "StepCompleted",
    "details": {
      "output": {},
      "stepType": "COPY",
      "stepName": "copyToShared"
    },
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "server-id",
      "username": "mary",

```

```
    "sessionId": "session-id"
  },
  {
    "type": "ExecutionCompleted",
    "details": {},
    "workflowId": "w-abcdef01234567890",
    "executionId": "execution-id",
    "transferDetails": {
      "serverId": "s-server-id",
      "username": "mary",
      "sessionId": "session-id"
    }
  }
}
```

CloudWatch métriques pour les flux de travail

AWS Transfer Family fournit plusieurs mesures pour les flux de travail. Vous pouvez consulter les statistiques indiquant le nombre d'exécutions de flux de travail démarrées, terminées avec succès et échouées au cours de la minute précédente. Toutes les CloudWatch mesures relatives à Transfer Family sont décrites dans [Utilisation CloudWatch des métriques pour Transfer Family](#).

Création d'un flux de travail à partir d'un modèle

Vous pouvez déployer une AWS CloudFormation pile qui crée un flux de travail et un serveur à partir d'un modèle. Cette procédure contient un exemple que vous pouvez utiliser pour déployer rapidement un flux de travail.

Pour créer une AWS CloudFormation pile qui crée un AWS Transfer Family flux de travail et un serveur

1. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Enregistrez le code suivant dans un fichier.

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  SFTPServer:
    Type: 'AWS::Transfer::Server'
```

```

Properties:
  WorkflowDetails:
    OnUpload:
      - ExecutionRole: workflow-execution-role-arn
      WorkflowId: !GetAtt
        - TransferWorkflow
        - WorkflowId
  TransferWorkflow:
    Type: AWS::Transfer::Workflow
  Properties:
    Description: Transfer Family Workflows Blog
    Steps:
      - Type: COPY
      CopyStepDetails:
        Name: copyToUserKey
        DestinationFileLocation:
          S3FileLocation:
            Bucket: archived-records
            Key: ${transfer:UserName}/
            OverwriteExisting: 'TRUE'
      - Type: TAG
      TagStepDetails:
        Name: tagFileForArchive
        Tags:
          - Key: Archive
            Value: yes
      - Type: CUSTOM
      CustomStepDetails:
        Name: transferExtract
        Target: arn:aws:lambda:region:account-id:function:function-name
        TimeoutSeconds: 60
      - Type: DELETE
      DeleteStepDetails:
        Name: DeleteInputFile
        SourceFileLocation: '${original.file}'
    Tags:
      - Key: Name
        Value: TransferFamilyWorkflows

```

JSON

```

{
  "AWSTemplateFormatVersion": "2010-09-09",

```

```

"Resources": {
  "SFTPServer": {
    "Type": "AWS::Transfer::Server",
    "Properties": {
      "WorkflowDetails": {
        "OnUpload": [
          {
            "ExecutionRole": "workflow-execution-role-arn",
            "WorkflowId": {
              "Fn::GetAtt": [
                "TransferWorkflow",
                "WorkflowId"
              ]
            }
          ]
        }
      }
    }
  },
  "TransferWorkflow": {
    "Type": "AWS::Transfer::Workflow",
    "Properties": {
      "Description": "Transfer Family Workflows Blog",
      "Steps": [
        {
          "Type": "COPY",
          "CopyStepDetails": {
            "Name": "copyToUserKey",
            "DestinationFileLocation": {
              "S3FileLocation": {
                "Bucket": "archived-records",
                "Key": "${transfer:UserName}/"
              }
            },
            "OverwriteExisting": "TRUE"
          }
        },
        {
          "Type": "TAG",
          "TagStepDetails": {
            "Name": "tagFileForArchive",
            "Tags": [
              {
                "Key": "Archive",

```



```

        "Value": "yes"
    }
}
],
{
    "Type": "CUSTOM",
    "CustomStepDetails": {
        "Name": "transferExtract",
        "Target": "arn:aws:lambda:region:account-id:function:function-name",
        "TimeoutSeconds": 60
    }
},
{
    "Type": "DELETE",
    "DeleteStepDetails": {
        "Name": "DeleteInputFile",
        "SourceFileLocation": "${original.file}"
    }
}
],
"Tags": [
    {
        "Key": "Name",
        "Value": "TransferFamilyWorkflows"
    }
]
}
}
}
}

```

3. Remplacez les éléments suivants par vos valeurs réelles.

- Remplacez *workflow-execution-role-arn* avec le ARN pour un rôle d'exécution de flux de travail réel. Par exemple, `arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0`
- `arn:aws:lambda:region:account-id:function:function-name` Remplacez-le par le ARN pour votre fonction Lambda. Par exemple, `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`.

4. Suivez les instructions pour déployer une AWS CloudFormation pile à partir d'un modèle existant dans la section [Sélection d'un modèle de pile](#) dans le guide de AWS CloudFormation l'utilisateur.

Une fois la pile déployée, vous pouvez consulter les détails la concernant dans l'onglet Sorties de la CloudFormation console. Le modèle crée un nouveau AWS Transfer Family SFTP serveur qui utilise des utilisateurs gérés par des services, ainsi qu'un nouveau flux de travail, et associe le flux de travail au nouveau serveur.

Supprimer un flux de travail d'un serveur Transfer Family

Si vous avez associé un flux de travail à un serveur Transfer Family et que vous souhaitez à présent supprimer cette association, vous pouvez le faire à l'aide de la console ou par programmation.

Console

Pour supprimer un flux de travail d'un serveur Transfer Family

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers.
3. Choisissez l'identifiant du serveur dans la colonne ID du serveur.
4. Sur la page de détails du serveur, faites défiler la page vers le bas jusqu'à la section Détails supplémentaires, puis choisissez Modifier.
5. Sur la page Modifier les informations supplémentaires, dans la section Flux de travail gérés, effacez les informations relatives à tous les paramètres :
 - Sélectionnez le tiret (-) dans la liste des flux de travail pour le flux de travail pour les téléchargements complets de fichiers.
 - Si ce n'est pas déjà fait, sélectionnez le tiret (-) dans la liste des flux de travail pour le flux de travail pour les téléchargements partiels de fichiers.
 - Sélectionnez le tiret (-) dans la liste des rôles pour le rôle d'exécution des flux de travail gérés.

Si vous ne voyez pas le tiret, faites défiler l'écran vers le haut jusqu'à ce qu'il apparaisse, car il s'agit de la première valeur de chaque menu.

L'écran doit ressembler à ce qui suit.

- Faites défiler l'écran vers le bas et choisissez Enregistrer pour enregistrer vos modifications.

CLI

Vous utilisez l'appel `update-server` (ou `UpdateServer forAPI`) et vous fournissez des arguments vides pour les `OnPartialUpload` paramètres `OnUpload` et.

À partir de AWS CLI, exécutez la commande suivante :

```
aws transfer update-server --server-id your-server-id --workflow-details
'{"OnPartialUpload":[], "OnUpload":[]}'
```

Remplacez *your-server-id* par l'ID de votre serveur. Par exemple, si l'ID de votre serveur est `s-01234567890abcdef`, la commande est la suivante :

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
'{"OnPartialUpload":[], "OnUpload":[]}'
```

Restrictions et limites des flux de travail gérés

Restrictions

Les restrictions suivantes s'appliquent actuellement aux flux de travail de traitement après le téléchargement pour AWS Transfer Family.

- Les AWS Lambda fonctions entre comptes et entre régions ne sont pas prises en charge. Vous pouvez toutefois les copier sur plusieurs comptes, à condition que vos AWS Identity and Access Management (IAM) politiques soient correctement configurées.
- Pour toutes les étapes du flux de travail, tous les compartiments Amazon S3 auxquels le flux de travail accède doivent se trouver dans la même région que le flux de travail lui-même.
- Pour une étape de déchiffrement, la destination de déchiffrement doit correspondre à la source pour la région et le magasin de sauvegarde (par exemple, si le fichier à déchiffrer est stocké dans Amazon S3, la destination spécifiée doit également se trouver dans Amazon S3).
- Seules les étapes personnalisées asynchrones sont prises en charge.
- Les délais d'expiration des étapes personnalisés sont approximatifs. En d'autres termes, le délai d'expiration peut prendre un peu plus de temps que ce qui est spécifié. De plus, le flux de travail dépend de la fonction Lambda. Par conséquent, si la fonction est retardée pendant son exécution, le flux de travail n'en est pas conscient.
- Si vous dépassez votre limite de limitation, Transfer Family n'ajoute aucune opération de flux de travail à la file d'attente.
- Les flux de travail ne sont pas initiés pour les fichiers dont la taille est égale à 0. Les fichiers dont la taille est supérieure à 0 initient le flux de travail associé.

Limites

En outre, les limites fonctionnelles suivantes s'appliquent aux flux de travail de Transfer Family :

- Le nombre de flux de travail par région, par compte, est limité à 10.
- Le délai maximum pour les étapes personnalisées est de 30 minutes.
- Le nombre maximal d'étapes d'un flux de travail est de 8.
- Le nombre maximum de balises par flux de travail est de 50.
- Le nombre maximum d'exécutions simultanées contenant une étape de déchiffrement est de 250 par flux de travail.
- Vous pouvez stocker un maximum de 3 clés PGP privées, par serveur Transfer Family, par utilisateur.
- La taille maximale d'un fichier déchiffré est de 10 Go.
- Nous limitons le nouveau taux d'exécution à l'aide d'un système de [bucket à jetons](#) d'une capacité en rafale de 100 et d'un taux de recharge de 1.

- Chaque fois que vous supprimez un flux de travail d'un serveur et que vous le remplacez par un nouveau, ou que vous mettez à jour la configuration du serveur (ce qui a un impact sur le rôle d'exécution d'un flux de travail), vous devez attendre environ 10 minutes avant d'exécuter le nouveau flux de travail. Le serveur Transfer Family met en cache les détails du flux de travail et met 10 minutes au serveur pour actualiser son cache.

En outre, vous devez vous déconnecter de toutes les SFTP sessions actives, puis vous reconnecter après la période d'attente de 10 minutes pour voir les modifications.

Gestion des serveurs

Dans cette section, vous trouverez des informations sur la façon d'afficher la liste de vos serveurs, d'afficher les détails de votre serveur, de modifier les détails de votre serveur et de modifier la clé d'hôte de votre SFTP serveur activé.

Rubriques

- [Afficher la liste des serveurs](#)
- [Supprimer un serveur](#)
- [Afficher SFTP FTPS et détails FTP du serveur](#)
- [Afficher les détails AS2 du serveur](#)
- [Modifier les détails du serveur](#)
- [Gérez les clés d'hôte pour votre SFTP serveur compatible](#)
- [Surveillance de l'utilisation dans la console](#)

Afficher la liste des serveurs

Sur la AWS Transfer Family console, vous trouverez la liste de tous vos serveurs situés dans la AWS région que vous avez choisie.

Pour trouver la liste de vos serveurs existant dans une AWS région

- Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.

Si vous avez un ou plusieurs serveurs dans la AWS région actuelle, la console s'ouvre pour afficher la liste de vos serveurs. Si la liste des serveurs ne s'affiche pas, assurez-vous que vous vous trouvez dans la bonne région. Vous pouvez également choisir Servers (Serveurs) dans le panneau de navigation.

Pour plus d'informations sur l'affichage des détails de votre serveur, consultez [Afficher SFTP FTPS et détails FTP du serveur](#).

Supprimer un serveur

Cette procédure explique comment supprimer un serveur Transfer Family à l'aide de la AWS Transfer Family console ou AWS CLI.

Important

Vous êtes facturé, pour chacun des protocoles activés pour accéder à votre terminal, jusqu'à ce que vous supprimiez le serveur.

Warning

La suppression d'un serveur entraîne la suppression de tous ses utilisateurs. Les données du compartiment auxquelles on a accédé via le serveur ne sont pas supprimées et restent accessibles aux AWS utilisateurs qui ont des privilèges sur ces compartiments Amazon S3.

Console

Pour supprimer un serveur à l'aide de la console

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers.
3. Cochez la case du serveur que vous souhaitez supprimer.
4. Pour Actions, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation qui apparaît, entrez le mot **delete**, puis choisissez Supprimer pour confirmer que vous souhaitez supprimer le serveur.

Le serveur est supprimé de la page Serveurs et il ne vous est plus facturé.

AWS CLI

Pour supprimer un serveur à l'aide du CLI

1. (Facultatif) Exécutez la commande suivante pour afficher les détails du serveur que vous souhaitez supprimer définitivement.

```
aws transfer describe-server --server-id your-server-id
```

Cette `describe-server` commande renvoie tous les détails de votre serveur.

2. Exécutez la commande suivante pour supprimer le serveur.

```
aws transfer delete-server --server-id your-server-id
```

En cas de succès, la commande supprime le serveur et ne renvoie aucune information.

Afficher SFTP FTPS et détails FTP du serveur

Vous trouverez la liste des détails et des propriétés d'un AWS Transfer Family serveur individuel. Les propriétés du serveur incluent les protocoles, le fournisseur d'identité, le statut, le type de point de terminaison, le nom d'hôte personnalisé, le point de terminaison, les utilisateurs, le rôle de journalisation, la clé d'hôte du serveur et les balises.

Pour afficher les détails du serveur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, choisissez Servers (Serveurs).
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur, illustrée ci-dessous.

Vous pouvez modifier les propriétés du serveur sur cette page en choisissant Modifier. Pour plus d'informations sur la modification des détails du serveur, consultez [Modifier les détails du serveur](#). La page de détails des AS2 serveurs est légèrement différente. Pour AS2 les serveurs, voir [Afficher les détails AS2 du serveur](#).

Protocols Edit	Identity provider Edit
Protocols over which clients can connect to your server's endpoint • SFTP	Identity provider type Info Custom - AWS Lambda AWS Lambda function test-UserAuthenticationLambda 

Note

Les valeurs de description et de date d'importation de la clé hôte du serveur sont nouvelles depuis septembre 2022. Ces valeurs ont été introduites pour prendre en charge la fonctionnalité de clés hôtes multiples. Cette fonctionnalité nécessitait la migration de toutes les clés d'hôte uniques utilisées avant l'introduction de plusieurs clés d'hôte.

La valeur Date importée pour la clé d'hôte d'un serveur migré est définie sur la date de dernière modification du serveur. En d'autres termes, la date que vous voyez pour votre clé d'hôte migrée correspond à la date à laquelle vous avez modifié le serveur pour la dernière fois, avant la migration de la clé d'hôte du serveur.

La seule clé qui a été migrée est la plus ancienne ou la seule clé d'hôte de serveur.

Toutes les clés supplémentaires ont leur date réelle à partir de laquelle vous les avez importées. En outre, la clé migrée possède une description qui permet de l'identifier facilement comme ayant été migrée.

La migration a eu lieu entre le 2 et le 13 septembre. La date de migration réelle comprise dans cette page dépend de la région de votre serveur.

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

Afficher les détails AS2 du serveur

Vous trouverez la liste des détails et des propriétés d'un AWS Transfer Family serveur individuel. Les propriétés du serveur incluent les protocoles, le statut, etc. Pour les AS2 serveurs, vous pouvez également consulter les adresses IP de MDN sortie AS2 asynchrones.

Protocols

Edit

Protocols over which clients can connect to your server's endpoint

- AS2

Identity provider

Edit

 **AS2 Auth**
Basic authentication is not supported for AS2. Access can be controlled through VPC security groups.

Trois adresses IP statiques sont attribuées à chaque AS2 serveur. Utilisez ces adresses IP pour envoyer des messages asynchrones MDNs à vos partenaires commerciaux. AS2

AS2 asynchronous MDN egress IP details

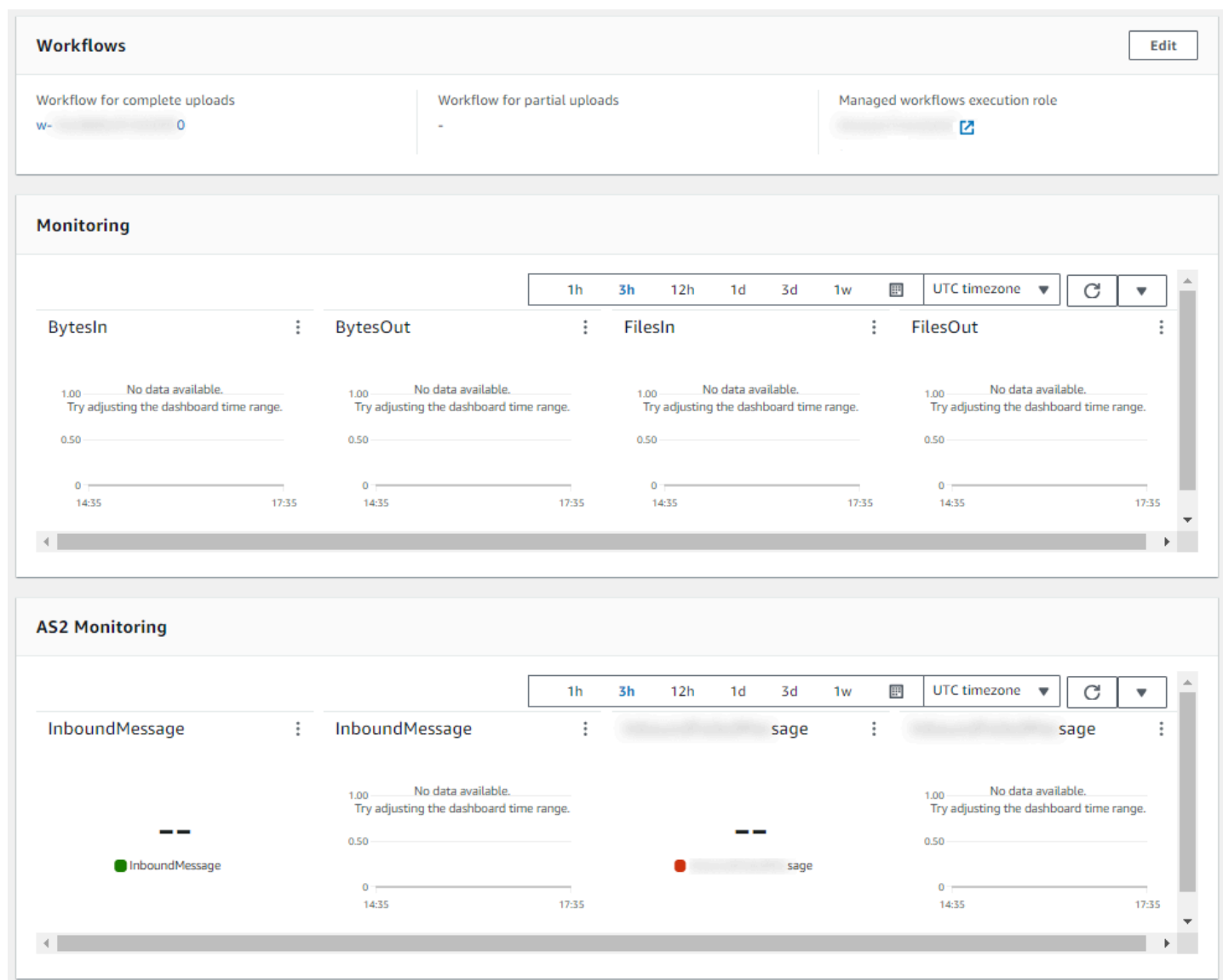
Below are the service managed static IP addresses used for sending your asynchronous MDNs to trading partners over AS2







La partie inférieure de la page de détails du AS2 serveur contient les détails de tout flux de travail associé ainsi que des informations de surveillance et de balisage.



Modifier les détails du serveur

Après avoir créé un AWS Transfer Family serveur, vous pouvez modifier sa configuration.

Rubriques

- [Modifier les protocoles de transfert de fichiers](#)
- [Modifier les paramètres du fournisseur d'identité personnalisé](#)
- [Modifier le point de terminaison du serveur](#)
- [Modifiez votre configuration de journalisation](#)
- [Modifier la politique de sécurité](#)

- [Modifier le flux de travail géré pour votre serveur](#)
- [Modifier les bannières d'affichage de votre serveur](#)
- [Mettez votre serveur en ligne ou hors ligne](#)

Pour modifier la configuration d'un serveur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers.
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur, illustrée ci-dessous.

Vous pouvez modifier les propriétés du serveur sur cette page en choisissant Modifier :

- Pour modifier les protocoles, voir [Modifier les protocoles de transfert de fichiers](#).
- Pour le fournisseur d'identité, notez que vous ne pouvez pas modifier le type de fournisseur d'identité d'un serveur après avoir créé le serveur. Pour changer de fournisseur d'identité, supprimez le serveur et créez-en un nouveau avec le fournisseur d'identité souhaité.

 Note

Si votre serveur utilise un fournisseur d'identité personnalisé, vous pouvez modifier certaines propriétés. Pour plus de détails, consultez [Modifier les paramètres du fournisseur d'identité personnalisé](#).

- Pour modifier le type de point de terminaison ou le nom d'hôte personnalisé, consultez [Modifier le point de terminaison du serveur](#).
- Pour ajouter un accord, vous devez d'abord l'ajouter AS2 en tant que protocole à votre serveur. Pour plus de détails, consultez [Modifier les protocoles de transfert de fichiers](#).
- Pour gérer les clés d'hôte de votre serveur, consultez [Gérez les clés d'hôte pour votre SFTP serveur compatible](#).
- Sous Détails supplémentaires, vous pouvez modifier les informations suivantes :
 - Pour modifier le rôle de journalisation, voir [Modifiez votre configuration de journalisation](#).
 - Pour modifier la politique de sécurité, consultez [Modifier la politique de sécurité](#).
 - Pour modifier la clé d'hôte du serveur, consultez [Gérez les clés d'hôte pour votre SFTP serveur compatible](#).

- Pour modifier le flux de travail géré de votre serveur, consultez [Modifier le flux de travail géré pour votre serveur](#).
- Pour modifier les bannières d'affichage de votre serveur, consultez [Modifier les bannières d'affichage de votre serveur](#).
- Sous Configuration supplémentaire, vous pouvez modifier les informations suivantes :
 - SetStat option : activez cette option pour ignorer l'erreur générée lorsqu'un client tente de l'utiliser SETSTAT sur un fichier que vous téléchargez dans un compartiment Amazon S3. Pour plus de détails, consultez la SetStatOption documentation dans cette [ProtocolDetails](#) rubrique.
 - TLS reprise de session : fournit un mécanisme permettant de reprendre ou de partager une clé secrète négociée entre le contrôle et la connexion de données pour une FTPS session. Pour plus de détails, consultez la TlsSessionResumptionMode documentation dans cette [ProtocolDetails](#) rubrique.
 - IP passive : indique le mode passif, pour FTP et les FTPS protocoles. Entrez une IPv4 adresse unique, telle que l'adresse IP publique d'un pare-feu, d'un routeur ou d'un équilibreur de charge. Pour plus de détails, consultez la PassiveIp documentation dans cette [ProtocolDetails](#) rubrique.
- Pour démarrer ou arrêter votre serveur, consultez [Mettez votre serveur en ligne ou hors ligne](#).
- Pour supprimer un serveur, voir [Supprimer un serveur](#).
- Pour modifier les propriétés d'un utilisateur, voir [Gestion des contrôles d'accès](#).

Protocols	Identity provider
Protocols over which clients can connect to your server's endpoint • SFTP	Identity provider type Info Custom - AWS Lambda AWS Lambda function test-UserAuthenticationLambda ↗

Note

Les valeurs de description et de date d'importation de la clé hôte du serveur sont nouvelles depuis septembre 2022. Ces valeurs ont été introduites pour prendre en charge la fonctionnalité de clés hôtes multiples. Cette fonctionnalité nécessitait la

migration de toutes les clés d'hôte uniques utilisées avant l'introduction de plusieurs clés d'hôte.

La valeur Date importée pour la clé d'hôte d'un serveur migré est définie sur la date de dernière modification du serveur. En d'autres termes, la date que vous voyez pour votre clé d'hôte migrée correspond à la date à laquelle vous avez modifié le serveur pour la dernière fois, avant la migration de la clé d'hôte du serveur.

La seule clé qui a été migrée est la plus ancienne ou la seule clé d'hôte de serveur. Toutes les clés supplémentaires ont leur date réelle à partir de laquelle vous les avez importées. En outre, la clé migrée possède une description qui permet de l'identifier facilement comme ayant été migrée.

La migration a eu lieu entre le 2 et le 13 septembre. La date de migration réelle comprise dans cette plage dépend de la région de votre serveur.

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

Modifier les protocoles de transfert de fichiers

Sur la AWS Transfer Family console, vous pouvez modifier le protocole de transfert de fichiers. Le protocole de transfert de fichiers connecte le client au point de terminaison de votre serveur.

Pour modifier les protocoles

1. Sur la page des détails du serveur, choisissez Modifier à côté de Protocoles.
2. Sur la page Modifier les protocoles, cochez ou décochez la ou les cases à cocher pour ajouter ou supprimer les protocoles de transfert de fichiers suivants :

- Protocole de transfert de fichiers Secure Shell (SSH/SFTP) : transfert de fichiers via SSH

Pour plus d'informations sur SFTP, voir [Création d'un SFTP serveur activé](#).

- File Transfer Protocol Secure (FTPS) — transfert de fichiers avec TLS chiffrement

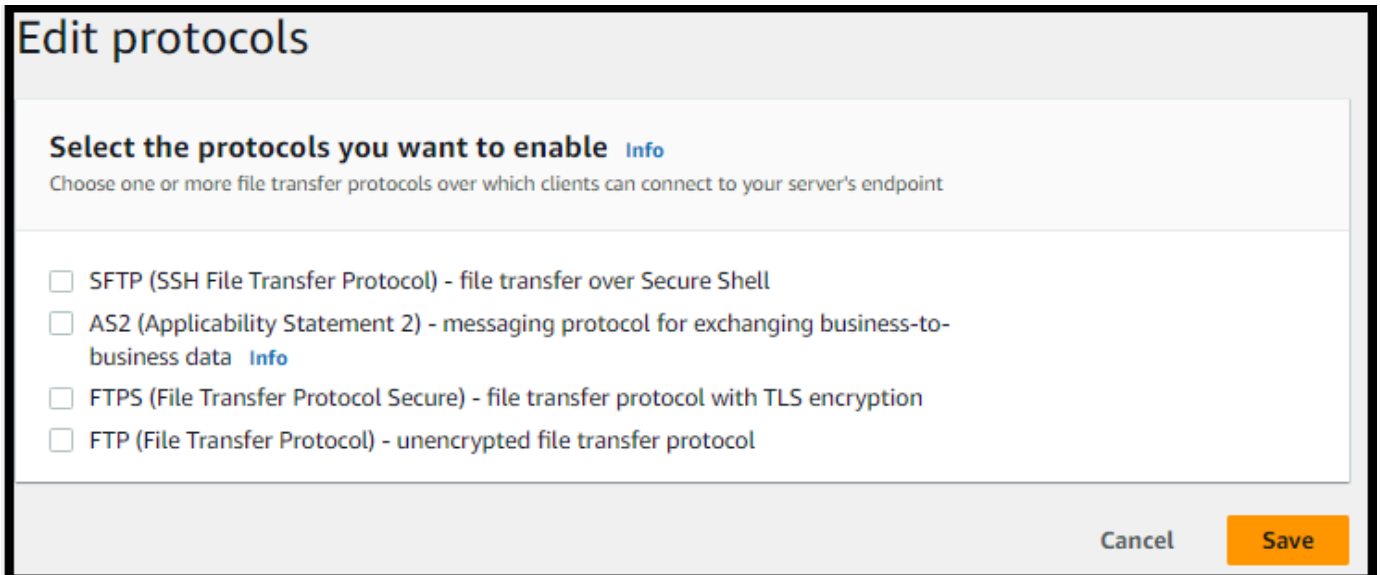
Pour plus d'informations sur FTPS, voir [Création d'un FTPS serveur activé](#).

- Protocole de transfert de fichiers (FTP) : transfert de fichiers non chiffré

Pour plus d'informations sur FTPS, voir [Création d'un FTP serveur activé](#).

Note

Si un serveur existant est activé uniquement pour SFTP, et que vous souhaitez ajouter FTPS et FTP, vous devez vous assurer que vous disposez des bons paramètres de fournisseur d'identité et de type de point de terminaison compatibles avec FTPS et FTP.



Edit protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☐ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

Cancel Save

Si vous le sélectionnez FTPS, vous devez choisir un certificat stocké dans AWS Certificate Manager (ACM) qui sera utilisé pour identifier votre serveur lorsque des clients s'y connecteront FTPS.

Pour demander un nouveau certificat public, consultez la section [Demander un certificat public](#) dans le guide de AWS Certificate Manager l'utilisateur.

Pour importer un certificat existant dans ACM, consultez la section [Importation de certificats ACM](#) dans le guide de AWS Certificate Manager l'utilisateur.

Pour demander un certificat privé à utiliser FTPS via des adresses IP privées, consultez la section [Demande d'un certificat privé](#) dans le guide de AWS Certificate Manager l'utilisateur.

Les certificats avec les algorithmes de chiffrement et les tailles de clés suivants sont pris en charge :

- 2048 bits RSA (_2048) RSA
- 4096 bits (_4096RSA) RSA
- Elliptic Prime Curve 256 octets (EC_prime256v1)
- Elliptic Prime Curve 384 octets (EC_secp384r1)
- Elliptic Prime Curve 521 octets (EC_secp521r1)

 Note

Le certificat doit être un SSL TLS certificat/X.509 version 3 valide avec une FQDN adresse IP spécifiée et des informations sur l'émetteur.

Choose protocols

Select the protocols you want to enable [Info](#)

Choose one or more file transfer protocols over which clients can connect to your server's endpoint

- ☐ SFTP (SSH File Transfer Protocol) - file transfer over Secure Shell
- ☐ AS2 (Applicability Statement 2) - messaging protocol for exchanging business-to-business data [Info](#)
- ☒ FTPS (File Transfer Protocol Secure) - file transfer protocol with TLS encryption
- ☐ FTP (File Transfer Protocol) - unencrypted file transfer protocol

AWS Certificate Manager (ACM) certificate [Info](#)

Server certificate
Choose a certificate stored in ACM which will be used to identify your server when clients connect to it over FTPS

[Cancel](#) [Next](#)

3. Choisissez Save (Enregistrer). Vous êtes renvoyé à la page des détails du serveur.

Modifier les paramètres du fournisseur d'identité personnalisé

Sur la AWS Transfer Family console, pour les fournisseurs d'identité personnalisés, vous pouvez modifier certains paramètres, selon que vous utilisez une fonction Lambda ou une API passerelle. Dans les deux cas, si votre serveur utilise le SFTP protocole, vous pouvez modifier votre méthode d'authentification.

- Si vous utilisez un Lambda comme fournisseur d'identité, vous pouvez modifier la fonction Lambda sous-jacente.

Transfer Family > Servers > s- > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ Service managed
Create and manage users within the service

☐ AWS Directory Service [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☐ Custom Identity Provider [Info](#)
Manage users by integrating an identity provider of your choice

☐ Use AWS Lambda to connect your identity provider [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☐ Use Amazon API Gateway to connect your identity provider [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

AWS Lambda function

▼



Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ Password OR public key

☐ Password ONLY

☐ Public Key ONLY

☐ Password AND public key

 Either a valid password or valid private key will be required during user authentication

Cancel Save

- Si vous utilisez une API passerelle comme fournisseur d'identité, vous pouvez mettre à jour la passerelle URL ou le rôle d'invocation, ou les deux.

Transfer Family > Servers > s-[redacted] > Edit identity provider

Edit identity provider

Identity Provider for SFTP, FTPS, or FTP

Identity provider type
An identity provider manages user access for authentication and authorization

☐ **Service managed**
Create and manage users within the service

☐ **AWS Directory Service** [Info](#)
Enable users in AWS Managed AD or use your own self-managed AD in your on-premises environment or in AWS

☒ **Custom Identity Provider** [Info](#)
Manage users by integrating an identity provider of your choice

☐ **Use AWS Lambda to connect your identity provider** [Info](#)
Invoke an AWS Lambda function to call your identity provider's API for user authentication and authorization

☒ **Use Amazon API Gateway to connect your identity provider** [Info](#)
Use a RESTful API method to call your identity provider's API for user authentication and authorization

Provide an Amazon API Gateway URL

Invocation role
IAM role for the service to invoke your Amazon API Gateway URL

Authentication methods
Choose which authentication methods are required for users to connect to your server

☒ **Password OR public key**
☐ Password ONLY
☐ Public Key ONLY
☐ Password AND public key

Either a valid password or valid private key will be required during user authentication

Cancel Save

Modifier le point de terminaison du serveur

Sur la AWS Transfer Family console, vous pouvez modifier le type de point de terminaison du serveur et le nom d'hôte personnalisé.

Pour modifier les détails du point de terminaison du serveur

1. Sur la page Détails du serveur, choisissez Modifier à côté des détails du point de terminaison.
2. Sur la page Modifier la configuration du point de terminaison, pour le type de point de terminaison, choisissez l'une des options suivantes :

- Public — Cette option rend votre serveur accessible via Internet.
- VPC— Cette option rend votre serveur accessible dans votre cloud privé virtuel (VPC). Pour plus d'informations sur VPC, voir [Création d'un serveur dans un cloud privé virtuel](#).

3. Pour Nom d'hôte personnalisé, choisissez l'une des options suivantes :

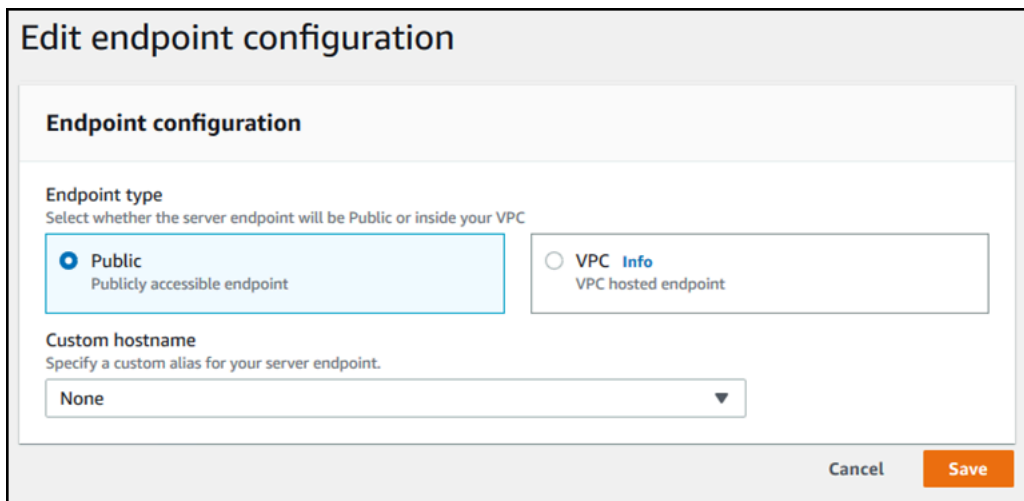
- Aucun : si vous ne souhaitez pas utiliser de domaine personnalisé, choisissez Aucun.

Vous obtenez un nom d'hôte de serveur fourni par AWS Transfer Family. Le nom d'hôte du serveur se présente sous la forme `serverId.server.transfer.regionId.amazonaws.com`.

- DNSAlias Amazon Route 53 — Pour utiliser un DNS alias créé automatiquement pour vous dans Route 53, choisissez cette option.
- Autre DNS : pour utiliser un nom d'hôte que vous possédez déjà dans un DNS service externe, choisissez Autre DNS.

Le choix de l'DNSAlias Amazon Route 53 ou autre DNS indique la méthode de résolution de noms à associer au point de terminaison de votre serveur.

Par exemple, votre domaine personnalisé peut être `sftp.inbox.example.com`. Un nom d'hôte personnalisé utilise un DNS nom que vous fournissez et qu'un DNS service peut résoudre. Vous pouvez utiliser Route 53 comme DNS résolveur ou utiliser votre propre fournisseur de DNS services. Pour savoir comment AWS Transfer Family utilise Route 53 pour acheminer le trafic de votre domaine personnalisé vers le point de terminaison du serveur, consultez [Utilisation de noms d'hôtes personnalisés](#).



4. Choisissez Save (Enregistrer). Vous êtes renvoyé à la page des détails du serveur.

Modifiez votre configuration de journalisation

Sur la AWS Transfer Family console, vous pouvez modifier votre configuration de journalisation.

Note

Si Transfer Family a créé un IAM rôle de CloudWatch journalisation pour vous lorsque vous avez créé un serveur, le IAM rôle est appelé `AWSTransferLoggingAccess`. Vous pouvez l'utiliser pour tous vos serveurs Transfer Family.

Pour modifier votre configuration de journalisation

1. Sur la page Détails du serveur, choisissez Modifier à côté de Détails supplémentaires.
2. Selon votre configuration, choisissez entre un rôle de journalisation, une JSON journalisation structurée ou les deux. Pour de plus amples informations, veuillez consulter [Mise à jour de la journalisation pour un serveur](#).

Modifier la politique de sécurité

Cette procédure explique comment modifier la politique de sécurité d'un serveur Transfer Family à l'aide de la AWS Transfer Family console ou AWS CLI.

Note

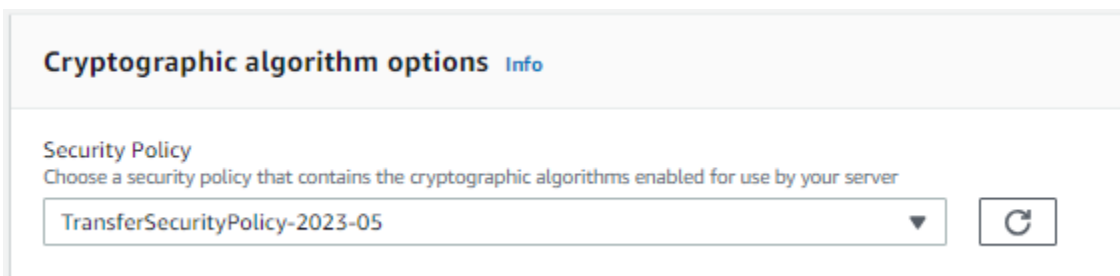
Si votre terminal est FIPS activé, vous ne pouvez pas remplacer la politique de FIPS sécurité par une politique non liée à la FIPS sécurité.

Console

Pour modifier la politique de sécurité à l'aide de la console

1. Sur la page Détails du serveur, choisissez Modifier à côté de Détails supplémentaires.
2. Dans la section Options d'algorithmes cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur.

Pour plus d'informations sur les stratégies de sécurité, consultez [Politiques de sécurité pour AWS Transfer Family](#).



Cryptographic algorithm options Info

Security Policy
Choose a security policy that contains the cryptographic algorithms enabled for use by your server

TransferSecurityPolicy-2023-05

3. Choisissez Save (Enregistrer).

Vous êtes renvoyé à la page des détails du serveur où vous pouvez voir la politique de sécurité mise à jour.

AWS CLI

Pour modifier la politique de sécurité à l'aide du CLI

1. Exécutez la commande suivante pour afficher la politique de sécurité actuelle attachée à votre serveur.

```
aws transfer describe-server --server-id your-server-id
```

Cette `describe-server` commande renvoie tous les détails de votre serveur, y compris la ligne suivante :

```
"SecurityPolicyName": "TransferSecurityPolicy-2018-11"
```

Dans ce cas, la politique de sécurité du serveur est `TransferSecurityPolicy-2018-11`.

2. Assurez-vous de fournir le nom exact de la politique de sécurité à la commande.
Par exemple, exécutez la commande suivante pour mettre à jour le serveur vers `TransferSecurityPolicy-2023-05`.

```
aws transfer update-server --server-id your-server-id --security-policy-name  
"TransferSecurityPolicy-2023-05"
```

 Note

Les noms des politiques de sécurité disponibles sont répertoriés dans [Politiques de sécurité pour AWS Transfer Family](#).

En cas de succès, la commande renvoie le code suivant et met à jour la politique de sécurité de votre serveur.

```
{  
  "ServerId": "your-server-id"  
}
```

Modifier le flux de travail géré pour votre serveur

Sur la AWS Transfer Family console, vous pouvez modifier le flux de travail géré associé au serveur.

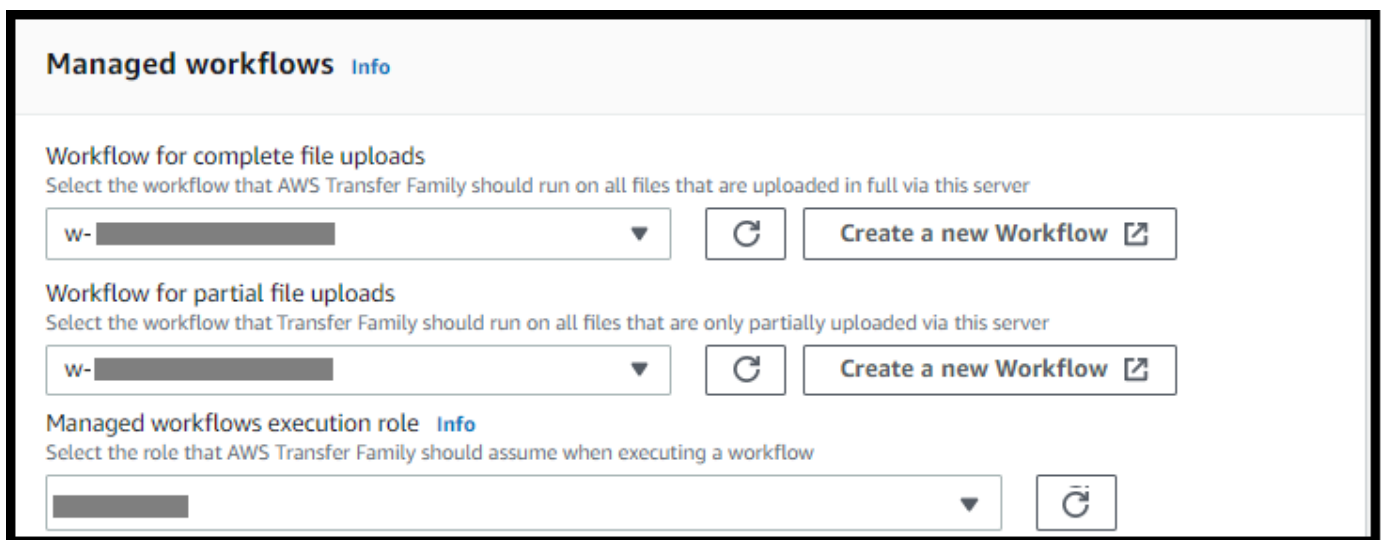
Pour modifier le flux de travail géré

1. Sur la page Détails du serveur, choisissez Modifier à côté de Détails supplémentaires.
2. Sur la page Modifier les informations supplémentaires, dans la section Flux de travail gérés, sélectionnez un flux de travail à exécuter sur tous les téléchargements.

Note

Si vous n'avez pas encore de flux de travail, choisissez Créer un nouveau flux de travail pour en créer un.

- a. Sélectionnez l'ID de flux de travail à utiliser.
- b. Choisissez un rôle d'exécution. C'est le rôle que Transfer Family assume lors de l'exécution des étapes du flux de travail. Pour de plus amples informations, veuillez consulter [IAMpolitiques relatives aux flux de travail](#). Choisissez Save (Enregistrer).



Managed workflows [Info](#)

Workflow for complete file uploads
Select the workflow that AWS Transfer Family should run on all files that are uploaded in full via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Workflow for partial file uploads
Select the workflow that Transfer Family should run on all files that are only partially uploaded via this server

w- [dropdown] [refresh] [Create a new Workflow](#)

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

[dropdown] [refresh]

3. Choisissez Save (Enregistrer). Vous êtes renvoyé à la page des détails du serveur.

Modifier les bannières d'affichage de votre serveur

Sur la AWS Transfer Family console, vous pouvez modifier les bannières d'affichage associées au serveur.

Pour modifier les bannières d'affichage

1. Sur la page Détails du serveur, choisissez Modifier à côté de Détails supplémentaires.
2. Sur la page Modifier les informations supplémentaires, dans la section Afficher les bannières, entrez le texte des bannières d'affichage disponibles.

3. Choisissez Save (Enregistrer). Vous êtes renvoyé à la page des détails du serveur.

Mettez votre serveur en ligne ou hors ligne

Sur la AWS Transfer Family console, vous pouvez mettre votre serveur en ligne ou le mettre hors ligne.

Pour mettre votre serveur en ligne

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, choisissez Servers (Serveurs).
3. Cochez la case du serveur hors ligne.
4. Pour Actions, choisissez Start (Démarrer).

Le passage d'un serveur hors ligne à un serveur en ligne peut prendre quelques minutes.

Note

Lorsque vous arrêtez un serveur pour le mettre hors ligne, vous devez toujours payer des frais de service pour ce serveur. Pour éliminer les frais supplémentaires liés au serveur, supprimez ce serveur.

Pour mettre votre serveur hors ligne

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation, choisissez Servers (Serveurs).
3. Cochez la case du serveur en ligne.
4. Pour Actions, choisissez Arrêter.

Lorsqu'un serveur démarre ou s'arrête, les serveurs ne sont pas disponibles pour les opérations sur les fichiers. La console n'affiche pas les états de démarrage et d'arrêt.

Si vous trouvez la condition d'erreur START_FAILED ou STOP_FAILED contactez-nous AWS Support pour vous aider à résoudre vos problèmes.

Gérez les clés d'hôte pour votre SFTP serveur compatible

Important

Si vous ne prévoyez pas de migrer des utilisateurs existants d'un serveur SFTP compatible existant vers un nouveau SFTP serveur activé, ignorez cette section.

La modification accidentelle de la clé d'hôte d'un serveur peut être perturbante. Selon la configuration de votre SFTP client, celui-ci peut échouer immédiatement, avec le message indiquant qu'aucune clé d'hôte fiable n'existe, ou présenter des messages menaçants. S'il existe des scripts pour automatiser les connexions, ils échoueront probablement également.

AWS Transfer Family Fournit par défaut une clé d'hôte pour votre SFTP serveur activé. Vous pouvez remplacer la clé d'hôte par défaut par une clé d'hôte d'un autre serveur. Ne le faites que si vous prévoyez de déplacer des utilisateurs existants d'un SFTP serveur compatible existant vers votre nouveau SFTP serveur activé.

Pour éviter que vos utilisateurs ne soient invités à vérifier à nouveau l'authenticité de votre SFTP serveur activé, importez la clé d'hôte de votre serveur local sur le SFTP serveur activé. Cela empêche également vos utilisateurs de recevoir un avertissement concernant une man-in-the-middle attaque potentielle.

Vous pouvez également effectuer une rotation périodique des clés d'hôte, par mesure de sécurité supplémentaire.

Note

Bien que la console Transfer Family vous permette de spécifier et d'ajouter des clés d'hôte pour tous les serveurs, ces clés ne sont utiles que pour les serveurs qui utilisent le SFTP protocole.

Rubriques

- [Ajouter une clé d'hôte de serveur supplémentaire](#)
- [Supprimer la clé d'hôte d'un serveur](#)
- [Faites pivoter les clés de l'hôte du serveur](#)

- [Informations supplémentaires sur la clé de l'hôte du serveur](#)

Ajouter une clé d'hôte de serveur supplémentaire

Sur la AWS Transfer Family console, vous pouvez ajouter des clés d'hôte de serveur supplémentaires. L'ajout de clés d'hôte supplémentaires de différents formats peut être utile pour identifier un serveur lorsque des clients s'y connectent, ainsi que pour améliorer votre profil de sécurité. Par exemple, si votre clé d'origine est une RSA clé, vous pouvez ajouter une ECDSA clé supplémentaire.

Note

Le SFTP client se connecte à l'aide de la première clé publique dont il dispose et qui peut correspondre à l'une des clés du serveur actif.

Pour ajouter une clé d'hôte de serveur supplémentaire

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers, puis choisissez un serveur qui utilise le SFTP protocole.
3. Sur la page de détails du serveur, faites défiler la page vers le bas jusqu'à la section Clés d'hôte du serveur.

Server host keys (1)						Actions	Add host key
☐	Host key ID	Fingerprint	Description	Key type	Date imported		
☐	hostkey-	SHA256: [fingerprint]	ECDSA server host key	ecdsa-sha2-nistp256	2022-08-26		

4. Choisissez Ajouter une clé d'hôte.

La page clé Ajouter un hôte de serveur s'affiche.

5. Dans la section Clé d'hôte du serveur RSAECDSA, entrez une clé ED25519 privée ou une clé privée utilisée pour identifier votre serveur lorsque les clients s'y connectent via le SFTP serveur activé.

Note

Lorsque vous créez une clé d'hôte de serveur, assurez-vous de la spécifier -N "" (pas de phrase secrète). Consultez [Création de SSH clés sous macOS, Linux ou Unix](#) pour plus de détails sur la façon de générer des paires de clés.

Server Host Key [Info](#)**Private key - optional**

Upload an RSA, ECDSA, or ED25519 private key that will be used to identify your SFTP server when clients connect to it. Additional keys can be added once the server is created.

Enter an optional RSA, ECDSA, or ED25519 key

Description - optional

Add a description to differentiate between multiple private keys

Enter optional description

i You can ignore this section unless you are migrating users from an existing SFTP server.

6. (Facultatif) Ajoutez une description pour différencier les clés d'hôte de plusieurs serveurs. Vous pouvez également ajouter des tags à votre clé.
7. Sélectionnez Ajouter une clé. Vous êtes renvoyé à la page des détails du serveur.

Pour ajouter une clé d'hôte à l'aide de AWS Command Line Interface (AWS CLI), utilisez l'[the section called "ImportHostKey"](#) API opération et fournissez la nouvelle clé d'hôte. Si vous créez un nouveau SFTP serveur activé, vous fournissez votre clé d'hôte en tant que paramètre de l'[the section called "CreateServer"](#) API opération. Vous pouvez également utiliser le AWS CLI pour mettre à jour la description d'une clé d'hôte existante.

L'exemple de `import-host-key` AWS CLI commande suivant importe une clé d'hôte pour le SFTP serveur activé spécifié.

```
aws transfer import-host-key --description key-description --server-id your-server-id
--host-key-body file://my-host-key
```

Supprimer la clé d'hôte d'un serveur

Sur la AWS Transfer Family console, vous pouvez supprimer une clé d'hôte de serveur.

Pour supprimer la clé d'hôte d'un serveur

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Dans le volet de navigation de gauche, choisissez Servers, puis choisissez un serveur qui utilise le SFTP protocole.
3. Sur la page de détails du serveur, faites défiler la page vers le bas jusqu'à la section Clés d'hôte du serveur.

Server host keys (1)

Actions

Add host key

1

☐	Host key ID	Fingerprint	Description	Key type	Date imported
☐	hostkey-	SHA256:	ECDSA server host key	ecdsa-sha2-nistp256	2022-08-26

4. Dans la section Clés d'hôte du serveur, sélectionnez une clé, puis sous Actions, choisissez Supprimer.
5. Dans la boîte de dialogue de confirmation qui apparaît, entrez le mot **delete**, puis choisissez Supprimer pour confirmer que vous souhaitez supprimer la clé d'hôte.

La clé d'hôte est supprimée de la page Serveurs.

Pour supprimer la clé d'hôte à l'aide de AWS CLI, utilisez l'[the section called "DeleteHostKey"](#) APopération et fournissez l'ID du serveur et l'ID de la clé d'hôte.

L'exemple de `delete-host-key` AWS CLI commande suivant supprime une clé d'hôte pour le SFTP serveur activé spécifié.

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

Faites pivoter les clés de l'hôte du serveur

Vous pouvez régulièrement alterner la clé d'hôte de votre serveur.

Note

Transfer Family utilise la première clé ajoutée pour chaque algorithme comme clé d'hôte active. Vous pouvez associer jusqu'à 10 clés d'hôte par SFTP serveur, mais une seule clé par algorithme est active à un moment donné.

Supposons, par exemple, que vous ayez ajouté le jeu de clés d'hôte suivant à votre serveur.

Clés d'hôte du serveur

Type de clé d'hôte	Date d'ajout au serveur	Actif ?
RSA	1er avril 2020	Non
ECDSA	1er février 2020	Non
ED25519	1 décembre 2019	Non
RSA	1er octobre 2019	Oui
ECDSA	1er juin 2019	Oui
ED25519	1 mars 2019	Oui

La clé la plus ancienne de chaque algorithme est active. Si vous supprimez la RSA clé que vous avez ajoutée le 1er octobre 2019, la RSA clé que vous avez ajoutée le 1er avril 2020 devient active.

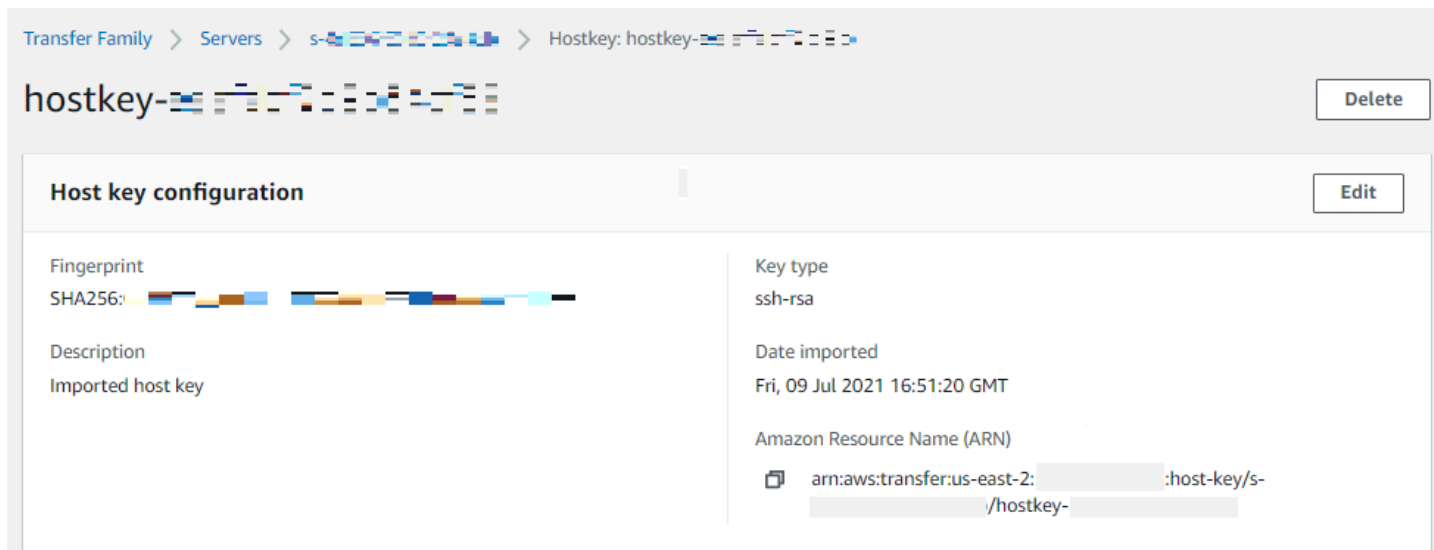
Pour faire pivoter la clé d'hôte du serveur

1. Ajoutez une nouvelle clé d'hôte de serveur. Cette procédure est décrite dans [Ajouter une clé d'hôte de serveur supplémentaire](#).
2. Supprimez une ou plusieurs clés d'hôte du même type que celles que vous avez ajoutées précédemment. Cette procédure est décrite dans [Supprimer la clé d'hôte d'un serveur](#).

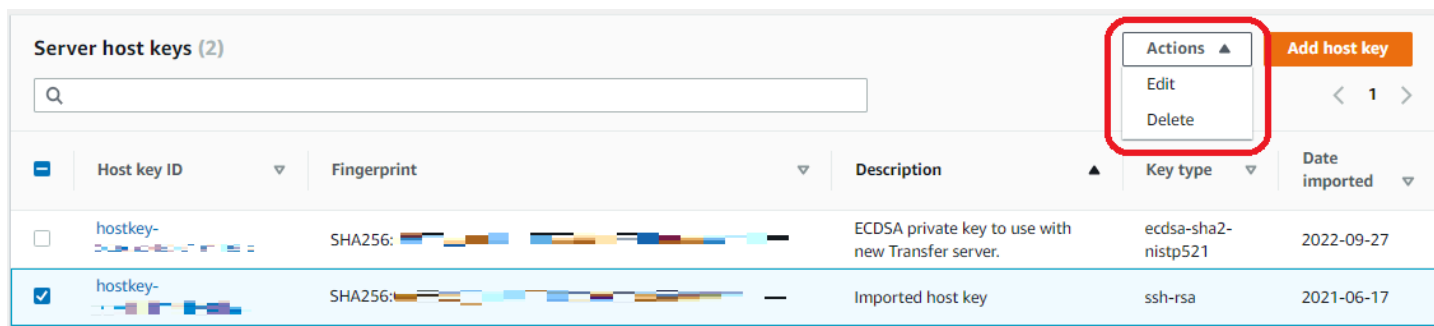
- Assurez-vous que la plus ancienne clé restante du même type est celle que vous souhaitez activer.

Informations supplémentaires sur la clé de l'hôte du serveur

Vous pouvez sélectionner une clé d'hôte pour afficher les détails de cette clé.



Vous pouvez supprimer une clé d'hôte ou modifier sa description dans le menu Actions de l'écran des détails du serveur. Sélectionnez la clé d'hôte, puis choisissez l'action appropriée dans le menu.



Surveillance de l'utilisation dans la console

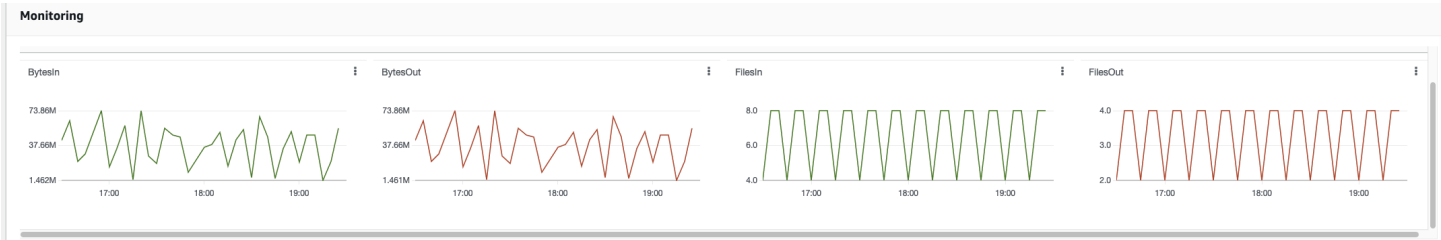
Vous pouvez obtenir des informations sur les métriques de votre serveur sur la page de détails du serveur. Vous disposez ainsi d'un emplacement unique pour surveiller vos charges de travail liées aux transferts de fichiers. Vous pouvez suivre le nombre de fichiers que vous avez échangés avec vos partenaires et suivre de près leur utilisation à l'aide d'un tableau de bord centralisé. Pour plus de détails, consultez [Afficher SFTP FTPS et détails FTP du serveur](#). Le tableau suivant décrit les indicateurs disponibles pour Transfer Family.

Espace de noms	Métrique	Description
AWS/Transfer	BytesIn	Nombre total d'octets transférés vers le serveur. Unités : nombre Période : 5 minutes
	BytesOut	Nombre total d'octets transférés hors du serveur. Unité : nombre Période : 5 minutes
	FilesIn	Le nombre total de fichiers transférés sur le serveur. Pour les serveurs utilisant le AS2 protocole, cette métrique représente le nombre de messages reçus. Unités : nombre Période : 5 minutes
	FilesOut	Le nombre total de fichiers transférés hors du serveur. Unités : nombre Période : 5 minutes
	InboundMessage	Nombre total de AS2 messages reçus avec succès d'un partenaire commercial. Unités : nombre Période : 5 minutes
	InboundFailedMessage	Nombre total de AS2 messages reçus sans succès de la part d'un partenaire commercial. En d'autres termes, un partenaire commercial a envoyé un message, mais le serveur Transfer Family n'a pas réussi à le traiter. Unités : nombre

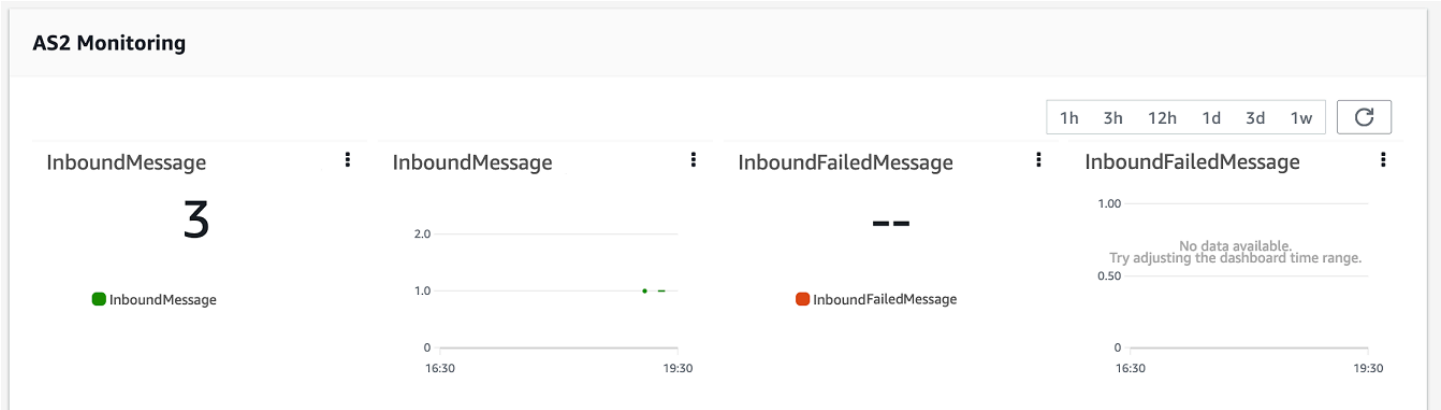
Espace de noms	Métrique	Description
		Période : 5 minutes
	OnPartialUploadExecutionsStarted	Nombre total d'exécutions de on-partial-upload flux de travail démarrées sur le serveur. Unités : nombre Durée : 1 minute
	OnPartialUploadExecutionsSuccess	Nombre total d'exécutions de on-partial-upload flux de travail réussies sur le serveur. Unités : nombre Durée : 1 minute
	OnPartialUploadExecutionsFailed	Nombre total d'exécutions de on-partial-upload flux de travail infructueuses sur le serveur. Unités : nombre Durée : 1 minute
	OnUploadExecutionsStarted	Nombre total d'exécutions de flux de travail démarrées sur le serveur. Unités : nombre Durée : 1 minute
	OnUploadExecutionsSuccess	Nombre total d'exécutions de flux de travail réussies sur le serveur. Unités : nombre Durée : 1 minute

Espace de noms	Métrique	Description
	OnUploadExecutionsFailed	Nombre total d'exécutions de flux de travail infructueuses sur le serveur. Unités : nombre Durée : 1 minute

La section Surveillance contient quatre graphiques individuels. Ces graphiques indiquent les octets entrants, les octets sortants, les fichiers entrants et les fichiers sortants.



Pour les serveurs sur lesquels le AS2 protocole est activé, une section AS2Surveillance se trouve sous les informations de surveillance. Cette section contient des informations détaillées sur le nombre de messages entrants, qu'ils aient été réussis ou non.



Pour ouvrir le graphique sélectionné dans sa propre fenêtre, cliquez sur l'icône de développement (). Vous pouvez également cliquer sur l'icône représentant des points de suspension verticaux () d'un graphique pour ouvrir un menu déroulant contenant les éléments suivants :

- Agrandir — Ouvre le graphique sélectionné dans sa propre fenêtre.

- **Actualiser** : recharge le graphique avec les données les plus récentes.
- **Afficher dans les métriques** — Ouvre les informations relatives aux métriques correspondantes dans Amazon CloudWatch.
- **Afficher les journaux** — Ouvre le groupe de journaux correspondant dans CloudWatch.

Gestion des contrôles d'accès

Vous pouvez contrôler l'accès d'un utilisateur aux AWS Transfer Family ressources à l'aide d'une politique AWS Identity and Access Management (IAM). Une IAM politique est une déclaration, généralement sous JSON forme, qui autorise un certain niveau d'accès à une ressource. Vous utilisez une IAM politique pour définir les opérations sur les fichiers que vous souhaitez autoriser ou non vos utilisateurs à effectuer. Vous pouvez également utiliser une IAM politique pour définir le ou les compartiments Amazon S3 auxquels vous souhaitez donner accès à vos utilisateurs. Pour définir ces politiques pour les utilisateurs, vous créez un IAM rôle AWS Transfer Family auquel la IAM politique et la relation de confiance sont associées.

Un IAM rôle est attribué à chaque utilisateur. Le type de IAM rôle AWS Transfer Family utilisé est appelé rôle de service. Lorsqu'un utilisateur se connecte à votre serveur, il AWS Transfer Family assume le IAM rôle qui lui est attribué. Pour en savoir plus sur la création d'un IAM rôle permettant à un utilisateur d'accéder à un compartiment Amazon S3, consultez la section [Création d'un rôle pour déléguer des autorisations à un AWS service](#) dans le Guide de IAM l'utilisateur.

Vous pouvez accorder un accès en écriture uniquement aux objets Amazon S3 en utilisant certaines autorisations dans le cadre d'une IAM politique. Pour plus de détails, consultez [Autoriser uniquement l'écriture et la liste des fichiers](#).

Le blog sur le AWS stockage contient un article expliquant comment configurer l'accès avec le moindre privilège. Pour plus de détails, voir [Implémentation de l'accès avec le moindre privilège dans un AWS Transfer Family flux de travail](#).

Note

Si votre compartiment Amazon S3 est chiffré à l'aide de AWS Key Management Service (AWS KMS), vous devez spécifier des autorisations supplémentaires dans votre politique. Pour plus de détails, consultez [Chiffrement des données dans Amazon S3](#). En outre, vous pouvez obtenir plus d'informations sur [les politiques de session](#) dans le guide de IAM l'utilisateur.

Rubriques

- [Autoriser l'accès en lecture et en écriture à un compartiment Amazon S3](#)
- [Création d'une politique de session pour un compartiment Amazon S3](#)

- [Empêcher les utilisateurs de s'exécuter mkdir dans un compartiment S3](#)

Autoriser l'accès en lecture et en écriture à un compartiment Amazon S3

Cette section explique comment créer une IAM politique qui autorise l'accès en lecture et en écriture à un compartiment Amazon S3 spécifique. L'attribution d'un IAM rôle doté de cette IAM politique à votre utilisateur donne à celui-ci un accès en lecture/écriture au compartiment Amazon S3 spécifié.

La politique suivante fournit un accès programmatique en lecture, écriture et balisage à un compartiment Amazon S3. Les PutObjectACL relevés GetObjectACL et ne sont nécessaires que si vous devez activer l'accès multicompte. En d'autres termes, votre serveur Transfer Family doit accéder à un bucket d'un autre compte.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadWriteS3",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"]
    }
  ]
}
```

```
}
```

L'action `ListBucket` nécessite une autorisation sur le compartiment lui-même. Les actions `PUT`, `GET` et `DELETE` nécessitent des autorisations pour un objet. Comme il s'agit de ressources différentes, elles sont spécifiées à l'aide de différents noms de ressources Amazon (ARNs).

Pour restreindre davantage l'accès de vos utilisateurs au seul home préfixe du compartiment Amazon S3 spécifié, consultez [Création d'une politique de session pour un compartiment Amazon S3](#).

Création d'une politique de session pour un compartiment Amazon S3

Une politique de session est une politique AWS Identity and Access Management (IAM) qui limite les utilisateurs à certaines parties d'un compartiment Amazon S3. Pour cela, elle évalue l'accès en temps réel.

Note

Les politiques de session ne sont utilisées qu'avec Amazon S3. Pour AmazonEFS, vous utilisez les autorisations relatives aux POSIX fichiers pour limiter l'accès.

Vous pouvez utiliser une politique de session lorsque vous devez accorder le même accès à un groupe d'utilisateurs à une partie spécifique de votre compartiment Amazon S3. Par exemple, un groupe d'utilisateurs peut avoir besoin d'accéder uniquement au répertoire home. Ce groupe d'utilisateurs partage le même IAM rôle.

Note

La longueur maximale d'une politique de session est de 2 048 caractères. Pour plus de détails, consultez le [paramètre de demande de politique](#) pour l'`CreateUseraction` dans la API référence.

Pour créer une politique de session, utilisez les variables de stratégie suivantes dans votre IAM stratégie :

- `${transfer:HomeBucket}`

- `${transfer:HomeDirectory}`
- `${transfer:HomeFolder}`
- `${transfer:UserName}`

Important

Vous ne pouvez pas utiliser les variables précédentes dans les politiques gérées. Vous ne pouvez pas non plus les utiliser comme variables de politique dans une définition de IAM rôle. Vous créez ces variables dans une IAM politique et vous les fournissez directement lors de la configuration de votre utilisateur. De plus, vous ne pouvez pas utiliser la `${aws:Username}` variable dans cette politique de session. Cette variable fait référence à un nom IAM d'utilisateur et non au nom d'utilisateur requis par AWS Transfer Family.

Le code suivant montre un exemple de politique de session.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::${transfer:HomeBucket}"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "${transfer:HomeFolder}/*",
            "${transfer:HomeFolder}"
          ]
        }
      }
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
```

```
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:DeleteObjectVersion",
      "s3:DeleteObject",
      "s3:GetObjectVersion",
      "s3:GetObjectACL",
      "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
  }
}
```

Note

L'exemple de politique précédent suppose que le répertoire personnel des utilisateurs est configuré pour inclure une barre oblique finale, pour indiquer qu'il s'agit d'un répertoire. Si, par contre, vous définissez le nom d'un utilisateur `HomeDirectory` sans la barre oblique finale, vous devez l'inclure dans votre politique.

Dans l'exemple de stratégie précédent, notez l'utilisation des paramètres de `transfer:HomeDirectory` stratégie `transfer:HomeFolder` `transfer:HomeBucket`, et. Ces paramètres sont définis pour `HomeDirectory` ce qui est configuré pour l'utilisateur, comme décrit dans [HomeDirectory](#) et [Implémentation de votre méthode API Gateway](#). Ces paramètres ont les définitions suivantes :

- Le `transfer:HomeBucket` paramètre est remplacé par le premier composant de `HomeDirectory`.
- Le `transfer:HomeFolder` paramètre est remplacé par les parties restantes du `HomeDirectory` paramètre.
- La barre oblique (/) initiale du `transfer:HomeDirectory` paramètre a été supprimée afin de pouvoir être utilisé dans le cadre d'un nom de ressource Amazon S3 (ARN) dans une `Resource` instruction.

 Note

Si vous utilisez des répertoires logiques, c'est-à-dire ceux de l'utilisateur, LOGICAL ces paramètres de homeDirectoryType stratégie (HomeBucketHomeDirectory, etHomeFolder) ne sont pas pris en charge.

Supposons, par exemple, que le HomeDirectory paramètre configuré pour l'utilisateur de Transfer Family soit /home/bob/amazon/stuff/.

- `transfer:HomeBucket` est réglé sur /home.
- `transfer:HomeFolder` est réglé sur /bob/amazon/stuff/.
- `transfer:HomeDirectory` devient /home/bob/amazon/stuff/.

Le premier "Sid" permet à l'utilisateur de répertorier tous les répertoires à partir de /home/bob/amazon/stuff/.

La seconde "Sid" limite l'utilisateur put et l'get accès à ce même chemin, /home/bob/amazon/stuff/.

Avec la politique précédente en place, lorsqu'un utilisateur se connecte, il ne peut accéder qu'aux objets de son répertoire personnel. Au moment de la connexion, AWS Transfer Family remplace ces variables par les valeurs appropriées pour l'utilisateur. Cela permet d'appliquer plus facilement les mêmes documents de stratégie à plusieurs utilisateurs. Cette approche réduit les coûts liés à la gestion des IAM rôles et des politiques pour gérer l'accès de vos utilisateurs à votre compartiment Amazon S3.

Vous pouvez également utiliser une politique de session pour personnaliser l'accès de chacun de vos utilisateurs en fonction des besoins de votre entreprise. Pour plus d'informations, consultez [les sections Autorisations pour AssumeRole AssumeRoleWithSAML, et AssumeRoleWithWebIdentity](#) dans le Guide de IAM l'utilisateur.

 Note

AWS Transfer Family stocke la politiqueJSON, au lieu du nom de ressource Amazon (ARN) de la politique. Ainsi, lorsque vous modifiez la politique dans la IAM console, vous devez revenir à la AWS Transfer Family console et informer vos utilisateurs du contenu de la

politique le plus récent. Vous pouvez mettre à jour l'utilisateur dans l'onglet Informations sur la politique de la section Configuration utilisateur.

Si vous utilisez le AWS CLI, vous pouvez utiliser la commande suivante pour mettre à jour la politique.

```
aws transfer update-user --server-id server --user-name user --policy \  
    "$(aws iam get-policy-version --policy-arn policy --version-id version --  
    output json)"
```

Empêcher les utilisateurs de s'exécuter `mkdir` dans un compartiment S3

Vous pouvez limiter la capacité des utilisateurs à créer un répertoire dans un compartiment Amazon S3. Pour ce faire, vous devez créer une IAM politique qui autorise `s3:PutObject`, mais qui la refuse également lorsque la touche se termine par un `«/»` (barre oblique). L'exemple de politique suivant permet aux utilisateurs de télécharger des fichiers dans un compartiment Amazon S3 mais refuse la `mkdir` commande dans le compartiment Amazon S3.

```
{  
  "Sid": "DenyMkdir",  
  "Action": [  
    "s3:PutObject"  
  ],  
  "Effect": "Deny",  
  "Resource": [  
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/",  
    "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*/*"  
  ]  
}
```

Note

La deuxième ligne de ressources empêche les utilisateurs de créer des sous-dossiers en exécutant une commande telle que `put my-file DOC-EXAMPLE-BUCKET/new-folder/my-file`.

Logging pour AWS Transfer Family

AWS Transfer Family s'intègre à la fois à Amazon AWS CloudTrail et aux deux CloudWatch.

CloudTrail et CloudWatch répondent à des objectifs différents mais complémentaires :

- CloudTrail est un AWS service qui crée un enregistrement des actions entreprises au sein de votre Compte AWS. Il surveille et enregistre en permanence les API appels pour des activités telles que les connexions à la console, AWS Command Line Interface les commandes SDK et/ou API les appels. Cela vous permet de garder un journal indiquant qui a pris quelle action, quand et d'où. CloudTrail contribue à l'audit, à la gestion des accès et à la conformité réglementaire en fournissant un historique de toutes les activités de votre AWS environnement. Pour plus de détails, consultez le [guide de AWS CloudTrail l'utilisateur](#).
- CloudWatch est un service de surveillance des AWS ressources et des applications. Il collecte des métriques et des journaux pour fournir une visibilité sur l'utilisation des ressources, les performances des applications et l'état général du système. CloudWatch facilite les tâches opérationnelles telles que le dépannage des problèmes, le réglage des alarmes et le dimensionnement automatique. Pour plus de détails, consultez le [guide de CloudWatch l'utilisateur Amazon](#).

Rubriques

- [AWS CloudTrailconnexion pour AWS Transfer Family](#)
- [Amazon CloudWatch Logging pour AWS Transfer Family](#)

AWS CloudTrailconnexion pour AWS Transfer Family

AWS Transfer Familyest intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dansAWS Transfer Family.

CloudTrail capture tous les appels d'API AWS Transfer Family sous forme d'événements. Les appels capturés incluent des appels de la console AWS Transfer Family et les appels de code vers les opérations d'API AWS Transfer Family.

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.

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'AWS Transfer Family, 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 de suivi dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour en savoir plus, 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 AWS Transfer Family actions sont enregistrées CloudTrail et documentées dans le [ActionsAPI reference](#). Par exemple, les appels au `CreateServer`, `ListUsers` et les `StopServer` actions 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 effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter l'[élément userIdentity CloudTrail](#) .

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 Transfer Family. 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 Transfer Family, 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](#).

Rubriques

- [Activer la AWS CloudTrail journalisation](#)
- [Exemple d'entrée de journal pour la création d'un serveur](#)

Activer la AWS CloudTrail journalisation

Vous pouvez surveiller les appels d'API AWS Transfer Family à l'aide d'AWS CloudTrail. En surveillant les appels d'API, vous pouvez obtenir des informations utiles sur la sécurité et les opérations. Si la [journalisation au niveau des objets Amazon S3 est activée](#), elle RoleSessionName est contenue dans le champ Demandeur sous [AWS:Role Unique Identifier]/username.sessionid@server-id la forme. Pour plus d'informations sur les identifiants uniques de rôle AWS Identity and Access Management (IAM), consultez la section Identifiants [uniques dans le guide](#) de l'AWS Identity and Access Management utilisateur.

Important

La longueur maximale du RoleSessionName est de 64 caractères. S'il RoleSessionName est plus long, il est server-id tronqué.

Exemple d'entrée de journal pour la création d'un serveur

L'exemple suivant montre une entrée de CloudTrail journal (au format JSON) qui illustre l>CreateServeraction.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAA4FFF5HHHHH6NNWWW:user1",
```

```

    "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
    "accountId": "123456789102",
    "accessKeyId": "AAAA52C2WWWWW3BB4Z",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-12-18T20:03:57Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAAA4FFF5HHHHH6NNWWW",
        "arn": "arn:aws:iam::123456789102:role/Admin",
        "accountId": "123456789102",
        "userName": "Admin"
      }
    },
    "eventTime": "2024-02-05T19:18:53Z",
    "eventSource": "transfer.amazonaws.com",
    "eventName": "CreateServer",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "11.22.1.2",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 Safari/537.36",
    "requestParameters": {
      "domain": "S3",
      "hostKey": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "protocols": [
        "SFTP"
      ],
      "protocolDetails": {
        "passiveIp": "AUTO",
        "tlsSessionResumptionMode": "ENFORCED",
        "setStatOption": "DEFAULT"
      },
      "securityPolicyName": "TransferSecurityPolicy-2020-06",
      "s3StorageOptions": {
        "directoryListingOptimization": "ENABLED"
      }
    },
    "responseElements": {
      "serverId": "s-1234abcd5678efghi"
    },
    "requestID": "6fe7e9b1-72fc-45b0-a7f9-5840268aeadf",

```

```
"eventID": "4781364f-7c1e-464e-9598-52d06aa9e63a",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789102",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "transfer.us-east-1.amazonaws.com"
},
"sessionCredentialFromConsole": "true"
}
```

Amazon CloudWatch Logging pour AWS Transfer Family

Amazon CloudWatch surveille vos AWS Transfer Family ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez les utiliser CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer pour vos ressources et vos applications.

La page d' CloudWatch accueil affiche automatiquement les statistiques relatives à Transfer Family et à tous les autres AWS services que vous utilisez. Vous pouvez également créer des tableaux de bord personnalisés pour afficher les métriques relatives à vos applications personnalisées, ainsi que des collections personnalisées de métriques de votre choix.

Vous pouvez créer des alertes pour surveiller les métriques et envoyer des notifications ou apporter automatiquement des modifications aux ressources surveillées, lorsqu'un seuil est dépassé. Par exemple, vous pouvez surveiller les fichiers transférés vers un serveur Transfer Family et utiliser ces données pour déterminer si vous devez déployer des serveurs supplémentaires pour gérer une charge accrue. Vous pouvez également utiliser ces données pour arrêter ou supprimer des instances sous-utilisées afin de réaliser des économies.

Rubriques

- [Création, mise à jour et affichage de la journalisation pour les serveurs](#)
- [Gestion de la journalisation des flux de travail](#)
- [Configurer le rôle de CloudWatch journalisation](#)
- [Afficher les flux de log de Transfer Family](#)
- [Création d' CloudWatch alarmes Amazon](#)

- [Enregistrement des API appels Amazon S3 dans les journaux d'accès S3](#)
- [Exemples pour limiter le problème de confusion des adjoints](#)
- [CloudWatch structure du journal pour Transfer Family](#)
- [Exemples d'entrées de CloudWatch journal](#)
- [Utilisation CloudWatch des métriques pour Transfer Family](#)
- [Utilisation Notifications des utilisateurs AWS avec AWS Transfer Family](#)

Création, mise à jour et affichage de la journalisation pour les serveurs

Pour tous les AWS Transfer Family serveurs, vous pouvez choisir entre deux options de journalisation : `LoggingRole` (utilisée pour la journalisation des flux de travail attachés au serveur) ou `StructuredLogDestinations`. L'utilisation de `StructuredLogDestinations` comporte les avantages suivants :

- Recevez les journaux dans un JSON format structuré.
- Interrogez vos journaux avec Amazon CloudWatch Logs Insights, qui découvre automatiquement les champs JSON formatés.
- Le partage de groupes de journaux entre les AWS Transfer Family ressources vous permet de combiner les flux de journaux provenant de plusieurs serveurs en un seul groupe de journaux, ce qui facilite la gestion de vos configurations de surveillance et de vos paramètres de conservation des journaux.
- Créez des statistiques agrégées et des visualisations qui peuvent être ajoutées aux CloudWatch tableaux de bord.
- Suivez les données d'utilisation et de performance en utilisant des groupes de journaux pour créer des métriques de journal, des visualisations et des tableaux de bord consolidés.

Les options pour `LoggingRole` ou `StructuredLogDestinations` sont configurées et contrôlées séparément. Pour chaque serveur, vous pouvez configurer une ou les deux méthodes de journalisation, ou configurer votre serveur pour qu'il n'y ait aucune journalisation (bien que cela ne soit pas recommandé).

Si vous créez un nouveau serveur à l'aide de la console Transfer Family, la journalisation est activée par défaut. Après avoir créé le serveur, vous pouvez utiliser l'`UpdateServerAPI` appel pour modifier votre configuration de journalisation. Pour plus de détails, voir [StructuredLogDestinations](#).

Actuellement, pour les flux de travail, si vous souhaitez activer la journalisation, vous devez spécifier un rôle de journalisation :

- Si vous associez un flux de travail à un serveur à l'aide de l'UpdateServerAPI appel `CreateServer` or, le système ne crée pas automatiquement de rôle de journalisation. Si vous souhaitez enregistrer les événements de votre flux de travail, vous devez explicitement associer un rôle de journalisation au serveur.
- Si vous créez un serveur à l'aide de la console Transfer Family et que vous associez un flux de travail, les journaux sont envoyés à un groupe de journaux dont le nom contient l'ID du serveur. Le format est `/aws/transfer/server-id`, par exemple, `/aws/transfer/s-1111aaaa2222bbbb3`. Les journaux du serveur peuvent être envoyés à ce même groupe de journaux ou à un autre.

Considérations relatives à la journalisation pour la création et la modification de serveurs dans la console

- Les nouveaux serveurs créés via la console ne prennent en charge que la JSON journalisation structurée, sauf si un flux de travail est attaché au serveur.
- L'absence de journalisation n'est pas une option pour les nouveaux serveurs que vous créez dans la console.
- Les serveurs existants peuvent activer la JSON journalisation structurée via la console à tout moment.
- L'activation de la JSON journalisation structurée via la console désactive la méthode de journalisation existante, afin de ne pas facturer deux fois les clients. L'exception se produit si un flux de travail est attaché au serveur.
- Si vous activez la JSON journalisation structurée, vous ne pourrez pas la désactiver ultérieurement via la console.
- Si vous activez la JSON journalisation structurée, vous pouvez modifier à tout moment la destination du groupe de journaux via la console.
- Si vous activez la JSON journalisation structurée, vous ne pouvez pas modifier le rôle de journalisation via la console si vous avez activé les deux types de journalisation via le API. L'exception est si votre serveur est associé à un flux de travail. Cependant, le rôle de journalisation continue d'apparaître dans Détails supplémentaires.

Considérations relatives à la journalisation pour la création et la modification de serveurs à l'aide de API SDK

- Si vous créez un nouveau serveur via le API, vous pouvez configurer l'un des types de journalisation ou les deux, ou choisir de ne pas enregistrer de journalisation.
- Pour les serveurs existants, activez et désactivez la JSON journalisation structurée à tout moment.
- Vous pouvez modifier le groupe de journaux API à tout moment via le.
- Vous pouvez modifier le rôle de journalisation via le API à tout moment.

Pour activer la journalisation structurée, vous devez être connecté à un compte avec les autorisations suivantes

- logs:CreateLogDelivery
- logs>DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs>ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

Un exemple de politique est disponible dans la section [Configurer le rôle de CloudWatch journalisation](#).

Rubriques

- [Création d'une journalisation pour les serveurs](#)
- [Mise à jour de la journalisation pour un serveur](#)
- [Affichage de la configuration du serveur](#)

Création d'une journalisation pour les serveurs

Lorsque vous créez un nouveau serveur, sur la page Configurer les détails supplémentaires, vous pouvez spécifier un groupe de journaux existant ou en créer un nouveau.

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☒ Create a new log group ☐ Choose an existing log group

Choose an existing log group

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

ⓘ Logging role is only required when selecting a workflow in the Managed workflows section below.

Si vous choisissez un groupe de journaux existant, vous devez en sélectionner un qui est associé à votre Compte AWS.

Transfer Family > Servers > Create server

Step 1
Choose protocols

Step 2
Choose an identity provider

Step 3
Choose an endpoint

Step 4
Choose a domain

Step 5
Configure additional details

Step 6
Review and create

Configure additional details

Logging Info

Log group Info
Choose the CloudWatch log group where your events will be delivered in a structured JSON format

☐ Create a new log group ☒ Choose an existing log group

/aws/transfer/

Logging role Info
Choose the IAM role that will be used to deliver events to your CloudWatch logs

☐ Create a new role ☐ Choose an existing role

ⓘ Logging role is only required when selecting a workflow in the Managed workflows section below.

Si vous choisissez Créer un groupe de journaux, la CloudWatch console (<https://console.aws.amazon.com/cloudwatch/>) s'ouvre sur la page Créer un groupe de journaux. Pour plus de détails, voir [Création d'un groupe de CloudWatch journaux dans Logs](#).

Mise à jour de la journalisation pour un serveur

Les informations relatives à la journalisation dépendent du scénario de votre mise à jour.

Note

Lorsque vous optez pour la JSON journalisation structurée, il peut arriver, dans de rares cas, que Transfer Family arrête de se connecter dans l'ancien format, mais qu'il faille un certain temps pour commencer à se connecter dans le nouveau JSON format. Cela peut entraîner des événements qui ne sont pas enregistrés. Il n'y aura aucune interruption de service, mais vous devez être prudent lorsque vous transférez des fichiers au cours de la première heure suivant le changement de méthode de journalisation, car les journaux pourraient être supprimés.

Si vous modifiez un serveur existant, vos options dépendent de l'état du serveur.

- Un rôle de journalisation est déjà activé sur le serveur, mais la JSON journalisation structurée n'est pas activée.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/scooter ▼



Create log group [↗](#)

Enabling the structured JSON log format will override your existing logging configuration. Potential changes include new log format and log group.

Logging Role [Info](#)

Select an existing role from your account

AWSTransferLoggingAccess ▼



Workflows events will be delivered to a log group labelled with the server ID.

- Aucune journalisation n'est activée sur le serveur.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☐ Enable structured JSON logging

Choose an existing log group ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- La JSON journalisation structurée est déjà activée sur le serveur, mais aucun rôle de journalisation n'est spécifié.

Edit additional details

Logging [Info](#)

Log group [Info](#)

Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

/aws/transfer/ ▼



Create log group [↗](#)

Logging Role [Info](#)

Select an existing role from your account

Choose a role ▼



Logging role is only required when selecting a workflow in the Managed workflows section below.

- La JSON journalisation structurée est déjà activée sur le serveur et un rôle de journalisation est également spécifié.

Edit additional details

Logging [Info](#)

Log group [Info](#)
Choose an existing log group from the dropdown or create a new log group in Amazon CloudWatch

☒ Enable structured JSON logging

▼

Logging Role [Info](#)
Select an existing role from your account

▼

 Workflows events will be delivered to a log group labelled with the server ID.

Affichage de la configuration du serveur

Les détails de la page de configuration du serveur dépendent de votre scénario :

Selon votre scénario, la page de configuration du serveur peut ressembler à l'un des exemples suivants :

- Aucune journalisation n'est activée.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role -	Passive IP -

- La JSON journalisation structurée est activée.

Additional details
Edit

Log group /aws/transfer/s[redacted]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- Le rôle de journalisation est activé, mais pas la JSON journalisation structurée.

Additional details
Edit

Log group -	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-[redacted]	SetStat option Ignore
Server host key Info SHA256:lx39/[redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2018-11	Managed workflows execution role [redacted] execution-role [redacted]	Passive IP -

- Les deux types de journalisation (rôle de journalisation et JSON journalisation structurée) sont activés.

Additional details

Edit

Log group /aws/transfer/s-	Domain Amazon S3	Login display banner View the display message
Logging role Info AWSTransferLoggingAccess	Workflow for complete uploads w-	SetStat option Ignore
Server host key Info SHA256:	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role transfer-workflows	Passive IP -

Gestion de la journalisation des flux de travail

CloudWatch fournit un audit et une journalisation consolidés de la progression et des résultats du flux de travail. AWS Transfer Family Fournit également plusieurs mesures pour les flux de travail. Vous pouvez consulter les statistiques indiquant le nombre d'exécutions de flux de travail démarrées, terminées avec succès et échouées au cours de la minute précédente. Toutes les CloudWatch mesures relatives à Transfer Family sont décrites dans [Utilisation CloudWatch des métriques pour Transfer Family](#).

Afficher les CloudWatch journaux Amazon pour les flux de travail

1. Ouvrez la CloudWatch console Amazon à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le volet de navigation de gauche, choisissez Logs, puis Log groups.
3. Sur la page Groupes de journaux, dans la barre de navigation, choisissez la région appropriée pour votre AWS Transfer Family serveur.
4. Choisissez le groupe de journaux correspondant à votre serveur.

Par exemple, si l'ID de votre serveur est -1234567890abcdef0, votre groupe de journaux l'est /aws/transfer/s-1234567890abcdef0.

5. Sur la page des détails du groupe de journaux de votre serveur, les flux de journaux les plus récents sont affichés. Il existe deux flux de log pour l'utilisateur que vous explorez :

- Un pour chaque session Secure Shell (SSH) File Transfer Protocol (SFTP).
- Un pour le flux de travail en cours d'exécution pour votre serveur. Le format du flux de journal pour le flux de travail est `username.workflowID.uniqueStreamSuffix`.

Par exemple, si votre utilisateur l'est `mary-major`, vous disposez des flux de journaux suivants :

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

Note

Les identifiants alphanumériques à 16 chiffres répertoriés dans cet exemple sont fictifs. Les valeurs que vous voyez sur Amazon CloudWatch sont différentes.

La page Enregistrer les événements de `mary-major-usa-east.1234567890abcdef0` affiche les détails de chaque session utilisateur, et le flux de `mary.w-abcdef01234567890.021345abcdef6789` journal contient les détails du flux de travail.

Voici un exemple de flux de journal pour `mary.w-abcdef01234567890.021345abcdef6789`, basé sur un flux de travail (`w-abcdef01234567890`) contenant une étape de copie.

```
{
  "type": "ExecutionStarted",
  "details": {
    "input": {
      "initialFileLocation": {
        "bucket": "DOC-EXAMPLE-BUCKET",
        "key": "mary/workflowSteps2.json",
        "versionId": "version-id",
        "etag": "etag-id"
      }
    }
  },
  "workflowId": "w-abcdef01234567890",
  "executionId": "execution-id",
  "transferDetails": {
    "serverId": "s-server-id",
    "username": "mary",
```

```

        "sessionId":"session-id"
    },
    {
        "type":"StepStarted",
        "details": {
            "input": {
                "fileLocation": {
                    "backingStore":"S3",
                    "bucket":"DOC-EXAMPLE-BUCKET",
                    "key":"mary/workflowSteps2.json",
                    "versionId":"version-id",
                    "etag":"etag-id"
                }
            },
            "stepType":"COPY",
            "stepName":"copyToShared"
        },
        "workflowId":"w-abcdef01234567890",
        "executionId":"execution-id",
        "transferDetails": {
            "serverId":"s-server-id",
            "username":"mary",
            "sessionId":"session-id"
        }
    },
    {
        "type":"StepCompleted",
        "details":{
            "output":{},
            "stepType":"COPY",
            "stepName":"copyToShared"
        },
        "workflowId":"w-abcdef01234567890",
        "executionId":"execution-id",
        "transferDetails":{
            "serverId":"server-id",
            "username":"mary",
            "sessionId":"session-id"
        }
    },
    {
        "type":"ExecutionCompleted",
        "details": {},
    }

```

```
"workflowId": "w-abcdef01234567890",
"executionId": "execution-id",
"transferDetails": {
  "serverId": "s-server-id",
  "username": "mary",
  "sessionId": "session-id"
}
}
```

Configurer le rôle de CloudWatch journalisation

Pour définir l'accès, vous devez créer une IAM politique basée sur les ressources et un IAM rôle fournissant ces informations d'accès.

Pour activer la CloudWatch journalisation Amazon, vous devez commencer par créer une IAM politique qui active la CloudWatch journalisation. Vous créez ensuite un IAM rôle et vous y associez la politique. Vous pouvez le faire lorsque vous [créez un serveur](#) ou en [modifiant un serveur existant](#). Pour plus d'informations CloudWatch, consultez [Qu'est-ce qu'Amazon CloudWatch ?](#) et [qu'est-ce qu'Amazon CloudWatch Logs ?](#) dans le guide de CloudWatch l'utilisateur Amazon.

Utilisez les exemples de IAM politiques suivants pour autoriser la CloudWatch journalisation.

Use a logging role

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
    }
  ]
}
```

Use structured logging

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": "arn:aws:logs:region-id:Compte AWS:log-group:/aws/transfer/*"
    }
  ]
}
```

Dans l'exemple de politique précédent, pour le **Resource**, remplacez *region-id* and *Compte AWS* avec vos valeurs. Par exemple, **"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**

Vous créez ensuite un rôle et associez la politique de CloudWatch journalisation que vous avez créée.

Pour créer un IAM rôle et y associer une politique

1. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.

Sur la page Créer un rôle, assurez-vous que le AWS service est sélectionné.

2. Choisissez Transfer (Transférer) dans la liste des services, puis Next: Permissions (Suivant : Autorisations). Cela établit une relation de confiance entre AWS Transfer Family et le IAM rôle. De plus, ajoutez `aws:SourceAccount` et `aws:SourceArn` conditionnez des clés pour vous protéger contre le problème de confusion des adjoints. Consultez la documentation suivante pour plus de détails :

- Procédure pour établir une relation de confiance avec AWS Transfer Family : [Étape 1 : Établir une relation d'approbation](#)
 - Description du problème des députés confus : [le problème des députés confus](#)
3. Dans la section Joindre des politiques d'autorisation, recherchez et choisissez la politique de CloudWatch journalisation que vous venez de créer, puis choisissez Next : Tags.
 4. (Facultatif) Entrez une clé et une valeur pour une balise, puis choisissez Next: Review (Suivant : Vérifier).
 5. Sur la page Review (Vérifier), entrez un nom et une description pour votre nouveau rôle, puis choisissez Create role (Créer un rôle).
 6. Pour consulter les journaux, choisissez l'ID du serveur pour ouvrir la page de configuration du serveur, puis choisissez Afficher les journaux. Vous êtes redirigé vers la CloudWatch console où vous pouvez consulter vos flux de journaux.

Sur la CloudWatch page de votre serveur, vous pouvez voir les enregistrements de l'authentification des utilisateurs (réussite et échec), des téléchargements de données (PUTopérations) et des téléchargements de données (GETopérations).

Afficher les flux de log de Transfer Family

Pour consulter les journaux de votre serveur Transfer Family

1. Accédez à la page de détails d'un serveur.
2. Choisissez Afficher les journaux. Cela ouvre Amazon CloudWatch.
3. Le groupe de journaux du serveur que vous avez sélectionné s'affiche.

The screenshot shows the AWS CloudWatch console interface. On the left, the navigation sidebar is visible with the 'Log groups' section highlighted. The main content area displays the details for a specific log group, `/aws/transfer/s-`. The 'Log group details' section includes the ARN, creation time (2 years ago), retention (Never expire), and stored bytes (39.39 MB). Below this, there are tabs for 'Log streams', 'Metric filters', 'Subscription filters', 'Contributor Insights', 'Tags', and 'Data protection - new'. The 'Log streams' tab is currently selected, showing a list of log streams with a search bar and filters. The list includes a stream named 'ERRORS' and several streams from 'scooterstack4'.

4. Vous pouvez sélectionner un flux de journal pour afficher les détails et les entrées individuelles du flux.
 - S'il existe une liste pour ERRORS, vous pouvez la sélectionner pour afficher les détails des dernières erreurs survenues sur le serveur.

CloudWatch > Log groups > /aws/transfer/s- > ERRORS

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions

Create metric filter

Q

Filter events

Clear

1m

30m

1h

12h

Custom

Display

	Timestamp	Message	
		There are older events to load. Load more.	
	2023-03-23T16:08:29.281-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:30.979-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:32.647-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:34.306-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:36.010-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:08:37.659-04:00	ERRORS AUTH_FAILURE Method=password User=ubuntu Message= SourceIP=	
	2023-03-23T16:12:33.307-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
	2023-03-23T16:12:34.943-04:00	ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" Source...	
		ERRORS AUTH_FAILURE Method=password User=scooterstack4 Message="Missing POSIX profile" SourceIP=	Copy
	2023-03-23T16:12:56.857-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
	2023-03-23T16:12:58.430-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	
		ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	Copy
	2023-03-23T16:13:00.106-04:00	ERRORS AUTH_FAILURE Method=password User=debian Message= SourceIP=	

- Choisissez une autre entrée pour voir un exemple de flux de journal.

CloudWatch > Log groups > /aws/transfer/s- > scooterstack4.

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions

Create metric filter

Q

Filter events

Clear

1m

30m

1h

12h

Custom

Display

	Timestamp	Message	
		No older events at this moment. Retry	
	2023-03-23T16:19:43.747-04:00	scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- scooterstack4. CONNECTED SourceIP= User=scooterstack4 HomeDir=/fs- Client=SSH-2.0- OpenSSH_7.4 Role=arn:aws:iam:: :role/ Kex=	Copy
	2023-03-23T16:19:47.030-04:00	scooterstack4. DISCONNECTED scooterstack4. DISCONNECTED	Copy
		No newer events at this moment. Auto retry paused. Resume	

- Si un flux de travail géré est associé à votre serveur, vous pouvez consulter les journaux des exécutions du flux de travail.

Note

Le format du flux de journal pour le flux de travail est `username.workflowId.uniqueStreamSuffix`. Par exemple, `decrypt-user.w-a1111222233334444.aaaa1111bbbb2222` peut être le nom d'un flux de journal pour l'utilisateur et le flux de travail. **decrypt-user w-a1111222233334444**

CloudWatch > Log groups > /aws/transfer/s- > decrypt-user.w-

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Actions Create metric filter

Filter events Clear 1m 30m 1h 12h Custom Display

Timestamp	Message
	There are older events to load. Load more .
2023-03-21T13:37:57.795-04:00	<code>{"type": "StepStarted", "details": {"input": {"fileLocation": {"backingStore": "S3", "bucket": "", "key": "decrypt-"</code>
2023-03-21T14:12:02.850-04:00	<code>{"type": "StepStarted", "details": {"input": {"fileLocation": {"backingStore": "S3", "bucket": "", "key": "decrypt-"</code>
	<pre>{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "", "key": "decrypt-user/test.json.gpg", "versionId": "", "etag": "" } } }, "stepType": "DECRYPT", "stepName": "decrypt-step" }, "workflowId": "w-", "executionId": "", "transferDetails": { "serverId": "s-", "username": "decrypt-user", "sessionId": "" } }</pre>
2023-03-21T14:12:03.464-04:00	<code>{"type": "StepCompleted", "details": {"output": {}}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-</code>

Note

Pour toute entrée de journal étendue, vous pouvez copier l'entrée dans le presse-papiers en choisissant Copier. Pour plus de détails sur les CloudWatch journaux, consultez la section [Affichage des données des journaux](#).

Création d' CloudWatch alarmes Amazon

L'exemple suivant montre comment créer des CloudWatch alarmes Amazon à l'aide de la AWS Transfer Family métrique,FilesIn.

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-000000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
    cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

AWS CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-000000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

Enregistrement des API appels Amazon S3 dans les journaux d'accès S3

Si vous [utilisez les journaux d'accès Amazon S3 pour identifier les demandes S3](#) effectuées au nom de vos utilisateurs de transfert de fichiers, ils RoleSessionName sont utilisés pour

afficher le IAM rôle assumé pour assurer les transferts de fichiers. Il affiche également des informations supplémentaires telles que le nom d'utilisateur, l'identifiant de session et l'identifiant du serveur utilisés pour les transferts. Le format est `[AWS:Role Unique Identifier]/username.sessionid@server-id` et est contenu dans le champ Demandeur. Par exemple, voici le contenu d'un exemple de champ Demandeur issu d'un journal d'accès S3 pour un fichier copié dans le compartiment S3.

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

Dans le champ Demandeur ci-dessus, il indique le IAM rôle appelé `IamRoleName`. Pour plus d'informations sur les identifiants uniques des IAM rôles, consultez la section [Identifiants uniques du Guide](#) de l'AWS Identity and Access Management utilisateur.

Exemples pour limiter le problème de confusion des adjoints

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 la confusion des adjoints. Pour en savoir plus, consultez [Prévention du problème de l'adjoint confus entre services](#).

Note

Dans les exemples suivants, remplacez chaque *user input placeholder* avec vos propres informations.

Dans ces exemples, vous pouvez supprimer les ARN détails d'un flux de travail si aucun flux de travail n'est associé à votre serveur.

L'exemple de politique de journalisation et d'appel suivant permet à n'importe quel serveur (et flux de travail) du compte d'assumer le rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": "transfer.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "account-id"
        },
        "ArnLike": {
            "aws:SourceArn": [
                "arn:aws:transfer:region:account-id:server/*",
                "arn:aws:transfer:region:account-id:workflow/*"
            ]
        }
    }
}
]
}

```

L'exemple de politique de journalisation et d'appel suivant permet à un serveur (et à un flux de travail) spécifiques d'assumer le rôle.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificServerWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                },
                "ArnEquals": {
                    "aws:SourceArn": [
                        "arn:aws:transfer:region:account-id:server/server-id",
                        "arn:aws:transfer:region:account-id:workflow/workflow-id"
                    ]
                }
            }
        }
    ]
}

```

```
]
}
```

CloudWatch structure du journal pour Transfer Family

Cette rubrique décrit les champs renseignés dans les journaux Transfer Family : à la fois pour les entrées de journal structurées en JSON et pour les entrées de journal existantes.

Rubriques

- [Journaux structurés JSON pour Transfer Family](#)
- [Les anciens journaux de Transfer Family](#)

Journaux structurés JSON pour Transfer Family

Le tableau suivant contient des informations détaillées sur les champs de saisie des journaux pour les actions Transfer Family SFTP/FTP/FTPS, dans le nouveau format de journal structuré JSON.

Champ	Description	Exemple d'entrée
activity-type	The action by the user	OUVERT FERMÉ PARTIAL_CLOSE DÉCONNECTÉ CONNECTÉ
bytes-in	Number of bytes uploaded by the user	29238420042
bytes-out	Number of bytes downloaded by the user	23094032490328
ciphers	Specifies the SSH cipher negotiated for the connection (available ciphers are listed in Algorithmes cryptographiques)	aes256-gcm@openssh.com
client	The user's client software	SSH-2.0-OpenSSH_7.4
home-dir	The directory that the end user lands on when they connect to the endpoint if their home	/user-home-bucket/test

Champ	Description	Exemple d'entrée
	directory type is PATH: if they have a logical home directory, this value is always /	
kex	Specifies the negotiated SSH key exchange (KEX) for the connection (available KEX are listed in Algorithmes cryptographiques)	diffie-hellman-group14-sha256
message	Provides more information related to the error	<i><string></i>
method	The authentication method	publickey
mode	Specifies how a client opens a file	CREATE TRUNCATE WRITE
operation	The client operation on a file	OPEN CLOSE
path	Actual file path affected	/user-test-bucket/test-file-1.pdf
resource-arn	A system-assigned, unique identifier for a specific resource (for example, a server)	arn:aws:transfer:ap-northeast-1:12346789012 : server/s-1234567890akeu2js2
role	The IAM role of the user	arn:aws:iam : :0293883675:role/testuser-role
session-id	A system-assigned, unique identifier for a single session	9ca9a0e1cec6ad9d
source-ip	Client IP address	18.323.0.129
user	The end user's username	myname192

Champ	Description	Exemple d'entrée
user-policy	The permissions specified for the end user: this field is populated if the user's policy is a session policy.	The JSON code for the session policy that is being used

Les anciens journaux de Transfer Family

Le tableau suivant contient des informations détaillées sur les entrées du journal relatives aux différentes actions de Transfer Family.

Note

Ces entrées ne sont pas dans le nouveau format de journal structuré JSON.

Le tableau suivant contient des informations détaillées sur les entrées de journal relatives aux différentes actions Transfer Family, dans le nouveau format de journal structuré JSON.

Action	Journaux correspondants dans Amazon CloudWatch Logs
Authentication failures (Échecs d'authentification)	ERREURS AUTH_FAILURE METHOD=PublicKey User=LHR Message="RSA SHA256:LFZ3R2NMLY4RAK+B7RB1RSVUIBAE+A+HXG0C7L1JIZ0" SourceIP=3.8.172.211
Flux de travail COPIER/TAG/SUPPRIMER/DÉCHIFFRER	<pre> {"type" : "StepStarted", "details" : {"input" : {"Emplacement du fichier" : {"BackingStore" : "EFS", "FileSystemID" : fs-12345678", "path" : "/lhr/regex.py"}}, "StepType" : "StepName" : "successful_tag_step", "WorkflowID" : w-1111aaa a22bb22bb22b bb3", "ExecutionID" : « 81234abcd-1234-efgh-5678-ijklmnopqr90 », </pre>

Action	Journaux correspondants dans Amazon CloudWatch Logs
	« TransferDetails » : {« serverID » ="s-1234abcd5678efghi », « nom d'utilisateur » lhr », « ID de session » 1_1234567890abcdef0"}}
Flux de travail par étapes personnalisé	{ "type » : » CustomStepInvoked « , « details » : { "output » : { "token » : { "jeton » ?MZM4mjg5ywuty EzMy 00 Yjlz LWI3OG MtYz U4OGI2ZjQyMz E5" }, « StepType » /CUSTOM », « StepName » "efs-s3_copy_2", « WorkflowID » "w-9283e49d33297c3f7", « ExecutionId » 1234abcd-1234-efgh-5678-ijklmnopqr90 », « TransferDetails » : {« serverID » : « s-zzzzzzz111aaaa22223 », « nom d'utilisateur » « lhr », « ID de session » : 1234567890abcdef0"}}
Suppressions	lhr.33a8fb495ffb383b SUPPRIMER LE CHEMIN=/bucket/user/123.jpg
Téléchargements	lhr.33a8fb495ffb383b OPEN PATH=/bucket/user/123.jpg Mode=LIRE lhr.33a8fb495ffb383b FERMER LE CHEMIN=/Bucket/User/123.jpg =3618546 BytesOut
Connexions/Déconnexions	user.914984e553bcd6db6 CONNECTED SourceIP=1.22.111.222 User=LHR =LOGICAL CLIENT=SSH-2.0-OpenSSH_7.4 role=ARN: aws : :iam : :123456789012:role/sftp-s3-access HomeDir user.914984e553bcd6db6 DÉCONNECTÉ
Renomme	lhr.33a8fb495ffb383b RENOMMER LE CHEMIN =/bucket/user/lambo.png =/bucket/utilisateur/ferrari.png NewPath

Action	Journaux correspondants dans Amazon CloudWatch Logs
Exemple de journal des erreurs du flux de travail	<pre>{ "type": "StepErrored", "details": { "ErrorType": "BAD_REQUEST", "ErrorMessage": "Impossible de baliser le fichier Efs", "StepType": "StepName", "StepName": "successful_tag_step", "ExecutionId": "i-1234abcd-1234-efghi-5678-ijklmnopqr90", "TransferDetails": { "serverID": "s-1234abcd5678efghi", "nom d'utilisateur": "lhr", "ID de session": "1234567890abcdef0" } } }</pre>
Liens symboliques	<pre>lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs-12345678/lhr/pqr.jpg =abc.jpg LinkPath TargetPath</pre>
Chargements	<pre>lhr.33a8fb495ffb383b OPEN PATH=/bucket/ user/123.jpg Mode=Cr��er Troncat ��crire lhr.33a8fb495ffb383b FERMER LE CHEMIN=/B ucket/User/123.jpg =3618546 BytesIn</pre>

Action	Journaux correspondants dans Amazon CloudWatch Logs
Flux de travail	<pre> {"type": "ExecutionStarted", "details": { "input": { "BackingStore": "EFS", "FileSystemID": "fs-12345678", "initialFileLocation": { "path": "/lhr/regex.py" } }, "WorkflowID": "w-1111aaaa2222bbbb3", "ExecutionID": "1234abcd-1234-efmgh-5678-ijklmnopqr90", "TransferDetails": { "serverID": "s-zzzz1111aaaa22223", "nom d'utilisateur": "lhr", "ID de session": "c:1234567890abcdef0" } }}</pre> <pre> {"type": "StepStarted", "details": { "input": { "Emplacement du fichier": { "BackingStore": "EFS", "FileSystemID": "fs-12345678", "path": "/lhr/regex.py" } }, "StepType": "CUSTOM", "StepName": "efs-s3_copy_2", "WorkflowID": "w-9283e49dd297c3f7", "ExecutionID": "1234abcd-1234-efgh-5678-ijklmnopqr90", "TransferDetails": { "ServerID": "s-18ca49dce5d842e0b", "nom d'utilisateur": "lhr", "ID de session": "1234567890abcdef0" } }}</pre>

Exemples d'entrées de CloudWatch journal

Cette rubrique présente des exemples d'entrées de journal.

Rubriques

- [Exemples d'entrées du journal des sessions de transfert](#)
- [Exemples d'entrées de journal pour les SFTP connecteurs](#)
- [Exemples d'entrées de journal pour les défaillances de l'algorithme d'échange de clés](#)

Exemples d'entrées du journal des sessions de transfert

Dans cet exemple, un SFTP utilisateur se connecte à un serveur Transfer Family, télécharge un fichier, puis se déconnecte de la session.

L'entrée de journal suivante indique qu'un SFTP utilisateur se connecte à un serveur Transfer Family.

```
{
  "role": "arn:aws:iam::500655546075:role/scooter-transfer-s3",
  "activity-type": "CONNECTED",
  "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
  "client": "SSH-2.0-OpenSSH_7.4",
  "source-ip": "52.94.133.133",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "home-dir": "/scooter-test/log-me",
  "user": "log-me",
  "kex": "ecdh-sha2-nistp256",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

L'entrée de journal suivante indique que l'SFTP utilisateur télécharge un fichier dans son compartiment Amazon S3.

```
{
  "mode": "CREATE|TRUNCATE|WRITE",
  "path": "/scooter-test/log-me/config-file",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

Les entrées de journal suivantes indiquent que l'SFTP utilisateur s'est déconnecté de sa SFTP session. Tout d'abord, le client ferme la connexion au bucket, puis il déconnecte la SFTP session.

```
{
  "path": "/scooter-test/log-me/config-file",
  "activity-type": "CLOSE",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
}
```

```

"bytes-in": "121",
"session-id": "9ca9a0e1cec6ad9d"
}

{
  "activity-type": "DISCONNECTED",
  "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
  "session-id": "9ca9a0e1cec6ad9d"
}

```

Exemples d'entrées de journal pour les SFTP connecteurs

Cette section contient des exemples de journaux indiquant à la fois un transfert réussi et un transfert infructueux. Les journaux sont générés dans un groupe de journaux nommé `/aws/transfer/connector-id`, où *connector-id* est l'identifiant de votre SFTP connecteur.

Note

Les entrées de journal pour les SFTP connecteurs ne sont générées que lorsque vous exécutez une `StartFileTransfer` commande.

Cette entrée de journal concerne un transfert effectué avec succès.

```

{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T16:33:27.373720Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
  "file-path": "/remotebucket/remotefilepath",
  "status-code": "COMPLETED",
  "start-time": "2023-10-25T16:33:26.945481Z",
  "end-time": "2023-10-25T16:33:27.159823Z",
  "account-id": "480351544584",
  "connector-arn": "arn:aws:transfer:us-east-1:480351544584:connector/connector-id",
  "local-directory-path": "/connectors-localbucket"
}

```

Cette entrée de journal concerne un transfert qui a expiré et qui n'a donc pas été effectué correctement.

```
{
  "operation": "RETRIEVE",
  "timestamp": "2023-10-25T22:33:47.625703Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "url": "sftp://192.0.2.0",
  "file-path": "/remotebucket/remotefilepath",
  "status-code": "FAILED",
  "failure-code": "TIMEOUT_ERROR",
  "failure-message": "Transfer request timeout.",
  "account-id": "480351544584",
  "connector-arn": "arn:aws:transfer:us-east-1:480351544584:connector/connector-id",
  "local-directory-path": "/connectors-localbucket"
}
```

Descriptions de certains champs clés dans les exemples de journaux précédents.

- `timestamp` représente le moment où le journal est ajouté à CloudWatch. `start-time` et `end-time` correspondent au moment où le connecteur commence et termine réellement un transfert.
- `transfer-id` est un identifiant unique attribué à chaque `start-file-transfer` demande. Si l'utilisateur transmet plusieurs chemins de fichiers en un seul `start-file-transfer` API appel, tous les fichiers sont partagés de la même manière `transfer-id`.
- `file-transfer-id` est une valeur unique générée pour chaque fichier transféré. Notez que la partie initiale du `file-transfer-id` est identique à `transfer-id`.

Exemples d'entrées de journal pour les défaillances de l'algorithme d'échange de clés

Cette section contient des exemples de journaux dans lesquels l'algorithme d'échange de clés (KEX) a échoué. Voici des exemples tirés du flux de `ERRORS` journaux pour les journaux structurés.

Cette entrée de journal est un exemple d'erreur de type de clé d'hôte.

```
{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
```

```

    "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
    "message": "no matching host key type found",
    "kex": "ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ecdsa-sha2-
nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-
nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ssh-dss"
}

```

Cette entrée de journal est un exemple de KEX non-concordance.

```

{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
  "message": "no matching key exchange method found",
  "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}

```

Utilisation CloudWatch des métriques pour Transfer Family

Note

Vous pouvez également obtenir des statistiques pour Transfer Family à partir de la console Transfer Family elle-même. Pour plus d'informations, consultez [Surveillance de l'utilisation dans la console](#).

Vous pouvez obtenir des informations sur votre serveur à l'aide de CloudWatch métriques. Une métrique représente un ensemble chronologique de points de données publiés sur CloudWatch. Lorsque vous utilisez des métriques, vous devez spécifier l'espace de noms Transfer Family, le nom de la métrique et [la dimension](#). Pour plus d'informations sur les métriques, consultez [Metrics](#) dans le guide de CloudWatch l'utilisateur Amazon.

Le tableau suivant décrit les CloudWatch indicateurs de Transfer Family.

Espace de noms	Métrique	Description
AWS/Transfer	BytesIn	Nombre total d'octets transférés vers le serveur.

Espace de noms	Métrique	Description
		Unités : nombre Période : 5 minutes
	BytesOut	Nombre total d'octets transférés hors du serveur. Unité : nombre Période : 5 minutes
	FilesIn	Le nombre total de fichiers transférés sur le serveur. Pour les serveurs utilisant le AS2 protocole, cette métrique représente le nombre de messages reçus. Unités : nombre Période : 5 minutes
	FilesOut	Le nombre total de fichiers transférés hors du serveur. Unités : nombre Période : 5 minutes
	InboundMessage	Nombre total de AS2 messages reçus avec succès d'un partenaire commercial. Unités : nombre Période : 5 minutes
	InboundFailedMessage	Nombre total de AS2 messages reçus sans succès de la part d'un partenaire commercial. En d'autres termes, un partenaire commercial a envoyé un message, mais le serveur Transfer Family n'a pas réussi à le traiter. Unités : nombre Période : 5 minutes

Espace de noms	Métrique	Description
	OnPartialUploadExecutionsStarted	Nombre total d'exécutions de on-partial-upload flux de travail démarrées sur le serveur. Unités : nombre Durée : 1 minute
	OnPartialUploadExecutionsSuccessful	Nombre total d'exécutions de on-partial-upload flux de travail réussies sur le serveur. Unités : nombre Durée : 1 minute
	OnPartialUploadExecutionsFailed	Nombre total d'exécutions de on-partial-upload flux de travail infructueuses sur le serveur. Unités : nombre Durée : 1 minute
	OnUploadExecutionsStarted	Nombre total d'exécutions de flux de travail démarrées sur le serveur. Unités : nombre Durée : 1 minute
	OnUploadExecutionsSuccessful	Nombre total d'exécutions de flux de travail réussies sur le serveur. Unités : nombre Durée : 1 minute

Espace de noms	Métrique	Description
	OnUploadExecutionsFailed	Nombre total d'exécutions de flux de travail infructueuses sur le serveur. Unités : nombre Durée : 1 minute

Dimensions de Transfer Family

Une dimension est une paire nom-valeur qui fait partie de l'identité d'une métrique. Pour plus d'informations sur les dimensions, consultez la section [Dimensions](#) du guide de CloudWatch l'utilisateur Amazon.

Le tableau suivant décrit la CloudWatch dimension de Transfer Family.

Dimension	Description
ServerId	L'identifiant unique du serveur.

Utilisation Notifications des utilisateurs AWS avec AWS Transfer Family

Pour être informé AWS Transfer Family des événements, vous pouvez [Notifications des utilisateurs AWS](#) configurer différents canaux de diffusion. Lorsqu'un événement correspond à une règle que vous spécifiez, vous recevez une notification.

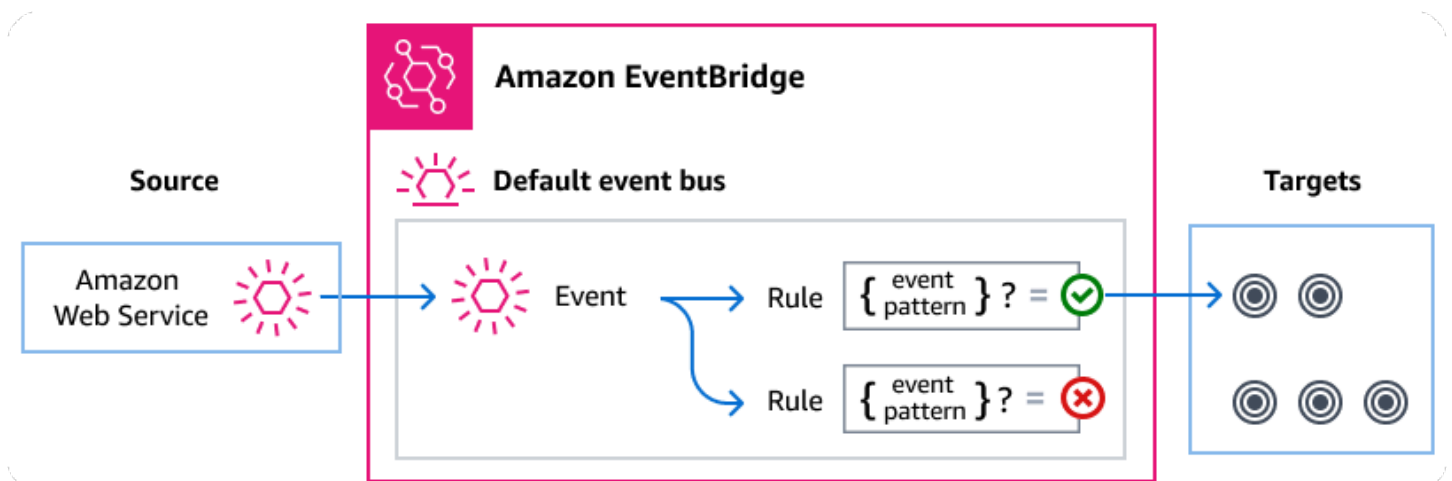
Vous pouvez recevoir des notifications relatives à des événements via plusieurs canaux, notamment des e-mails, des notifications de chat [Amazon Q Developer in chat applications](#) ou des notifications push [AWS Console Mobile Application](#). Vous pouvez également consulter les notifications dans le [centre de notifications de la console](#). Notifications des utilisateurs prend en charge l'agrégation, ce qui peut réduire le nombre de notifications que vous recevez lors d'événements spécifiques.

Pour plus d'informations, consultez le billet de blog [Personnaliser les notifications de livraison de fichiers AWS Transfer Family à l'aide de flux de travail gérés](#) et [Qu'est-ce que c'est Notifications des utilisateurs AWS ?](#) dans le guide de Notifications des utilisateurs AWS l'utilisateur.

Gestion des Transfer Family événements à l'aide de Amazon EventBridge

Amazon EventBridge est un service sans serveur qui utilise des événements pour connecter les composants de l'application entre eux, ce qui peut vous permettre de créer plus facilement des applications évolutives pilotées par des événements. L'architecture axée sur les événements est un style qui consiste à créer des systèmes logiciels faiblement couplés qui fonctionnent ensemble en émettant des événements et en y répondant. Les événements représentent un changement dans une ressource ou un environnement.

Comme c'est le cas pour de nombreux AWS services, Transfer Family génère et envoie des événements au bus d'événements EventBridge par défaut. Notez que le bus d'événements par défaut est automatiquement configuré dans chaque AWS compte. Un bus d'événements est un routeur qui reçoit des événements et les transmet à zéro ou plusieurs destinations, ou cibles. Vous définissez des règles pour le bus d'événements qui évalue les événements à leur arrivée. Chaque règle vérifie si un événement correspond au modèle d'événements de la règle. Si l'événement correspond, le bus d'événements envoie l'événement à une ou plusieurs cibles spécifiées.



Rubriques

- [Transfer Family événements](#)
- [Envoi d' Transfer Family événements à l'aide de EventBridge règles](#)
- [Amazon EventBridge autorisations](#)
- [EventBridge Ressources supplémentaires](#)
- [Transfer Family référence détaillée des événements](#)

Transfer Family événements

Transfer Family envoie automatiquement les événements au bus d' EventBridge événements par défaut. Vous pouvez créer des règles sur le bus d'événements, chaque règle incluant un modèle d'événement et une ou plusieurs cibles. Les événements qui correspondent au modèle d'événements d'une règle sont transmis aux cibles spécifiées dans la [mesure du possible](#), mais certains événements peuvent être livrés dans le désordre.

Les événements suivants sont générés par Transfer Family. Pour plus d'informations, consultez les [EventBridge événements](#) dans le guide de Amazon EventBridge l'utilisateur.

SFTPFTPS, et événements FTP du serveur

Type de détail de l'événement	Description
FTPTéléchargement du serveur de fichiers terminé	Un fichier a été téléchargé avec succès pour le FTP protocole.
FTPÉchec du téléchargement du serveur de fichiers	Une tentative de téléchargement de fichier a échoué pour le FTP protocole.
FTPChargement du serveur de fichiers terminé	Un fichier a été chargé avec succès pour le FTP protocole.
FTPEchec du téléchargement du serveur de fichiers	Une tentative de téléchargement de fichier a échoué pour le FTP protocole.
FTPSTéléchargement du serveur de fichiers terminé	Un fichier a été téléchargé avec succès pour le FTPS protocole.
FTPSÉchec du téléchargement du serveur de fichiers	Une tentative de téléchargement de fichier a échoué pour le FTPS protocole.
FTPSChargement du serveur de fichiers terminé	Un fichier a été chargé avec succès pour le FTPS protocole.
FTPSEchec du téléchargement du serveur de fichiers	Une tentative de téléchargement de fichier a échoué pour le FTPS protocole.

Type de détail de l'événement	Description
<u>SFTP</u>Téléchargement du fichier du serveur terminé	Un fichier a été téléchargé avec succès pour le SFTP protocole.
<u>SFTP</u>Échec du téléchargement du fichier du serveur	Une tentative de téléchargement de fichier a échoué pour le SFTP protocole.
<u>SFTP</u>Téléchargement du fichier du serveur terminé	Un fichier a été chargé avec succès pour le SFTP protocole.
<u>SFTP</u>Échec du téléchargement du fichier sur le serveur	Une tentative de téléchargement de fichier a échoué pour le SFTP protocole.

SFTP Événements liés aux connecteurs

Type de détail de l'événement	Description
<u>SFTP</u>Envoi du fichier du connecteur terminé	Un transfert de fichier d'un connecteur vers un SFTP serveur distant s'est terminé avec succès.
<u>SFTP</u>Échec de l'envoi du fichier du connecteur	Un transfert de fichier d'un connecteur vers un SFTP serveur distant a échoué.
<u>SFTP</u>Récupération du fichier du connecteur terminée	Un transfert de fichier d'un SFTP serveur distant vers un connecteur s'est terminé avec succès.
<u>SFTP</u>Échec de la récupération du fichier du connecteur	Un transfert de fichier d'un SFTP serveur distant vers un connecteur a échoué.

Événements A2S

Type de détail de l'événement	Description
<u>AS2</u>Réception de la charge utile terminée	La charge utile d'un AS2 message a été reçue.

Type de détail de l'événement	Description
AS2Échec de réception de la charge utile	La charge utile d'un AS2 message n'a pas été reçue.
AS2Envoi de la charge utile terminé	La charge utile d'un AS2 message a été envoyée avec succès.
AS2Échec de l'envoi de la charge utile	La charge utile d'un AS2 message n'a pas pu être envoyée.
AS2MDNRéception terminée	La notification de disposition d'un AS2 message a été reçue.
AS2MDNÉchec de réception	La notification de disposition d'un AS2 message n'a pas été reçue.
AS2MDNEnvoi terminé	La notification de disposition d'un AS2 message a été envoyée avec succès.
AS2MDNÉchec de l'envoi	La notification de disposition d'un AS2 message n'a pas pu être envoyée.

Envoi d' Transfer Family événements à l'aide de EventBridge règles

Si vous souhaitez que le bus d'événements EventBridge par défaut envoie Transfer Family des événements à une cible, vous devez créer une règle contenant un modèle d'événements correspondant aux données des Transfer Family événements souhaités.

Vous pouvez créer une règle en suivant ces étapes générales :

1. Créez un modèle d'événement pour la règle qui spécifie les éléments suivants :

- Transfer Family est la source des événements évalués par la règle.
- (Facultatif) Toute autre donnée d'événement à laquelle les comparer.

Pour de plus amples informations, veuillez consulter [???](#).

2. (Facultatif) Créez un transformateur d'entrée qui personnalise les données de l'événement avant de les EventBridge envoyer à la cible de la règle.

Pour plus d'informations, consultez la section [Transformation des entrées](#) dans le guide de EventBridge l'utilisateur.

3. Spécifiez les cibles auxquelles vous souhaitez EventBridge envoyer des événements qui correspondent au modèle d'événement.

Les cibles peuvent être d'autres AWS services, des applications SaaS (software as a service), des API destinations ou d'autres points de terminaison personnalisés. Pour plus d'informations, veuillez consulter la rubrique [Cibles](#) dans le Guide de l'utilisateur EventBridge .

Pour obtenir des instructions complètes sur la création de règles de bus d'événements, voir [Création de règles réagissant aux événements](#) dans le Guide de EventBridge l'utilisateur.

Création de modèles d'événements pour les Transfer Family événements

Lors Transfer Family de la transmission d'un événement au bus d'événements par défaut, EventBridge utilise le modèle d'événement défini pour chaque règle afin de déterminer si l'événement doit être transmis aux cibles de la règle. Un modèle d'événement correspond aux données des Transfer Family événements souhaités. Chaque modèle d'événement est un JSON objet qui contient les éléments suivants :

- Un attribut `source` qui identifie le service qui envoie l'événement. Pour les Transfer Family événements, la source est `aws.transfer`.
- (Facultatif) `detail-type` Attribut contenant un tableau des types d'événements à associer.
- (Facultatif) `detail` Attribut contenant toute autre donnée d'événement à laquelle faire correspondre.

Par exemple, le modèle d'événement suivant correspond à tous les événements provenant de Transfer Family :

```
{
  "source": ["aws.transfer"]
}
```

L'exemple de modèle d'événement suivant correspond à tous les événements du SFTP connecteur :

```
{
```

```
"source": ["aws.transfer"],
"detail-type": ["SFTP Connector File Send Completed", "SFTP Connector File Retrieve Completed",
                "SFTP Connector File Retrieve Failed", "SFTP Connector File Send Failed"]
}
```

L'exemple de modèle d'événement suivant correspond à tous les événements ayant échoué dans Transfer Family :

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
}
```

L'exemple de modèle d'événement suivant correspond à des SFTP téléchargements réussis pour l'utilisateur *username*:

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

Pour plus d'informations sur la rédaction de modèles d'événements, consultez la section [Modèles d'événements](#) dans le guide de EventBridge l'utilisateur.

Tester les modèles d' Transfer Family événements pour les événements dans EventBridge

Vous pouvez utiliser le EventBridge Sandbox pour définir et tester rapidement un modèle d'événement, sans avoir à terminer le processus général de création ou de modification d'une règle. À l'aide du Sandbox, vous pouvez définir un modèle d'événement et utiliser un exemple d'événement pour confirmer que le modèle correspond aux événements souhaités. EventBridge vous permet de créer une nouvelle règle en utilisant ce modèle d'événement directement depuis le sandbox.

Pour plus d'informations, consultez la section [Tester un modèle d'événement à l'aide du EventBridge Sandbox](#) dans le guide de l'EventBridge utilisateur.

Amazon EventBridge autorisations

Transfer Family ne nécessite aucune autorisation supplémentaire pour diffuser des événements à Amazon EventBridge.

Les cibles que vous spécifiez peuvent nécessiter des autorisations ou une configuration spécifiques. Pour plus de détails sur l'utilisation de services spécifiques pour les cibles, voir [Amazon EventBridge les cibles](#) dans le guide de Amazon EventBridge l'utilisateur.

EventBridge Ressources supplémentaires

Reportez-vous aux rubriques suivantes du [guide de Amazon EventBridge l'utilisateur](#) pour plus d'informations sur le traitement et la gestion des événements. EventBridge

- Pour des informations détaillées sur le fonctionnement des bus d'événements, consultez la section [bus Amazon EventBridge d'événements](#).
- Pour plus d'informations sur la structure des événements, consultez la section [Événements](#).
- Pour plus d'informations sur la création de modèles d'événements EventBridge à utiliser lors de la mise en correspondance d'événements par rapport à des règles, voir [Modèles d'événements](#).
- Pour plus d'informations sur la création de règles pour spécifier quels événements sont EventBridge traités, consultez la section [Règles](#).
- Pour plus d'informations sur la manière de spécifier les services ou autres destinations vers lesquels les événements correspondants EventBridge sont envoyés, consultez la section [Cibles](#).

Transfer Family référence détaillée des événements

Tous les événements des AWS services ont un ensemble commun de champs contenant des métadonnées relatives à l'événement. Ces métadonnées peuvent inclure le AWS service à l'origine de l'événement, l'heure à laquelle l'événement a été généré, le compte et la région dans lesquels l'événement a eu lieu, etc. Pour les définitions de ces champs généraux, voir la [référence relative à la structure des événements](#) dans le guide de Amazon EventBridge l'utilisateur.

En outre, chaque événement possède un champ `detail` qui contient des données spécifiques à cet événement en particulier. La référence suivante définit les champs de détail des différents Transfer Family événements.

Lorsque vous sélectionnez EventBridge et gérez des Transfer Family événements, tenez compte des points suivants :

- Le source champ pour tous les événements de Transfer Family est défini sur `aws.transfer`.
- Le champ detail-type indique le type d'événement.

Par exemple, `FTP File Server Download Completed`.

- Le champ detail contient les données spécifiques à cet événement en particulier.

Pour plus d'informations sur la création de modèles d'événements permettant aux règles de correspondre aux Transfer Family événements, voir [Modèles d'événements](#) dans le guide de Amazon EventBridge l'utilisateur.

Pour plus d'informations sur les événements et leur EventBridge traitement, reportez-vous à la section [Amazon EventBridge Événements](#) du Guide de Amazon EventBridge l'utilisateur.

Rubriques

- [SFTPFTPS, et événements FTP du serveur](#)
- [SFTPévénements liés aux connecteurs](#)
- [AS2événements](#)

SFTPFTPS, et événements FTP du serveur

Voici les champs détaillés pour SFTPFTPS, et les événements FTP du serveur :

- FTPTéléchargement du serveur de fichiers terminé
- FTPÉchec du téléchargement du serveur de fichiers
- FTPChargement du serveur de fichiers terminé
- FTPEchec du téléchargement du serveur de fichiers
- FTPSTéléchargement du serveur de fichiers terminé
- FTPSÉchec du téléchargement du serveur de fichiers
- FTPSChargement du serveur de fichiers terminé
- FTPSEchec du téléchargement du serveur de fichiers
- SFTPTéléchargement du fichier du serveur terminé
- SFTPÉchec du téléchargement du fichier du serveur

- SFTPTéléchargement du fichier du serveur terminé
- SFTPÉchec du téléchargement du fichier sur le serveur

Les `detail-type` champs source et sont inclus ci-dessous car ils contiennent des valeurs spécifiques pour les Transfer Family événements. Pour les définitions des autres champs de métadonnées inclus dans tous les événements, consultez la section [Référence de la structure des événements](#) dans le guide de Amazon EventBridge l'utilisateur.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "failure-code" : "string",
    "status-code" : "string",
    "protocol" : "string",
    "bytes" : "number",
    "client-ip" : "string",
    "failure-message" : "string",
    "end-timestamp" : "string",
    "etag" : "string",
    "file-path" : "string",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
}
```

detail-type

Identifie le type d'événement.

Pour cet événement, la valeur est l'un des noms FTPS d'événements FTP du serveur répertoriés précédemment. SFTP

source

Identifie le service qui a généré l'événement. Pour les événements Transfer Family, cette valeur est `aws.transfer`.

detail

JSONObjet contenant des informations sur l'événement. Le service qui génère l'événement détermine le contenu de ce champ.

Pour cet événement, les données incluent les éléments suivants :

failure-code

Catégorie expliquant pourquoi le transfert a échoué. Valeurs: PARTIAL_UPLOAD | PARTIAL_DOWNLOAD | UNKNOWN_ERROR

status-code

Si le transfert est réussi. Valeurs :COMPLETED | FAILED.

protocol

Protocole utilisé pour le transfert. Valeurs: SFTP | FTPS | FTP

bytes

Nombre d'octets transférés.

client-ip

Adresse IP du client impliqué dans le transfert

failure-message

Pour les transferts ayant échoué, les détails expliquant pourquoi le transfert a échoué.

end-timestamp

Pour les transferts réussis, horodatage indiquant la fin du traitement du fichier.

etag

La balise d'entité (uniquement utilisée pour les fichiers Amazon S3).

file-path

Le chemin d'accès au fichier transféré.

server-id

L'identifiant unique du serveur Transfer Family.

username

L'utilisateur qui effectue le transfert.

session-id

Identifiant unique de la session de transfert.

start-timestamp

Pour les transferts réussis, l'horodatage du début du traitement des fichiers.

Exemple SFTPExemple d'événement d'échec du téléchargement du fichier du serveur

L'exemple suivant montre un événement au cours duquel un téléchargement a échoué sur un SFTP serveur (Amazon EFS le stockage est-il utilisé).

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Server File Download Failed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2024-01-29T17:20:27Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
  ],
  "detail": {
    "failure-code": "PARTIAL_DOWNLOAD",
    "status-code": "FAILED",
    "protocol": "SFTP",
    "bytes": 4100,
    "client-ip": "IP-address",
    "failure-message": "File was partially downloaded.",
    "end-timestamp": "2024-01-29T17:20:27.749749117Z",
    "file-path": "/fs-1234abcd5678efghi/user0/test-file",
    "server-id": "s-1234abcd5678efghi",
    "username": "test",
    "session-id": "session-ID",
    "start-timestamp": "2024-01-29T17:20:16.706282454Z"
  }
}
```

Exemple FTPExemple d'événement « Téléchargement du serveur de fichiers terminé »

L'exemple suivant montre un événement au cours duquel un téléchargement s'Amazon S3 est terminé avec succès sur un FTP serveur (le stockage est-il utilisé).

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "FTP Server File Upload Completed",
  "source": "aws.transfer",
  "account": "958412138249",
  "time": "2024-01-29T16:31:43Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:transfer:us-east-1:958412138249:server/s-1111aaaa2222bbbb3"
  ],
  "detail": {
    "status-code": "COMPLETED",
    "protocol": "FTP",
    "bytes": 1048576,
    "client-ip": "10.0.0.141",
    "end-timestamp": "2024-01-29T16:31:43.311866408Z",
    "etag": "b6d81b360a5672d80c27430f39153e2c",
    "file-path": "/DOC-EXAMPLE-BUCKET/test/1mb_file",
    "server-id": "s-1111aaaa2222bbbb3",
    "username": "test",
    "session-id": "event-ID",
    "start-timestamp": "2024-01-29T16:31:42.462088327Z"
  }
}
```

SFTPÉvénements liés aux connecteurs

Les champs de détail relatifs aux événements du SFTP connecteur sont les suivants :

- SFTPEnvoi du fichier du connecteur terminé
- SFTPÉchec de l'envoi du fichier du connecteur
- SFTPRécupération du fichier du connecteur terminée
- SFTPÉchec de la récupération du fichier du connecteur

Les `detail-type` champs source et sont inclus ci-dessous car ils contiennent des valeurs spécifiques pour les Transfer Family événements. Pour les définitions des autres champs de métadonnées inclus dans tous les événements, consultez la section [Référence de la structure des événements](#) dans le guide de Amazon EventBridge l'utilisateur.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "operation" : "string",
    "connector-id" : "string",
    "transfer-id" : "string",
    "file-transfer-id" : "string",
    "url" : "string",
    "file-path" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "local-directory-path" : "string",
    "remote-directory-path" : "string",
    "bytes" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    }
  },
}
```

detail-type

Identifie le type d'événement.

Pour cet événement, la valeur est l'un des noms d'événements du SFTP connecteur répertoriés précédemment.

source

Identifie le service qui a généré l'événement. Pour les Transfer Family événements, cette valeur est `aws.transfer`.

detail

JSONObjet contenant des informations sur l'événement. Le service qui génère l'événement détermine le contenu de ce champ.

Pour cet événement, les données incluent les éléments suivants :

operation

Si la `StartFileTransfer` demande consiste à envoyer ou à récupérer un fichier.
Valeurs : `SEND` | `RETRIEVE`.

connector-id

Identifiant unique du SFTP connecteur utilisé.

transfer-id

L'identifiant unique de l'événement de transfert (une `StartFileTransfer` demande).

file-transfer-id

Identifiant unique du fichier transféré.

url

Celui URL du partenaire AS2 ou du SFTP point final.

file-path

Emplacement et fichier envoyés ou récupérés.

status-code

Si le transfert est réussi. Valeurs : `FAILED` | `COMPLETED`.

failure-code

En cas d'échec de transfert, code de raison pour lequel le transfert a échoué.

failure-message

Pour les transferts ayant échoué, les détails expliquant pourquoi le transfert a échoué.

`start-timestamp`

Pour les transferts réussis, l'horodatage du début du traitement des fichiers.

`end-timestamp`

Pour les transferts réussis, horodatage indiquant la fin du traitement du fichier.

`local-directory-path`

Pour les RETRIEVE demandes, emplacement dans lequel placer le fichier récupéré.

`remote-directory-path`

Pour les SEND demandes, le répertoire de fichiers dans lequel placer le fichier sur le SFTP serveur du partenaire. Il s'agit de la valeur `RemoteDirectoryPath` que l'utilisateur a transmise à la `StartFileTransfer` demande. Vous pouvez spécifier un répertoire par défaut sur le SFTP serveur du partenaire. Dans ce cas, ce champ est vide.

`bytes`

Le nombre d'octets transférés. La valeur est 0 pour les transferts échoués.

`local-file-location`

Ce paramètre contient les détails de l'emplacement du fichier AWS de stockage.

`domain`

Le stockage utilisé. Actuellement, la seule valeur est `S3`.

`bucket`

Le conteneur de l'objet dans Amazon S3.

`key`

Le nom attribué à l'objet dans Amazon S3.

Exemple SFTPExemple d'événement d'échec de l'envoi du fichier du connecteur

L'exemple suivant montre un événement au cours duquel un SFTP connecteur a échoué lors de la tentative d'envoi d'un fichier à un SFTP serveur distant.

```
{  
  "version": "0",
```



```

    "id": "event-ID",
    "detail-type": "SFTP Connector File Send Failed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T19:30:45Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "operation": "SEND",
        "connector-id": "c-f1111aaaa2222bbbb3",
        "transfer-id": "transfer-ID",
        "file-transfer-id": "file-transfer-ID",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
        "file-path": "/DOC-EXAMPLE-BUCKET/testfile.txt",
        "status-code": "FAILED",
        "failure-code": "CONNECTION_ERROR",
        "failure-message": "Unknown Host",
        "remote-directory-path": "",
        "bytes": 0,
        "start-timestamp": "2024-01-24T18:29:33.658729Z",
        "end-timestamp": "2024-01-24T18:29:33.993196Z",
        "local-file-location": {
            "domain": "S3",
            "bucket": "DOC-EXAMPLE-BUCKET",
            "key": "testfile.txt"
        }
    }
}

```

Exemple SFTPExemple d'événement Connector File Retrieve Completed

L'exemple suivant montre un événement au cours duquel un SFTP connecteur a réussi à récupérer un fichier envoyé par un SFTP serveur distant.

```

{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector File Retrieve Completed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T18:28:08Z",

```

```

    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "operation": "RETRIEVE",
        "connector-id": "c-fc68000012345aa18",
        "transfer-id": "file-transfer-ID",
        "file-transfer-id": "file-transfer-ID",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
        "file-path": "testfile.txt",
        "status-code": "COMPLETED",
        "local-directory-path": "/DOC-EXAMPLE-BUCKET",
        "bytes": 63533,
        "start-timestamp": "2024-01-24T18:28:07.632388Z",
        "end-timestamp": "2024-01-24T18:28:07.774898Z",
        "local-file-location": {
            "domain": "S3",
            "bucket": "DOC-EXAMPLE-BUCKET",
            "key": "testfile.txt"
        }
    }
}

```

AS2événements

Les champs de détail relatifs aux AS2 événements sont les suivants :

- AS2Réception de la charge utile terminée
- AS2Échec de réception de la charge utile
- AS2Envoi de la charge utile terminé
- AS2Échec de l'envoi de la charge utile
- AS2MDNRéception terminée
- AS2MDNÉchec de réception
- AS2MDNEnvoi terminé
- AS2MDNÉchec de l'envoi

Les detail-type champs source et sont inclus ci-dessous car ils contiennent des valeurs spécifiques pour les Transfer Family événements. Pour les définitions des autres champs de

métadonnées inclus dans tous les événements, consultez la section [Référence de la structure des événements](#) dans le guide de Amazon EventBridge l'utilisateur.

```
{
  . . . ,
  "detail-type": "string",
  "source": "aws.transfer",
  . . . ,
  "detail": {
    "s3-attributes" : {
      "file-bucket" : "string",
      "file-key" : "string",
      "json-bucket" : "string",
      "json-key" : "string",
      "mdn-bucket" : "string",
      "mdn-key" : "string"
    }
    "mdn-subject" : "string",
    "mdn-message-id" : "string",
    "disposition" : "string",
    "bytes" : "number",
    "as2-from" : "string",
    "as2-message-id" : "string",
    "as2-to" : "string",
    "connector-id" : "string",
    "client-ip" : "string",
    "agreement-id" : "string",
    "server-id" : "string",
    "requester-file-name" : "string",
    "message-subject" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "transfer-id" : "string"
  }
}
```

detail-type

Identifie le type d'événement.

Pour cet événement, la valeur est l'un des AS2 événements répertoriés précédemment.

source

Identifie le service qui a généré l'événement. Pour les Transfer Family événements, cette valeur est `aws.transfer`.

detail

JSONObjet contenant des informations sur l'événement. Le service qui génère l'événement détermine le contenu de ce champ.

s3-attributes

Identifie le compartiment Amazon S3 et la clé du fichier transféré. Pour les MDN événements, il identifie également le compartiment et la clé du MDN fichier.

file-bucket

Le conteneur de l'objet dans Amazon S3.

file-key

Le nom attribué à l'objet dans Amazon S3.

json-bucket

Pour COMPLETED ou pour FAILED les transferts, le conteneur du JSON fichier.

json-key

Pour COMPLETED ou pour les FAILED transferts, le nom attribué au JSON fichier dans Amazon S3.

mdn-bucket

Pour MDN les événements, le conteneur du MDN fichier.

mdn-key

Pour les MDN événements, le nom attribué au MDN fichier dans Amazon S3.

mdn-subject

Pour les MDN événements, une description textuelle de la disposition du message.

mdn-message-id

Pour les MDN événements, un identifiant unique pour le MDN message.

disposition

Pour les MDN événements, la catégorie correspondant à la disposition.

bytes

Le nombre d'octets contenus dans le message.

as2-from

Le partenaire AS2 commercial qui envoie le message.

as2-message-id

Identifiant unique du AS2 message transféré.

as2-to

Le partenaire AS2 commercial qui reçoit le message.

connector-id

Pour les AS2 messages envoyés depuis un serveur Transfer Family à un partenaire commercial, identifiant unique du AS2 connecteur utilisé.

client-ip

Pour les événements du serveur (transferts d'un partenaire commercial vers un serveur Transfer Family), adresse IP du client impliqué dans le transfert.

agreement-id

Pour les événements liés au serveur, identifiant unique de l'AS2accord.

server-id

Pour les événements du serveur, un identifiant unique uniquement pour le serveur Transfer Family.

requester-file-name

Pour les événements de charge utile, nom d'origine du fichier reçu lors du transfert.

message-subject

Description textuelle de l'objet du message.

start-timestamp

Pour les transferts réussis, l'horodatage du début du traitement des fichiers.

end-timestamp

Pour les transferts réussis, horodatage indiquant la fin du traitement du fichier.

status-code

Code correspondant à l'état du processus de transfert des AS2 messages. Valeurs valides :
COMPLETED | FAILED | PROCESSING.

failure-code

Pour les transferts ayant échoué, catégorie expliquant pourquoi le transfert a échoué.

failure-message

Pour les transferts ayant échoué, les détails expliquant pourquoi le transfert a échoué.

transfer-id

Identifiant unique de l'événement de transfert.

Exemple AS2Exemple d'événement Payload Receive Completed

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 Payload Receive Completed",
  "source": "aws.transfer",
  "account": "076722215406",
  "time": "2024-02-07T06:47:05Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:connector/c-1111aaaa2222bbbb3"],
  "detail": {
    "s3-attributes": {
      "file-key": "/inbound/processed/testAs2Message.dat",
      "file-bucket": "DOC-EXAMPLE-BUCKET"
    },
    "client-ip": "client-IP-address",
    "requester-file-name": "testAs2MessageVerifyFile.dat",
    "end-timestamp": "2024-02-07T06:47:06.040031Z",
    "as2-from": "as2-from-ID",
    "as2-message-id": "as2-message-ID",
    "message-subject": "Message from AS2 tests",
    "start-timestamp": "2024-02-07T06:47:05.410Z",
```

```

    "status-code": "PROCESSING",
    "bytes": 63,
    "as2-to": "as2-to-ID",
    "agreement-id": "a-1111aaaa2222bbbb3",
    "server-id": "s-1234abcd5678efghi"
  }
}

```

Exemple AS2MDNExemple d'événement d'échec de réception

```

{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 MDN Receive Failed",
  "source": "aws.transfer",
  "account": "889901007463",
  "time": "2024-02-06T22:05:09Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:server/s-1111aaaa2222bbbb3"],
  "detail": {
    "mdn-subject": "Your Requested MDN Response re: Test run from Id 123456789abcde to partner ijklmnop987654",
    "s3-attributes": {
      "json-bucket": "DOC-EXAMPLE-BUCKET1",
      "file-key": "/as2Integ/TestOutboundWrongCert.dat",
      "file-bucket": "DOC-EXAMPLE-BUCKET2",
      "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
    },
    "mdn-message-id": "MDN-message-ID",
    "end-timestamp": "2024-02-06T22:05:09.479878Z",
    "as2-from": "PartnerA",
    "as2-message-id": "as2-message-ID",
    "connector-id": "c-1234abcd5678efghj",
    "message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
    "start-timestamp": "2024-02-06T22:05:03Z",
    "failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
    "status-code": "FAILED",
    "as2-to": "MyCompany",
    "failure-message": "No public certificate matching message signature could be found in profile: p-1234abcd5678efghj",
    "transfer-id": "transfer-ID"
  }
}

```

Sécurité dans AWS Transfer Family

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 :

Pour savoir si un [programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité](#) spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de [AWS conformité Programmes AWS](#) de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#) .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Guides de démarrage rapide sur la sécurité et la conformité](#) : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- [Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services](#) : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

Note

Tous ne Services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez la [référence des services HIPAA éligibles](#).

- 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 reprennent 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](#).
- [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.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Transfer Family. Les rubriques suivantes expliquent comment procéder à la configuration AWS Transfer Family 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 AWS Transfer Family ressources.

Rubriques

- [Politiques de sécurité pour AWS Transfer Family](#)
- [Utilisation de l'échange de clés post-quantique hybride avec AWS Transfer Family](#)
- [Protection des données dans AWS Transfer Family](#)
- [Gestion des identités et des accès pour AWS Transfer Family](#)
- [Validation de conformité pour AWS Transfer Family](#)
- [Résilience dans AWS Transfer Family](#)
- [Sécurité de l'infrastructure dans AWS Transfer Family](#)
- [Ajouter un pare-feu pour applications Web](#)
- [Prévention du problème de l'adjoint confus entre services](#)
- [AWS politiques gérées pour AWS Transfer Family](#)

Politiques de sécurité pour AWS Transfer Family

Les politiques de sécurité du serveur vous AWS Transfer Family permettent de limiter l'ensemble des algorithmes cryptographiques (codes d'authentification des messages (MACs), échanges de clés (KEXs) et suites de chiffrement) associés à votre serveur. Pour obtenir la liste des algorithmes cryptographiques pris en charge, consultez [Algorithmes cryptographiques](#). Pour obtenir la liste des algorithmes clés pris en charge à utiliser avec les clés d'hôte du serveur et les clés utilisateur gérées par les services, consultez [Algorithmes pris en charge pour les clés utilisateur et serveur](#).

Note

Nous vous recommandons vivement de mettre vos serveurs à jour conformément à notre politique de sécurité la plus récente. Notre dernière politique de sécurité est celle par défaut. Tout client qui crée un serveur Transfer Family en utilisant CloudFormation et acceptant la politique de sécurité par défaut se verra automatiquement attribuer la dernière politique. Si la compatibilité des clients vous préoccupe, veuillez indiquer clairement la politique de sécurité que vous souhaitez utiliser lors de la création ou de la mise à jour d'un serveur plutôt que d'utiliser la politique par défaut, qui est sujette à modification.

Pour modifier la politique de sécurité d'un serveur, consultez [Modifier la politique de sécurité](#).

Pour plus d'informations sur la sécurité dans Transfer Family, consultez le billet de blog intitulé [Comment Transfer Family peut vous aider à créer une solution de transfert de fichiers géré sécurisée et conforme](#).

Rubriques

- [Algorithmes cryptographiques](#)
- [TransferSecurityPolicy-2024-01](#)
- [TransferSecurityPolicy-2023-05](#)
- [TransferSecurityPolicy-03](#)
- [TransferSecurityPolicy-2020-06](#)
- [TransferSecurityPolicy-2018-11](#)
- [TransferSecurityPolicy- FIPS -2024-01](#)
- [TransferSecurityPolicy- FIPS -2023-05](#)
- [TransferSecurityPolicy- FIPS -2020-06](#)

- [Politiques de sécurité post-Quantum](#)

 Note

`TransferSecurityPolicy-2024-01` est la politique de sécurité par défaut attachée à votre serveur lorsque vous créez un serveur à l'aide de la console API, ou CLI.

Algorithmes cryptographiques

Pour les clés d'hôte, nous prenons en charge les algorithmes suivants :

- `rsa-sha-256`
- `rsa-sha-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp512`
- `ssh-ed25519`

De plus, les politiques de sécurité de 2018 et 2020 le permettent `ssh-rsa`.

 Note

Il est important de comprendre la distinction entre le type de RSA clé (qui est toujours le cas) `ssh-rsa` et l'algorithme de clé RSA hôte, qui peut être n'importe lequel des algorithmes pris en charge.

Vous trouverez ci-dessous une liste des algorithmes cryptographiques pris en charge pour chaque politique de sécurité.

 Note

Dans le tableau et les politiques suivants, notez l'utilisation suivante des types d'algorithmes.

- SFTP Les serveurs n'utilisent des algorithmes que dans les `SshMac` sections `SshCiphers` `SshKexs`, et.

- FTPSles serveurs utilisent uniquement les algorithmes de la TlsCipherssection.
- FTPles serveurs, puisqu'ils n'utilisent pas de cryptage, n'utilisent aucun de ces algorithmes.

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
SshCiphers								
aes128-CTR	◆			◆	◆		◆	◆
aes128-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
aes192-ctr	◆	◆	◆	◆	◆	◆	◆	◆
aes256-ctr	◆	◆	◆	◆	◆	◆	◆	◆
aes256-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
chacha20-poly1305@openssh.com				◆				◆
SshKexs								

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
curve25519-sha256	◆	◆	◆					◆
curve25519-sha256@libssh.org	◆	◆	◆					◆
diffie-hellman-group14-sha1								◆
diffie-hellman-group14-sha256				◆			◆	◆
diffie-hellman-group16-sha-512	◆	◆	◆	◆	◆	◆	◆	◆
diffie-hellman-group18-sha512	◆	◆	◆	◆	◆	◆	◆	◆

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
diffie-hellman-group-exchange-sha256		◆	◆	◆		◆	◆	◆
ecdh-nist-p256-kurve-512r3-sha256-d00@openquantumsafe.org	◆				◆			
ecdh-nist-p384-kurve-768r3-sha384-d00@openquantumsafe.org	◆				◆			

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org	◆				◆			
ecdh-sha2-nistp255	◆			◆	◆		◆	◆
ecdh-sha2-nistp384	◆			◆	◆		◆	◆
ecdh-sha2-nistp521	◆			◆	◆		◆	◆
x25519-kyber-512r3-sha256-d00@amazon.com	◆							
SshMacs								

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
hmac-sha1								◆
hmac-sha1-etm@openssh.com								◆
hmac-sha2-256			◆	◆			◆	◆
hmac-sha2-256-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
hmac-sha2-512			◆	◆			◆	◆
hmac-sha2-512-etm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆
umac-128-etm@openssh.com				◆				◆

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
umac-128@openssh.com				◆				◆
umac-64-etm@openssh.com								◆
umac-64@openssh.com								◆
TlsCiphers								
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆
-- ECDSA WITH _AES CBC _128_ _SHA256								
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆
-- ECDSA WITH _AES GCM _128_ _SHA256								

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆
ECDSA								
WITH								
_AES								
CBC								
256								
SHA384								
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆
ECDSA								
WITH								
_AES								
GCM								
256								
SHA384								
TLS_ECDHE	◆	◆	◆	◆	◆	◆	◆	◆
_RSA								
WITH								
_AES								
CBC								
128								
SHA256								

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
TLS_ECDHE_RSA_WITH_AES_GCM_128_SHA256	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_CBC_256_SHA384	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_GCM_256_SHA384	◆	◆	◆	◆	◆	◆	◆	◆

Politique de sécurité	2024-01	2023-05	05.03	2020-06	FIPS-2024-01	FIPS-2023-05	FIPS-2020-06	2018-11
TLS_								◆
_RSA								
WITH								
_AES								
CBC								
128								
SHA256								
TLS_								◆
_RSA								
WITH								
_AES								
CBC								
256								
SHA256								

TransferSecurityPolicy-2024-01

Voici la politique de sécurité TransferSecurityPolicy -2024-01.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "x25519-kyber-512r3-sha256-d00@amazon.com",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
    ]
  }
}
```

```

        "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
        "ecdh-sha2-nistp256",
        "ecdh-sha2-nistp384",
        "ecdh-sha2-nistp521",
        "curve25519-sha256",
        "curve25519-sha256@libssh.org",
        "diffie-hellman-group18-sha512",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-256-etm@openssh.com",
        "hmac-sha2-512-etm@openssh.com"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-2023-05

Voici la politique de sécurité TransferSecurityPolicy -2023-05.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",

```

```

        "curve25519-sha256@libssh.org",
        "diffie-hellman-group16-sha512",
        "diffie-hellman-group18-sha512",
        "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-03

Ce qui suit montre la politique de sécurité TransferSecurityPolicy -03.03.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
  },
}

```

```

    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}

```

TransferSecurityPolicy-2020-06

Voici la politique de sécurité TransferSecurityPolicy -2020-06.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com",
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ]
  }
}

```

```

    ],
    "SshMacs": [
        "umac-128-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com",
        "hmac-sha2-512-etm@openssh.com",
        "umac-128@openssh.com",
        "hmac-sha2-256",
        "hmac-sha2-512"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy-2018-11

Voici la politique de sécurité TransferSecurityPolicy -2018-11.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
        "chacha20-poly1305@openssh.com",
        "aes128-ctr",
        "aes192-ctr",
        "aes256-ctr",
        "aes128-gcm@openssh.com",
        "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
        "curve25519-sha256",
        "curve25519-sha256@libssh.org",
        "ecdh-sha2-nistp256",
        "ecdh-sha2-nistp384",

```



```

    "ecdh-sha2-nistp521",
    "diffie-hellman-group-exchange-sha256",
    "diffie-hellman-group16-sha512",
    "diffie-hellman-group18-sha512",
    "diffie-hellman-group14-sha256",
    "diffie-hellman-group14-sha1"
  ],
  "SshMacs": [
    "umac-64-etm@openssh.com",
    "umac-128-etm@openssh.com",
    "hmac-sha2-256-etm@openssh.com",
    "hmac-sha2-512-etm@openssh.com",
    "hmac-sha1-etm@openssh.com",
    "umac-64@openssh.com",
    "umac-128@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512",
    "hmac-sha1"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_RSA_WITH_AES_256_CBC_SHA256"
  ]
}
}

```

TransferSecurityPolicy- FIPS -2024-01

Ce qui suit montre la politique de TransferSecurityPolicy sécurité - FIPS -2024-01.

Note

Le point FIPS de terminaison du service et la politique de sécurité TransferSecurityPolicy - FIPS -2024-01 ne sont disponibles que dans certaines régions. AWS Pour plus

d'informations, consultez [Points de terminaison et quotas AWS Transfer Family](#) dans le document Références générales AWS.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
      "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

TransferSecurityPolicy- FIPS -2023-05

Les détails de la FIPS AWS Transfer Family certification sont disponibles sur <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Ce qui suit montre la politique de TransferSecurityPolicy sécurité - FIPS -2023-05.

Note

Le point FIPS de terminaison du service et la politique de sécurité TransferSecurityPolicy - FIPS -2023-05 ne sont disponibles que dans certaines régions. AWS Pour plus d'informations, consultez [Points de terminaison et quotas AWS Transfer Family](#) dans le document Références générales AWS.

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
```

```

        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}

```

TransferSecurityPolicy- FIPS -2020-06

Les détails de la FIPS AWS Transfer Family certification sont disponibles sur <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Ce qui suit montre la politique de TransferSecurityPolicy sécurité - FIPS -2020-06.

Note

Le point FIPS de terminaison du service et la politique de sécurité TransferSecurityPolicy - FIPS -2020-06 ne sont disponibles que dans certaines régions. AWS Pour plus d'informations, consultez [Points de terminaison et quotas AWS Transfer Family](#) dans le document Références générales AWS.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2020-06",
    "SshCiphers": [
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",

```

```
    "hmac-sha2-512-etm@openssh.com",
    "hmac-sha2-256",
    "hmac-sha2-512"
  ],
  "TlsCiphers": [
    "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
    "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
  ]
}
```

Politiques de sécurité post-Quantum

Ce tableau répertorie les algorithmes utilisés pour les politiques de sécurité post-quantique de Transfer Family. Ces politiques sont décrites en détail dans [Utilisation de l'échange de clés post-quantique hybride avec AWS Transfer Family](#).

Les listes de politiques suivent le tableau.

Politique de sécurité	TransferSecurityPolicy-PQ- - Expérimental-2023-04 SSH	TransferSecurityPolicy-PQ- SSH - -Expérimental-2023-04 FIPS
SSH ciphers		
aes128-CTR		◆
aes128-gcm@openssh.com	◆	◆
aes192-ctr	◆	◆
aes256-ctr	◆	◆
aes256-gcm@openssh.com	◆	◆
KEXs		

Politique de sécurité	TransferSecurityPolicy-PQ- - Expérimental-2023-04 SSH	TransferSecurityPolicy-PQ- SSH - -Expérimental-2023-04 FIPS
ecdh-nistp256-kyber-512r3- sha256-d00@openquan tumsafe.org	◆	◆
ecdh-nistp384-kyber-768r3- sha384-d00@openquan tumsafe.org	◆	◆
ecdh-nistp521-kyber-1024r3- sha512-d00@openqua ntumsafe.org	◆	◆
x25519-kyber-512r3-sha256-d 00@amazon.com	◆	
diffie-hellman-group14-sha256		◆
diffie-hellman-group16 sha-512	◆	◆
diffie-hellman-group18-sha512	◆	◆
ecdh-sha2-nistp384		◆
ecdh-sha2-nistp521		◆
diffie-hellman-group-exchan ge-sha256	◆	◆
ecdh-sha2-nistp255		◆
curve25519-sha256@libssh.or g	◆	
curve25519-sha256	◆	

Politique de sécurité	TransferSecurityPolicy-PQ- - Expérimental-2023-04 SSH	TransferSecurityPolicy-PQ- SSH - -Expérimental-2023-04 FIPS
MACs		
hmac-sha2-256-etm@ openssh.com	◆	◆
hmac-sha2-256	◆	◆
hmac-sha2-512-etm@ openssh.com	◆	◆
hmac-sha2-512	◆	◆
TLS ciphers		
TLS_ ECDHE __ ECDSA WITH _ AES CBC _128__ SHA256	◆	◆
TLS_ ECDHE __ ECDSA WITH _ AES GCM _128__ SHA256	◆	◆
TLS_ ECDHE __ ECDSA WITH _ AES CBC _256__ SHA384	◆	◆
TLS_ ECDHE __ ECDSA WITH _ AES GCM _256__ SHA384	◆	◆
TLS_ ECDHE __ RSA WITH _ AES CBC _128__ SHA256	◆	◆
TLS_ ECDHE __ RSA WITH _ AES GCM _128__ SHA256	◆	◆

Politique de sécurité	TransferSecurityPolicy-PQ- - Expérimental-2023-04 SSH	TransferSecurityPolicy-PQ- SSH - -Expérimental-2023-04 FIPS
TLS_ ECDHE __ RSA WITH _ AES CBC _256__ SHA384	◆	◆
TLS_ ECDHE __ RSA WITH _ AES GCM _256__ SHA384	◆	◆

TransferSecurityPolicy-PQ- -Expérimental-2023-04 SSH

Voici la politique de sécurité TransferSecurityPolicy-PQ-SSH-Experimental -2023-04.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-Experimental-2023-04",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "x25519-kyber-512r3-sha256-d00@amazon.com",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
      "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ]
  },
}
```



```

    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}

```

TransferSecurityPolicy-PQ- SSH - -Expérimental-2023-04 FIPS

Ce qui suit montre la politique de sécurité TransferSecurityPolicy-PQ-SSH-FIPS - Experimental-2023-04.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-PQ-SSH-FIPS-
Experimental-2023-04",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org",
      "ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org",
      "ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [

```

```
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com",
        "hmac-sha2-512",
        "hmac-sha2-256"
    ],
    "TlsCiphers": [
        "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
        "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
}
}
```

Utilisation de l'échange de clés post-quantique hybride avec AWS Transfer Family

AWS Transfer Family prend en charge une option hybride d'établissement de clé post-quantique pour le protocole Secure Shell (SSH). L'établissement d'une clé post-quantique est nécessaire car il est déjà possible d'enregistrer le trafic réseau et de le sauvegarder pour le déchiffrer à l'avenir par un ordinateur quantique, ce que l'on appelle une *store-now-harvest-later* attaque.

Vous pouvez utiliser cette option lorsque vous vous connectez à Transfer Family pour des transferts de fichiers sécurisés vers et depuis le stockage Amazon Simple Storage Service (Amazon S3) ou Amazon Elastic File System (Amazon EFS). L'établissement de clés hybrides post-quantiques SSH introduit des mécanismes d'établissement de clés post-quantiques, qu'il utilise conjointement avec des algorithmes d'échange de clés classiques. SSH les clés créées à l'aide de suites de chiffrement classiques sont protégées contre les attaques par force brute grâce à la technologie actuelle. Cependant, le chiffrement classique ne devrait pas rester sécurisé après l'émergence de l'informatique quantique à grande échelle dans le futur.

Si votre organisation compte sur la confidentialité à long terme des données transmises via une connexion Transfer Family, vous devez envisager de passer à la cryptographie post-quantique avant que des ordinateurs quantiques à grande échelle ne soient disponibles.

Afin de protéger les données chiffrées aujourd'hui contre d'éventuelles attaques futures, AWS participe avec la communauté cryptographique au développement d'algorithmes résistants aux quanta ou post-quantiques. Nous avons mis en œuvre des suites de chiffrement hybrides par échange de clés post-quantiques dans Transfer Family qui combinent des éléments classiques et post-quantiques.

Ces suites de chiffrement hybrides peuvent être utilisées sur vos charges de travail de production dans la plupart AWS des régions. Cependant, étant donné que les caractéristiques de performance et les exigences en bande passante des suites de chiffrement hybrides sont différentes de celles des mécanismes d'échange de clés classiques, nous vous recommandons de les tester sur vos connexions Transfer Family.

Pour en savoir plus sur la cryptographie post-quantique, consultez le billet de blog sur la [sécurité post-quantique](#).

Table des matières

- [À propos de l'échange de clés hybrides post-quantiques dans SSH](#)
- [Comment fonctionne l'établissement de clés hybrides post-quantiques dans Transfer Family](#)
 - [Pourquoi Kyber ?](#)
 - [Échange de SSH clés hybrides post-quantiques et exigences cryptographiques \(140\) FIPS](#)
- [Test de l'échange de clés hybride post-quantique dans Transfer Family](#)
 - [Activez l'échange de clés hybrides post-quantiques sur votre terminal SFTP](#)
 - [Configurer un SFTP client qui prend en charge l'échange de clés hybrides post-quantiques](#)
 - [Confirmez l'échange de clés hybrides post-quantiques dans SFTP](#)

À propos de l'échange de clés hybrides post-quantiques dans SSH

[Transfer Family prend en charge les suites de chiffrement hybrides post-quantiques par échange de clés](#), qui utilisent à la fois l'algorithme classique d'échange de clés Elliptic Curve Diffie-Hellman (ECDH) et Kyber. [CRYSTALS Kyber](#) est un algorithme de chiffrement à clé publique post-quantique et d'établissement de clés que le [National Institute for Standards and Technology \(NIST\)](#) a désigné comme son premier algorithme standard d'accord de clé post-quantique.

Le client et le serveur procèdent toujours à un échange de ECDH clés. De plus, le serveur encapsule un secret partagé post-quantique dans la clé KEM publique post-quantique du client, qui est annoncée dans le message d'échange de clés du SSH client. Cette stratégie combine la haute

assurance d'un échange de clés classique avec la sécurité des échanges de clés post-quantiques proposés, afin de garantir que les poignées de main sont protégées tant que le secret partagé ECDH ou le secret partagé post-quantique ne peut pas être brisé.

Comment fonctionne l'établissement de clés hybrides post-quantiques dans Transfer Family

AWS a récemment annoncé la prise en charge de l'échange de clés post-quantiques lors des transferts de SFTP fichiers dans AWS Transfer Family. Transfer Family adapte en toute sécurité les transferts de business-to-business fichiers vers les services AWS de stockage à SFTP l'aide d'autres protocoles. SFTPe est une version plus sécurisée du protocole de transfert de fichiers (FTP) qui s'exécute sur SSH. La prise en charge de l'échange de clés post-quantique de Transfer Family élève la barre de sécurité pour les transferts de SFTP données.

La SFTP prise en charge de l'échange de clés hybride post-quantique dans Transfer Family inclut la combinaison des algorithmes post-quantiques Kyber-512, Kyber-768 et Kyber-1024, avec ECDH plus de courbes P256, P384, P521 ou Curve25519. Les méthodes d'échange de SSH clés correspondantes suivantes sont spécifiées dans [le projet d'échange de SSH clés hybride post-quantique](#).

- `ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org`
- `ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org`
- `ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org`
- `x25519-kyber-512r3-sha256-d00@amazon.com`

Note

Ces nouvelles méthodes d'échange de clés peuvent changer au fur et à mesure que le projet évolue vers la standardisation ou lorsqu'il NIST ratifie l'algorithme de Kyber.

Pourquoi Kyber ?

AWS s'engage à soutenir des algorithmes standardisés et interopérables. Kyber est le premier algorithme de chiffrement post-quantique sélectionné pour la standardisation par le projet [NIST Post-Quantum Cryptography](#). Certains organismes de normalisation intègrent déjà Kyber dans leurs protocoles. AWS prend déjà en charge Kyber TLS dans certains points de AWS API terminaison.

Dans le cadre de cet engagement, AWS a soumis un projet de proposition à la cryptographie post-quantique qui combine Kyber avec des courbes NIST approuvées, comme P256 IETF pour. SSH Afin de renforcer la sécurité de nos clients, la AWS mise en œuvre de l'échange de clés post-quantique figure dans SFTP et SSH suit ce projet. Nous prévoyons de prendre en charge les futures mises à jour jusqu'à ce que notre proposition soit adoptée par le IETF et devienne une norme.

Les nouvelles méthodes d'échange de clés (répertoriées dans la section [Comment fonctionne l'établissement de clés hybrides post-quantiques dans Transfer Family](#)) peuvent changer au fur et à mesure que le projet évolue vers la standardisation ou lors de la NIST ratification de l'algorithme de Kyber.

Note

La prise en charge des algorithmes post-quantiques est actuellement disponible pour l'échange de clés hybrides post-quantiques dans TLS for AWS KMS (voir [Utilisation d'un algorithme post-quantique hybride TLS avec AWS KMS](#)) et les points de AWS Certificate Manager terminaison. AWS Secrets Manager API

Échange de SSH clés hybrides post-quantiques et exigences cryptographiques (140) FIPS

Pour les clients qui ont besoin de FIPS conformité, Transfer Family fournit une cryptographie FIPS approuvée en SSH utilisant la bibliothèque cryptographique open source AWS FIPS certifiée 140, -LC. AWS Les méthodes d'échange de clés hybrides post-quantiques prises en charge dans le document TransferSecurityPolicy-PQ-SSH-FIPS -Experimental-2023-04 de Transfer FIPS Family sont approuvées [NISTconformément au SP 800-56Cr2 \(section 2\)](#). L'Office fédéral allemand de la sécurité de l'information ([BSI](#)) et l'Agence nationale de la sécurité des systèmes d'information ([ANSSI](#)) de France recommandent également de telles méthodes d'échange de clés hybrides post-quantiques.

Test de l'échange de clés hybride post-quantique dans Transfer Family

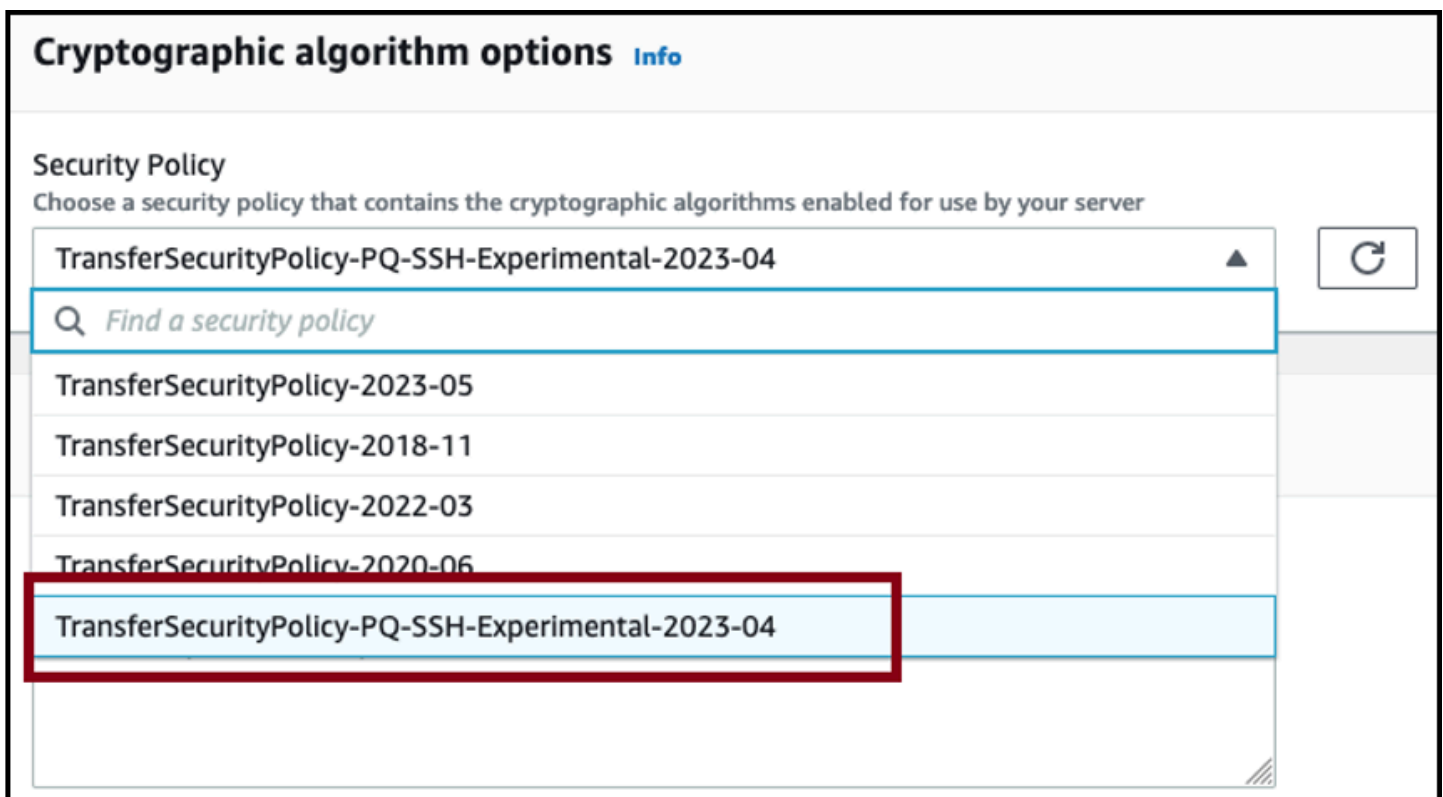
Cette section décrit les étapes à suivre pour tester l'échange de clés hybride post-quantique.

1. [Activez l'échange de clés hybrides post-quantiques sur votre terminal SFTP.](#)

2. Utilisez un SFTP client (tel que [Configurer un SFTP client qui prend en charge l'échange de clés hybrides post-quantiques](#)) qui prend en charge l'échange de clés hybrides post-quantiques en suivant les instructions du projet de spécification susmentionné.
3. Transférez un fichier à l'aide d'un serveur Transfer Family.
4. [Confirmez l'échange de clés hybrides post-quantiques dans SFTP](#).

Activez l'échange de clés hybrides post-quantiques sur votre terminal SFTP

Vous pouvez choisir la SSH politique lorsque vous créez un nouveau point de terminaison de SFTP serveur dans Transfer Family ou en modifiant les options de l'algorithme cryptographique dans un point de SFTP terminaison existant. L'instantané suivant montre un exemple de l' AWS Management Console endroit où vous mettez à jour la SSH politique.



Les noms de SSH politique qui prennent en charge l'échange de clés post-quantique sont TransferSecurityPolicy-PQ- -Experimental-2023-04 et -PQ- - SSH -Experimental-2023-04. TransferSecurityPolicy SSH FIPS Pour plus de détails sur les politiques de Transfer Family, consultez [Politiques de sécurité pour AWS Transfer Family](#).

Configurer un SFTP client qui prend en charge l'échange de clés hybrides post-quantiques

Après avoir sélectionné la bonne SSH politique post-quantique dans votre terminal SFTP Transfer Family, vous pouvez expérimenter la politique post-quantique SFTP dans Transfer Family. Vous pouvez utiliser un SFTP client (tel qu'[OQSOpen SSH](#)) qui prend en charge l'échange de clés hybrides post-quantiques en suivant les instructions du projet de spécification susmentionné.

OQSOpen SSH est un fork open source d'Open SSH qui ajoute une cryptographie sécurisée quantique en utilisant. SSH `liboqs` `liboqs` est une bibliothèque C open source qui implémente des algorithmes cryptographiques résistants aux quanta. OQS Ouvrez SSH et `liboqs` faites partie du projet Open Quantum Safe (OQS).

Pour tester l'échange de clés hybrides post-quantiques dans Transfer Family SFTP with OQS OpenSSH, vous devez créer OQS Open SSH comme expliqué dans le document du [README](#) projet. Après avoir créé OQS OpenSSH, vous pouvez exécuter l'exemple de SFTP client pour vous connecter à votre SFTP point de terminaison (par exemple, `s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`) en utilisant les méthodes d'échange de clés hybrides post-quantiques, comme indiqué dans la commande suivante.

```
./sftp -S ./ssh -v -o \
  KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org \
  -i username_private_key_PEM_file \
  username@server-id.server.transfer.region-id.amazonaws.com
```

Dans la commande précédente, remplacez les éléments suivants par vos propres informations :

- Remplacez *username_private_key_PEM_file* avec le fichier PEM codé par clé privée de l'utilisateur
- Remplacez *username* avec le nom SFTP d'utilisateur
- Remplacez *server-id* avec l'ID du serveur Transfer Family
- Remplacez *region-id* avec la région dans laquelle se trouve réellement votre serveur Transfer Family

Confirmez l'échange de clés hybrides post-quantiques dans SFTP

Pour vérifier que l'échange de clés hybride post-quantique a été utilisé lors d'une SSH connexion SFTP à Transfer Family, vérifiez la sortie du client. Vous pouvez éventuellement utiliser un programme de capture de paquets. Si vous utilisez le SSH client Open Quantum Safe Open, le résultat doit ressembler à ce qui suit (en omettant les informations non pertinentes par souci de concision) :

```
$. /sftp -S ./ssh -v -o KexAlgorithms=ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
OpenSSH_8.9-2022-01_p1, Open Quantum Safe 2022-08, OpenSSL 3.0.2 15 Mar 2022
debug1: Reading configuration data /home/lab/openssh/oqs-test/tmp/ssh_config
debug1: Authenticator provider $SSH_SK_PROVIDER did not resolve; disabling
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com [xx.yy.zz..12] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_8.9-2022-01_
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com:22 as 'username'
debug1: load_hostkeys: fopen /home/lab/.ssh/known_hosts2: No such file or directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes192-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes192-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649
[...]
debug1: rekey out after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 4294967296 blocks
```



```
[...]
Authenticated to AWS.Transfer.PQ.SFTP.test-endpoint.aws.com ([xx.yy.zz..12]:22) using
"publickey".s
debug1: channel 0: new [client-session]
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

Le résultat montre que la négociation avec le client a eu lieu à l'aide de la `ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org` méthode hybride post-quantique et qu'une SFTP session a été établie avec succès.

Protection des données dans AWS Transfer Family

Le [modèle de responsabilité AWS partagée](#) s'applique à la protection des données dans AWS Transfer Family (Transfer Family). Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble du AWS cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour les AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez la section [Confidentialité des données FAQ](#). Pour plus d'informations sur la protection des données en Europe, consultez le [modèle de responsabilité AWS partagée et](#) le billet de GDPR blog sur le blog sur la AWS sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification du AWS compte et de configurer des comptes utilisateur individuels avec AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- Utilisez SSL/TLS pour communiquer avec les AWS ressources. Nous soutenons la TLS version 1.2.
- Configuration API et journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données personnelles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 2 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou un API, utilisez un point de terminaison. FIPS Pour plus

d'informations sur les FIPS points de terminaison disponibles, consultez la [norme fédérale de traitement de l'information \(FIPS\) 140-2](#).

Nous vous recommandons vivement de ne jamais placer d'informations identifiables sensibles, telles que les numéros de compte de vos clients, dans des champs de formulaire comme Nom. Cela inclut lorsque vous travaillez avec Transfer Family ou d'autres AWS services à l'aide de la console API, AWS CLI, ou AWS SDKs. Toutes les données de configuration que vous entrez dans la configuration du service Transfer Family, ou dans les configurations d'autres services, peuvent être récupérées pour être incluses dans les journaux de diagnostic. Lorsque vous fournissez un URL à un serveur externe, n'incluez pas d'informations d'identification dans le URL pour valider votre demande auprès de ce serveur.

En revanche, les données issues des opérations de chargement et de téléchargement vers et depuis les serveurs de Transfer Family sont traitées comme totalement privées et n'existent jamais en dehors des canaux cryptés, tels qu'une SFTP connexion OR. FTPS Ces données ne sont toujours accessibles qu'aux personnes autorisées.

Rubriques

- [Chiffrement des données dans Amazon S3](#)
- [Gestion des clés](#)

Chiffrement des données dans Amazon S3

AWS Transfer Family utilise les options de chiffrement par défaut que vous avez définies pour votre compartiment Amazon S3 afin de chiffrer vos données. Lorsque vous activez le chiffrement par défaut sur un compartiment, tous les objets sont chiffrés au moment d'être stockés dans le compartiment. Les objets sont chiffrés à l'aide du chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3) ou des clés gérées AWS Key Management Service (-AWS KMS). SSE KMS Pour plus d'informations sur le chiffrement côté serveur, consultez la section [Protection des données à l'aide du chiffrement côté serveur dans](#) le guide de l'utilisateur d'Amazon Simple Storage Service.

Les étapes suivantes vous montrent comment chiffrer des données. AWS Transfer Family

Pour autoriser le chiffrement dans AWS Transfer Family

1. Activez le chiffrement par défaut pour votre compartiment Amazon S3. Pour obtenir des instructions, consultez le [chiffrement par défaut d'Amazon S3 pour les compartiments S3](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.
2. Mettez à jour la politique de rôle AWS Identity and Access Management (IAM) attachée à l'utilisateur pour accorder les autorisations requises AWS Key Management Service (AWS KMS).
3. Si vous utilisez une stratégie de session pour l'utilisateur, celle-ci doit accorder les AWS KMS autorisations requises.

L'exemple suivant montre une IAM politique qui accorde les autorisations minimales requises lors de l'utilisation AWS Transfer Family d'un compartiment Amazon S3 activé pour AWS KMS le chiffrement. Incluez cet exemple de politique à la fois dans la stratégie de IAM rôle d'utilisateur et dans la stratégie de session, si vous en utilisez une.

```
{
  "Sid": "Stmt1544140969635",
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt",
    "kms:GenerateDataKey"
  ],
  "Effect": "Allow",
  "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

Note

L'ID de KMS clé que vous spécifiez dans cette politique doit être le même que celui spécifié pour le chiffrement par défaut à l'étape 1.

Root, ou le IAM rôle utilisé pour l'utilisateur, doit être autorisé dans la politique AWS KMS clé.

Pour plus d'informations sur la politique AWS KMS clé, consultez la section [Utilisation des politiques clés AWS KMS dans](#) le Guide du AWS Key Management Service développeur.

Gestion des clés

Dans cette section, vous trouverez des informations sur SSH les clés, notamment sur la façon de les générer et de les faire pivoter. Pour en savoir plus sur l'utilisation de Transfer Family with AWS Lambda pour gérer les clés, consultez le billet de blog [Enabling user self-service key management with A AWS Transfer Family and AWS Lambda](#).

Note

AWS Transfer Family accepte RSAECDSA, et ED25519 clés.

Cette section explique également comment générer et gérer les clés Pretty Good Privacy (PGP).

Rubriques

- [Algorithmes pris en charge pour les clés utilisateur et serveur](#)
- [Génération de SSH clés pour les utilisateurs gérés par des services](#)
- [Faire pivoter SSH les touches](#)
- [Génération et gestion PGP des clés](#)
- [PGPClients pris en charge](#)

Algorithmes pris en charge pour les clés utilisateur et serveur

Les algorithmes clés suivants sont pris en charge pour les paires de clés utilisateur et serveur qu'elles contiennent. AWS Transfer Family

Note

Pour les algorithmes à utiliser avec le PGP déchiffrement dans les flux de travail, voir [Algorithmes pris en charge pour les paires de PGP clés](#).

- Pour ED25519 : `ssh-ed25519`
- Pour RSA :
 - `rsa-sha2-256`

- `rsa-sha2-512`
- Pour ECDSA :
 - `ecdsa-sha2-nistp256`
 - `ecdsa-sha2-nistp384`
 - `ecdsa-sha2-nistp521`

 Note

Nous prenons `ssh-rsa` en SHA1 charge nos anciennes politiques de sécurité. Pour plus de détails, consultez [Algorithmes cryptographiques](#).

Génération de SSH clés pour les utilisateurs gérés par des services

Vous pouvez configurer votre serveur pour authentifier les utilisateurs à l'aide de la méthode d'authentification gérée par le service, dans laquelle les noms d'utilisateur et SSH les clés sont stockés dans le service. La SSH clé publique de l'utilisateur est téléchargée sur le serveur en tant que propriété de l'utilisateur. Cette clé est utilisée par le serveur dans le cadre d'un processus d'authentification standard basé sur des clés. Chaque utilisateur peut avoir plusieurs SSH clés publiques enregistrées sur un serveur individuel. Pour connaître les limites du nombre de clés pouvant être stockées par utilisateur, voir les [AWS Transfer Family points de terminaison et les quotas](#) dans le Référence générale d'Amazon Web Services.

Comme alternative à la méthode d'authentification gérée par le service, vous pouvez authentifier les utilisateurs à l'aide d'un fournisseur d'identité personnalisé, ou AWS Directory Service for Microsoft Active Directory. Pour plus d'informations, consultez [Travailler avec des fournisseurs d'identité personnalisés](#) ou [Utilisation du fournisseur d'identité du AWS Directory Service](#).

Un serveur ne peut authentifier les utilisateurs qu'à l'aide d'une seule méthode (service géré, service d'annuaire ou fournisseur d'identité personnalisé), et cette méthode ne peut pas être modifiée une fois le serveur créé.

Rubriques

- [Création de SSH clés sous macOS, Linux ou Unix](#)
- [Création de SSH clés sous Microsoft Windows](#)
- [Convertir une clé SSH2 publique au PEM format](#)

Création de SSH clés sous macOS, Linux ou Unix

Sur les systèmes d'exploitation macOS, Linux ou Unix, vous utilisez la `ssh-keygen` commande pour créer une clé SSH publique et une clé SSH privée, également appelées paire de clés.

Pour créer des SSH clés sur un système d'exploitation macOS, Linux ou Unix

1. Sur les systèmes d'exploitation macOS, Linux ou Unix, ouvrez un terminal de commande.
2. AWS Transfer Family accepte les RSA clés ED25519 formatées en ECDSA -, - et -. Choisissez la commande appropriée en fonction du type de paire de clés que vous générez.

Note

Dans les exemples suivants, nous n'indiquons pas de phrase secrète : dans ce cas, l'outil vous demande de saisir votre mot de passe, puis de le répéter pour vérifier. La création d'une phrase secrète permet de mieux protéger votre clé privée et peut également améliorer la sécurité globale du système. Vous ne pouvez pas récupérer votre mot de passe : si vous l'oubliez, vous devez créer une nouvelle clé. Toutefois, si vous générez une clé d'hôte de serveur, vous devez spécifier une phrase secrète vide, en spécifiant l'-N ""option dans la commande (ou en appuyant **Enter** deux fois lorsque vous y êtes invité), car les serveurs Transfer Family ne peuvent pas demander de mot de passe au démarrage.

- Pour générer une RSA paire de clés de 4 096 bits :

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Pour générer une paire de clés ECDSA de 521 bits (ECDSA dont les tailles de bits sont de 256, 384 et 521) :

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Pour générer une paire de ED25519 clés :

```
ssh-keygen -t ed25519 -f key_name
```

Note

key_name est le nom du fichier de paires de SSH clés.

Voici un exemple de ssh-keygen sortie.

```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.

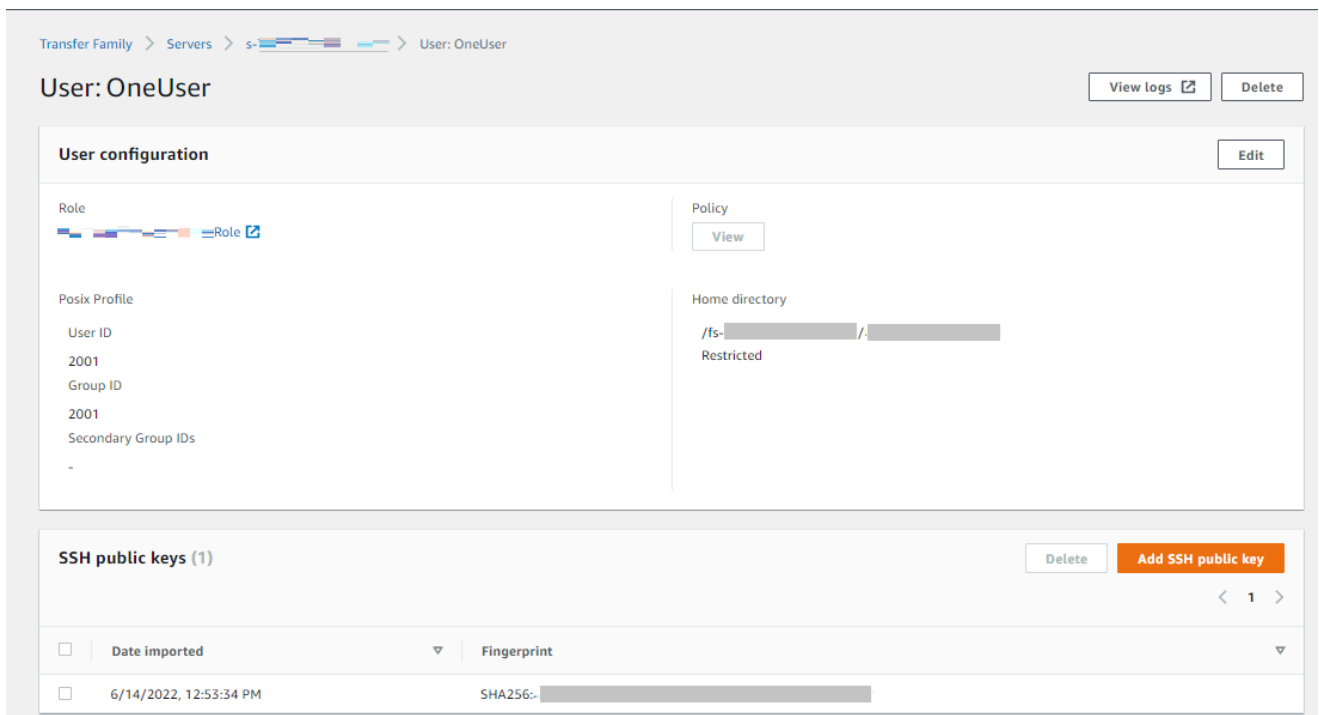
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVW0GW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]-----+
|  . ....E          |
|  .  = ...         |
| . . . = ..o       |
|  . o +  oo =      |
|  + =  .S.= *      |
|  . o o ..B + o    |
|    .o+.* .        |
|    =o**+.         |
|    ..*o*+.        |
+-----[SHA256]-----+
```

Note

Lorsque vous exécutez la commande ssh-keygen telle qu'elle est présentée ci-dessus, elle crée les clés publique et privée sous forme de fichiers dans le répertoire actuel.

Votre paire de SSH clés est maintenant prête à être utilisée. Suivez les étapes 3 et 4 pour enregistrer la clé SSH publique pour les utilisateurs gérés par le service. Ces utilisateurs utilisent les clés lorsqu'ils transfèrent des fichiers sur les terminaux du serveur Transfer Family.

3. Accédez au *key_name* .pub fichier et ouvrez-le.
4. Copiez le texte et collez-le dans la clé SSH publique pour l'utilisateur géré par le service.
 - a. Ouvrez la AWS Transfer Family console sur <https://console.aws.amazon.com/transfer/>, puis sélectionnez Serveurs dans le volet de navigation.
 - b. Sur la page Serveurs, sélectionnez l'ID du serveur qui contient l'utilisateur que vous souhaitez mettre à jour.
 - c. Sélectionnez l'utilisateur pour lequel vous ajoutez une clé publique.
 - d. Dans le volet des clés SSH publiques, choisissez Ajouter une clé SSH publique.



- e. Collez le texte de la clé publique que vous avez générée dans la zone de texte de la clé SSH publique, puis choisissez Ajouter une clé.

Transfer Family > Servers > s- > OneUser > Add key

Add key

SSH public keys

SSH public key [Info](#)
Paste the contents of SSH public key

Enter SSH public key

Cancel Add key

La nouvelle clé est répertoriée dans le volet SSH des clés publiques.

SSH public keys (2)			Delete	Add SSH public key
			< 1 >	
☐	Date imported	Fingerprint		
☐	6/14/2022, 12:53:34 PM	SHA256:-		
☐	10/20/2022, 4:26:51 PM	SHA256:-		

Création de SSH clés sous Microsoft Windows

Windows utilise un format de paire de SSH clés légèrement différent. La clé publique doit être au format PUB et la clé privée au format PPK. Sous Windows, vous pouvez utiliser P uTTYgen pour créer une paire de SSH clés dans les formats appropriés. Vous pouvez également utiliser P uTTYgen pour convertir une clé privée générée ssh-keygen à l'aide d'un .ppk fichier.

Note

Si vous présentez SCP à Win un fichier de clé privée non .ppk formaté, ce client propose de convertir la clé en .ppk format pour vous.

Pour un didacticiel sur la création de SSH clés à l'aide de P uTTYgen sous Windows, consultez le [site Web SSH .com](https://www.webssh.com/).

Convertir une clé SSH2 publique au PEM format

AWS Transfer Family accepte uniquement les clés publiques PEM formatées. Si vous avez une clé SSH2 publique, vous devez la convertir. Le format d'une clé SSH2 publique est le suivant :

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----
```

Le format d'une clé PEM publique est le suivant :

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

Exécutez la commande suivante pour convertir une clé publique SSH2 formatée en clé publique PEM formatée. Remplacez *ssh2-key* avec le nom de votre SSH2 clé, et *PEM-key* avec le nom de votre PEM clé.

```
ssh-keygen -i -f ssh2-key.pub > PEM-key.pub
```

Faire pivoter SSH les touches

Pour des raisons de sécurité, nous recommandons la meilleure pratique qui consiste à faire pivoter vos SSH clés. Généralement, cette rotation est spécifiée dans le cadre d'une politique de sécurité et est mise en œuvre de manière automatisée. Selon le niveau de sécurité, pour une communication très sensible, une paire de SSH clés peut être utilisée une seule fois. Cela élimine les risques liés au stockage des clés. Cependant, il est beaucoup plus courant de stocker les SSH informations d'identification pendant un certain temps et de définir un intervalle qui n'impose pas une charge excessive aux utilisateurs. Cette période est souvent de trois mois.

Deux méthodes sont utilisées pour effectuer la rotation des SSH touches :

- Sur la console, vous pouvez télécharger une nouvelle clé SSH publique et supprimer une clé SSH publique existante.
- À l'aide de API, vous pouvez mettre [DeleteSshPublicKey](#) API à jour les utilisateurs existants en utilisant la clé publique Secure Shell (SSH) d'un utilisateur et en ajoutant une nouvelle clé publique Secure Shell (SSH) au compte de l'utilisateur. [ImportSshPublicKey](#) API

Console

Pour effectuer une rotation des touches dans la console

1. Ouvrez la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.
2. Accédez à la page Serveurs.
3. Choisissez l'identifiant dans la colonne ID du serveur pour afficher la page de détails du serveur.
4. Sous Utilisateurs, cochez la case de l'utilisateur dont vous souhaitez faire pivoter la clé SSH publique, puis choisissez Actions, puis choisissez Ajouter une clé pour afficher la page Ajouter une clé.

or

Choisissez le nom d'utilisateur pour voir la page des détails de l'utilisateur, puis choisissez Ajouter une clé SSH publique pour afficher la page Ajouter une clé.

5. Entrez la nouvelle clé SSH publique et choisissez Ajouter une clé.

Important

Le format de la clé SSH publique dépend du type de clé que vous avez générée.

- Pour RSA les clés, le format est `ssh-rsa` *string*.
- Pour ED25519 les clés, le format est `ssh-ed25519` *string*.
- Pour ECDSA les clés, la clé commence par `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, ou `ecdsa-sha2-nistp521`, selon la taille de la clé que vous avez générée. La chaîne de début est ensuite suivie de *string*, comme pour les autres types de clés.

Vous êtes renvoyé à la page des détails de l'utilisateur, et la nouvelle clé SSH publique que vous venez de saisir apparaît dans la section des clés SSH publiques.

6. Cochez la case correspondant à l'ancienne touche YOU que vous souhaitez supprimer, puis choisissez Supprimer.
7. Confirmez l'opération de suppression en saisissant le mot `delete`, puis choisissez Supprimer.

API

Pour effectuer une rotation des touches à l'aide du API

1. Sur les systèmes d'exploitation macOS, Linux ou Unix, ouvrez un terminal de commande.
2. Récupérez la SSH clé que vous souhaitez supprimer en saisissant la commande suivante. Pour utiliser cette commande, remplacez-la *serverID* par l'ID de serveur de votre serveur Transfer Family, puis par *username* votre nom d'utilisateur.

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

La commande renvoie des informations sur l'utilisateur. Copiez le contenu du "SshPublicKeyId": champ. Vous devrez saisir cette valeur ultérieurement dans cette procédure.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. Importez ensuite une nouvelle SSH clé pour votre utilisateur. À l'invite , entrez la commande suivante. Pour utiliser cette commande, *serverID* remplacez-la par l'ID du serveur de votre serveur Transfer Family, *username* par votre nom d'utilisateur et *public-key* par l'empreinte digitale de votre nouvelle clé publique.

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'  
--ssh-public-key-body='public-key'
```

Si la commande aboutit, aucune sortie n'est renvoyée.

4. Enfin, supprimez l'ancienne clé en exécutant la commande suivante. Pour utiliser cette commande, remplacez *serverID* par l'ID de serveur de votre serveur Transfer Family, remplacez par *username* votre nom d'utilisateur et remplacez par la valeur *keyID-from-step-2* d'ID clé que vous avez copiée à l'étape 2 de cette procédure

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'  
--ssh-public-key-id='keyID-from-step-2'
```

5. (Facultatif) Pour confirmer que l'ancienne clé n'existe plus, répétez l'étape 2.

Génération et gestion PGP des clés

Vous pouvez utiliser le décryptage Pretty Good Privacy (PGP) avec les fichiers que Transfer Family traite avec les flux de travail. Pour utiliser le déchiffrement dans une étape du flux de travail, vous devez fournir une PGP clé.

Le blog sur le AWS stockage contient un article qui décrit comment crypter et déchiffrer des fichiers, crypter et [déchiffrer des fichiers avec et](#). PGP AWS Transfer Family

Générer des PGP clés

La méthode que vous utilisez pour générer vos PGP clés dépend de votre système d'exploitation et de la version du logiciel de génération de clés que vous utilisez.

Si vous utilisez Linux ou Unix, utilisez le programme d'installation de votre package pour l'installergpg. En fonction de votre distribution Linux, l'une des commandes suivantes devrait fonctionner pour vous.

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

Pour Windows ou macOS, vous pouvez télécharger ce dont vous avez besoin [sur https://gnupg.org/download/](https://gnupg.org/download/).

Après avoir installé votre logiciel de génération de PGP clés, vous devez exécuter la `gpg --gen-key` commande `gpg --full-gen-key` or pour générer une paire de clés.

Note

Si vous utilisez la GnuPG version 2.3.0 ou une version plus récente, vous devez exécuter `gpg --full-gen-key`. Lorsque vous êtes invité à saisir le type de clé à créer, choisissez RSA ou ECC. Toutefois, si vous le souhaitez ECC, assurez-vous de choisir l'un des deux NIST or BrainPool pour la courbe elliptique. Ne choisissez pas Curve 25519.

Algorithmes pris en charge pour les paires de PGP clés

Les algorithmes suivants sont pris en charge pour les paires de PGP clés :

- RSA

- Elgamal
- ECC:
 - NIST
 - BrainPool

 Note

Les touches Curve25519 ne sont pas prises en charge.

gpgSous-commandes utiles

Voici quelques sous-commandes utiles pour gpg :

- `gpg --help`— Cette commande répertorie les options disponibles et peut inclure quelques exemples.
- `gpg --list-keys`— Cette commande répertorie les détails de toutes les paires de clés que vous avez créées.
- `gpg --fingerprint`— Cette commande répertorie les détails de toutes vos paires de clés, y compris l'empreinte digitale de chaque clé.
- `gpg --export -a user-name`— Cette commande exporte la partie clé publique de la *user-name* clé utilisée lors de la génération de la clé.

Gérer les clés PGP

Pour gérer vos PGP clés, vous devez utiliser AWS Secrets Manager.

 Note

Votre nom secret inclut votre identifiant de serveur Transfer Family. Cela signifie que vous devez déjà avoir identifié ou créé un serveur avant de pouvoir y stocker vos informations PGP clés AWS Secrets Manager.

Si vous souhaitez utiliser une seule clé et une seule phrase secrète pour tous vos utilisateurs, vous pouvez enregistrer les informations du bloc de PGP clés sous le nom `secretaws/`

transfer/*server-id*/@pgp-default, où se *server-id* trouve l'identifiant de votre serveur Transfer Family. Cette clé par défaut est utilisée si aucune clé ne *user-name* correspond à l'utilisateur qui exécute le flux de travail.

Vous pouvez également créer une clé pour un utilisateur spécifique. Dans ce cas, le format du nom du secret est aws/transfer/*server-id*/*user-name* « où *user-name* correspond à l'utilisateur qui exécute le flux de travail pour un serveur Transfer Family ».

Note

Vous pouvez stocker un maximum de 3 clés PGP privées, par serveur Transfer Family, par utilisateur.

Pour configurer les PGP clés à utiliser avec le déchiffrement

1. Selon la version GPG que vous utilisez, exécutez l'une des commandes suivantes pour générer une paire de PGP clés qui n'utilise pas d'algorithme de chiffrement Curve 25519.
 - Si vous utilisez la **GnuPG** version 2.3.0 ou une version plus récente, exécutez la commande suivante :

```
gpg --full-gen-key
```

Vous pouvez choisir **RSA**, ou, si vous le souhaitez **ECC**, vous pouvez choisir l'une **NIST** ou **BrainPool** l'autre courbe elliptique. Si vous exécutez `gpg --gen-key` plutôt, vous créez une paire de clés qui utilise l'algorithme de chiffrement ECC Curve 25519, que nous ne prenons actuellement pas en charge pour les PGP clés.

- Pour les versions **GnuPG** antérieures à 2.3.0, vous pouvez utiliser la commande suivante, car RSA il s'agit du type de chiffrement par défaut.

```
gpg --gen-key
```

Important

Pendant le processus de génération des clés, vous devez fournir un mot de passe et une adresse e-mail. Assurez-vous de prendre note de ces valeurs. Vous devez fournir le

mot de passe lorsque vous entrez les détails de la clé AWS Secrets Manager plus loin dans cette procédure. Et vous devez fournir la même adresse e-mail pour exporter la clé privée à l'étape suivante.

2. Exécutez la commande suivante pour exporter la clé privée. Pour utiliser cette commande, *private.pgp* remplacez-la par le nom du fichier dans lequel vous souhaitez enregistrer le bloc de clé privée et *marymajor@example.com* par l'adresse e-mail que vous avez utilisée lors de la génération de la paire de clés.

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. AWS Secrets Manager Utilisez-le pour ranger votre PGP clé.
 - a. Connectez-vous à la AWS Secrets Manager console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/secretsmanager/>.
 - b. Dans le volet de navigation de gauche, choisissez Secrets.
 - c. Sur la page Secrets, choisissez Enregistrer un nouveau secret.
 - d. Sur la page Choisir un type de secret, pour Type de secret, sélectionnez Autre type de secret.
 - e. Dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.
 - Clé — Entrée **PGPPrivateKey**.

 Note

Vous devez saisir la **PGPPrivateKey** chaîne exactement : n'ajoutez aucun espace avant ou entre les caractères.

- valeur — Collez le texte de votre clé privée dans le champ de valeur. Le texte de votre clé privée se trouve dans le fichier (par exemple *private.pgp*) que vous avez spécifié lors de l'exportation de votre clé au début de cette procédure. La clé commence par -----BEGIN PGP PRIVATE KEY BLOCK----- et se termine par -----END PGP PRIVATE KEY BLOCK-----.

Note

Assurez-vous que le bloc de texte contient uniquement la clé privée et ne contient pas également la clé publique.

- f. Sélectionnez Ajouter une ligne et dans la section Paires clé/valeur, choisissez l'onglet clé/valeur.

- Clé — Entrée **PGPPassphrase**.

Note

Vous devez saisir la **PGPPassphrase** chaîne exactement : n'ajoutez aucun espace avant ou entre les caractères.

- valeur — Entrez le mot de passe que vous avez utilisé lors de la génération de votre paire PGP de clés.

Choose secret type

Secret type [Info](#)

☐ Credentials for Amazon RDS database
 ☐ Credentials for Amazon DocumentDB database
 ☐ Credentials for Amazon Redshift cluster

☐ Credentials for other database
 ☒ Other type of secret
API key, OAuth token, other.

Key/value pairs [Info](#)

Key/value	Plaintext	
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----	Remove
PGPPassphrase	mypassphrase	Remove
+ Add row		

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.

[Add new key](#)

 Note

Vous pouvez ajouter jusqu'à 3 jeux de clés et de phrases de passe. Pour ajouter un deuxième ensemble, ajoutez deux nouvelles lignes, entrez **PGPPrivateKey2** et **PGPPassphrase2** pour les clés, puis collez une autre clé privée et une autre phrase secrète. Pour ajouter un troisième ensemble, les valeurs clés doivent être **PGPPrivateKey3** et **PGPPassphrase3**.

- g. Choisissez Suivant.
- h. Sur la page Configurer le secret, entrez le nom et la description de votre secret.
 - Si vous créez une clé par défaut, c'est-à-dire une clé qui peut être utilisée par n'importe quel utilisateur de Transfer Family, entrez **aws/transfer/***server-id***@pgp-default**. Remplacez *server-id* par l'ID du serveur qui contient le flux de travail comportant une étape de déchiffrement.
 - Si vous créez une clé destinée à être utilisée par un utilisateur spécifique de Transfer Family, entrez **aws/transfer/***server-id***/***user-name*. Remplacez *server-id* par l'ID du serveur qui contient le flux de travail comportant une étape de déchiffrement et remplacez *user-name* par le nom de l'utilisateur qui exécute le flux de travail. *user-name* est stocké dans le fournisseur d'identité utilisé par le serveur Transfer Family.
- i. Choisissez Next et acceptez les valeurs par défaut sur la page Configurer la rotation. Ensuite, sélectionnez Suivant.
- j. Sur la page Révision, choisissez Store pour créer et stocker le secret.

La capture d'écran suivante montre les informations relatives à l'utilisateur **marymajor** pour un serveur Transfer Family spécifique. Cet exemple montre trois clés et les phrases de passe correspondantes.

/aws/transfer/s- /marymajor

Replicate secret to other Regions

Secret details

Actions

Encryption key
aws/secretsmanager

Secret name
/aws/transfer/s- /marymajor

Secret ARN
arn:aws:secretsmanager:us-east-2:-:secret:/aws/transfer/s- /marymajor-

Secret description
Contains the PGP secret keys and corresponding passphrases to use for user marymajor on Transfer Family server s-

Secret value

Info

Retrieve and view the secret value.

Close

Edit

Key/value

Plaintext

Secret key	Secret value
PGPPrivateKey	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase	mypassphrase
PGPPrivateKey2	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase2	mypassphrase2
PGPPrivateKey3	-----BEGIN PGP PRIVATE KEY BLOCK-----
PGPPassphrase3	mypassphrase3

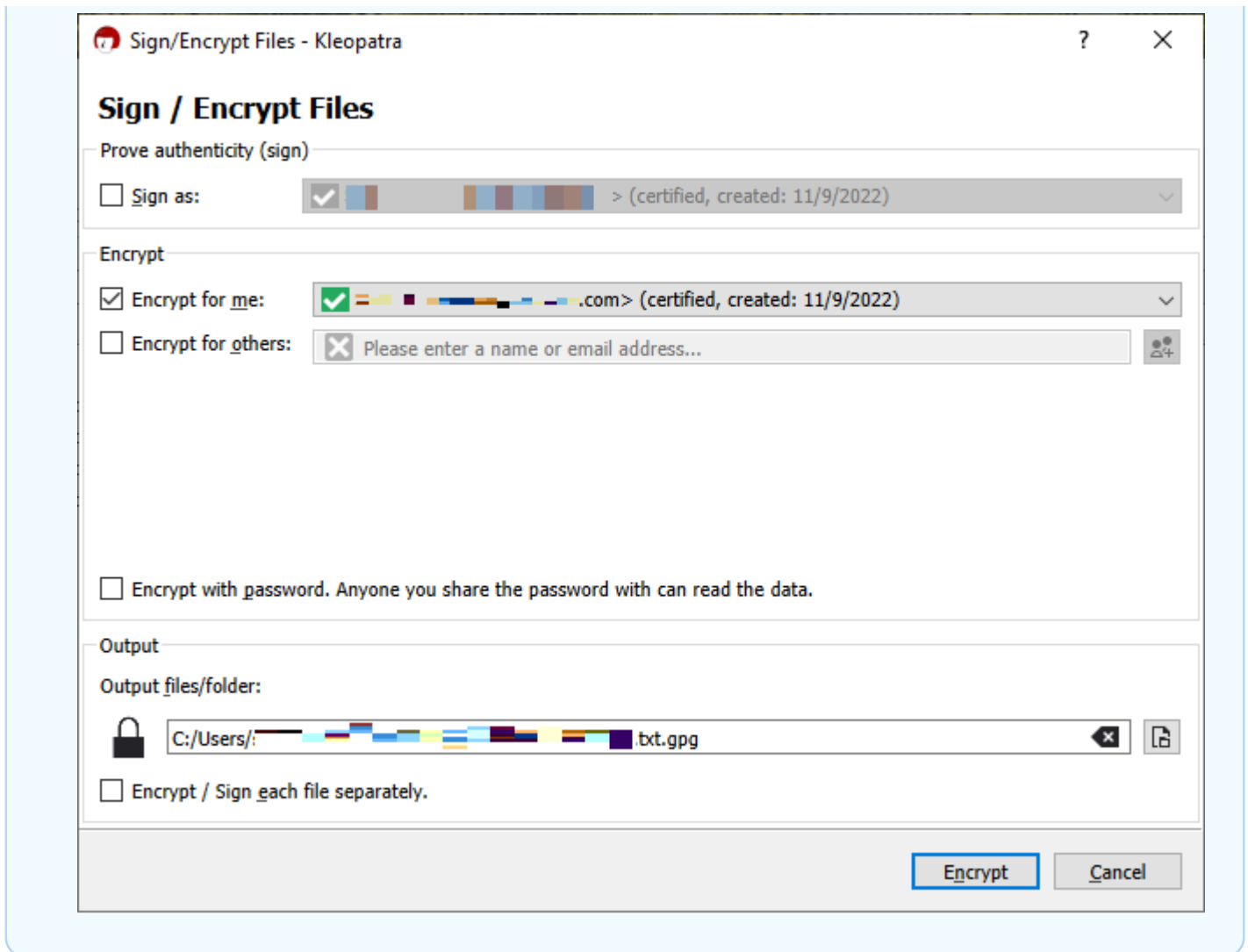
PGPClients pris en charge

Les clients suivants ont été testés avec Transfer Family et peuvent être utilisés pour générer des PGP clés et pour chiffrer des fichiers que vous souhaitez déchiffrer à l'aide d'un flux de travail.

- GPG4win + Cléopâtre.

 Note

Lorsque vous sélectionnez Signer/Chiffrer des fichiers, assurez-vous de désactiver la sélection pour Signer en tant que : nous ne prenons actuellement pas en charge la signature pour les fichiers chiffrés.



- Principales versions de GnuPG : 2.4, 2.3, 2.2, 2.0 et 1.4.

Notez que d'autres PGP clients peuvent également fonctionner, mais seuls les clients mentionnés ici ont été testés avec Transfer Family.

Gestion des identités et des accès pour AWS Transfer Family

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. IAM les administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les AWS Transfer Family ressources. IAM est un Service AWS stylo que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)

- [Authentification par des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [Comment AWS Transfer Family fonctionne avec IAM](#)
- [AWS Transfer Family exemples de politiques basées sur l'identité](#)
- [AWS Transfer Family exemples de politiques basées sur des balises](#)
- [Résolution des problèmes AWS Transfer Family d'identité et d'accès](#)

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez AWS Transfer Family.

Utilisateur du service : si vous utilisez le AWS Transfer Family service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS Transfer Family fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS Transfer Family, consultez [Résolution des problèmes AWS Transfer Family d'identité et d'accès](#).

Administrateur du service — Si vous êtes responsable des AWS Transfer Family ressources de votre entreprise, vous avez probablement un accès complet à AWS Transfer Family. C'est à vous de déterminer les AWS Transfer Family fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base de IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec AWS Transfer Family, voir [Comment AWS Transfer Family fonctionne avec IAM](#).

IAM administrateur — Si vous êtes IAM administrateur, vous souhaitez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS Transfer Family. Pour consulter des exemples de politiques AWS Transfer Family basées sur l'identité que vous pouvez utiliser dans IAM, consultez. [AWS Transfer Family exemples de politiques basées sur l'identité](#)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAMutilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAMIdentity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section [Comment vous connecter à votre compte Compte AWS dans](#) le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section [Signature des AWS API demandes](#) dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez [Authentification multifactorielle](#) dans le guide de AWS IAM Identity Center l'utilisateur et [Utilisation de l'authentification multifactorielle \(MFA\) AWS dans](#) le guide de l'IAMutilisateur.

Utilisateur racine d'un compte AWS

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine

peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section [Tâches nécessitant des informations d'identification utilisateur root](#) dans le guide de IAM l'utilisateur.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez [Qu'est-ce qu'IAM Identity Center ?](#) dans le guide de AWS IAM Identity Center l'utilisateur.

Utilisateurs et groupes IAM

Un [IAMutilisateur](#) est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de passe et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme](#) dans le Guide de IAM l'utilisateur.

Un [IAMgroupe](#) est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour

de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir [Quand créer un IAM utilisateur \(au lieu d'un rôle\)](#) dans le Guide de IAM l'utilisateur.

IAMrôles

Un [IAMrôle](#) est une identité au sein de Compte AWS vous dotée d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans le en AWS Management Console [changeant de rôle](#). Vous pouvez assumer un rôle en appelant une AWS API opération AWS CLI or ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section [Utilisation IAM des rôles](#) dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir [Création d'un rôle pour un fournisseur d'identité tiers](#) dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les jeux d'autorisations, consultez [Jeux d'autorisations](#) dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations IAM utilisateur temporaires : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- Accès entre comptes : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès

entre comptes, consultez la section [En quoi les IAM rôles diffèrent des politiques basées sur les ressources](#) dans le Guide de l'utilisateur. IAM

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- Sessions d'accès transmises (FAS) — Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant au Service AWS, combinées à la demande Service AWS pour adresser des demandes aux services en aval. FAS les demandes ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives à l'envoi de FAS demandes, consultez la section [Transférer les sessions d'accès](#).
- Rôle de service — Un rôle de service est un [IAM rôle](#) qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieur IAM. Pour plus d'informations, consultez [la section Création d'un rôle auquel déléguer des autorisations Service AWS](#) dans le Guide de IAM l'utilisateur.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui font AWS CLI des AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section [Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir [Quand créer un IAM rôle \(au lieu d'un utilisateur\)](#) dans le guide de IAM l'utilisateur.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir [Présentation des JSON politiques](#) dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

IAMLes politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur doté de cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console AWS CLI, ou du AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section [Création de IAM politiques](#) dans le Guide de l'IAMutilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les

politiques AWS gérées et les politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir [Choisir entre des politiques gérées et des politiques intégrées dans le Guide](#) de l'IAMutilisateur.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser de politiques AWS gérées depuis une IAM stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 et Amazon VPC sont des exemples de services compatibles ACLs. AWS WAF Pour en savoir plus ACLs, consultez la [présentation de la liste de contrôle d'accès \(ACL\)](#) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limites d'autorisations** — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui

spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section Limites d'[autorisations pour les IAM entités](#) dans le Guide de IAM l'utilisateur.

- **Politiques de contrôle des services (SCPs) :** SCPs JSON politiques qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Les SCP limites d'autorisations pour les entités présentes dans les comptes des membres, y compris chacune d'entre elles Utilisateur racine d'un compte AWS. Pour plus d'informations sur les OrganizationsSCPs, voir [Comment SCPs travailler](#) dans le Guide de AWS Organizations l'utilisateur.
- **Politiques de séance :** les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section [Politiques de session](#) dans le guide de IAM l'utilisateur.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de IAM l'utilisateur.

Comment AWS Transfer Family fonctionne avec IAM

Avant d'utiliser AWS Identity and Access Management (IAM) pour gérer l'accès à AWS Transfer Family, vous devez connaître les IAM fonctionnalités disponibles AWS Transfer Family. Pour obtenir une vue d'ensemble du mode de fonctionnement des autres AWS services AWS Transfer Family et des autres services IAM, consultez la section [AWS Services compatibles IAM](#) dans le Guide de IAM l'utilisateur.

Rubriques

- [AWS Transfer Family Politiques basées sur l'identité](#)
- [AWS Transfer Family Politiques basées sur les ressources](#)
- [Autorisation basée sur les balises AWS Transfer Family](#)
- [AWS Transfer Family IAM rôles](#)

AWS Transfer Family Politiques basées sur l'identité

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. AWS Transfer Family prend en charge des actions, des ressources et des clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une JSON politique, consultez la [référence aux éléments de IAM JSON politique](#) dans le Guide de AWS Identity and Access Management l'utilisateur.

Actions

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'Action élément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions de stratégie portent généralement le même nom que l' AWS API opération associée. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions de politique en AWS Transfer Family cours utilisent le préfixe suivant avant l'action :`transfer:`. Par exemple, pour autoriser quelqu'un à créer un serveur, avec l'`CreateServer` API opération Transfer Family, vous incluez l'`transfer:CreateServer` action dans sa politique. Les déclarations de politique doivent inclure un élément `Action` ou `NotAction`. AWS Transfer Family définit son propre ensemble d'actions qui décrivent les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule instruction, séparez-les par des virgules, comme suit :

```
"Action": [  
  "transfer:action1",  
  "transfer:action2"
```

Vous pouvez aussi préciser plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante.

```
"Action": "transfer:Describe*"
```

Pour consulter la liste des AWS Transfer Family actions, reportez-vous à la section [Actions définies par AWS Transfer Family](#) dans la référence d'autorisation de service.

Ressources

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Resource` JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de spécifier une ressource en utilisant son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

La ressource du serveur Transfer Family contient les éléments suivantsARN.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

Par exemple, pour spécifier le serveur `s-01234567890abcdef` Transfer Family dans votre relevé, utilisez ce qui suitARN.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

Pour plus d'informations sur le format de ARNs, consultez [Amazon Resource Names \(ARNs\)](#) dans le Service Authorization Reference ou [IAM ARNs](#) dans le Guide de IAM l'utilisateur.

Pour spécifier toutes les instances qui appartiennent à un compte spécifique, utilisez le caractère générique (*).

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

Certaines AWS Transfer Family actions sont effectuées sur plusieurs ressources, telles que celles utilisées dans IAM les politiques. Dans ces cas-là, vous devez utiliser le caractère générique (*).

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

Dans certains cas, vous devez spécifier plusieurs types de ressources, par exemple si vous créez une politique qui autorise l'accès aux serveurs et aux utilisateurs de Transfer Family. Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules.

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

Pour consulter la liste des AWS Transfer Family ressources, consultez la section [Types de ressources définis par AWS Transfer Family](#) dans la référence d'autorisation de service.

Clés de condition

Les administrateurs peuvent utiliser AWS JSON des politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément Condition (ou le bloc Condition) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément Condition est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments Condition dans une instruction, ou plusieurs clés dans un seul élément Condition, AWS les évalue à l'aide d'une opération AND logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR

opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez [IAM la section Éléments de politique : variables et balises](#) dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les [clés contextuelles de condition AWS globales](#) dans le guide de IAM l'utilisateur.

AWS Transfer Family définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour consulter la liste des clés de AWS Transfer Family condition, reportez-vous à la section [Clés de condition pour AWS Transfer Family](#) la référence d'autorisation de service.

Exemples

Pour consulter des exemples de politiques AWS Transfer Family basées sur l'identité, consultez. [AWS Transfer Family exemples de politiques basées sur l'identité](#)

AWS Transfer Family Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de JSON politique qui spécifient les actions qu'un principal spécifié peut effectuer sur la AWS Transfer Family ressource et dans quelles conditions. Amazon S3 prend en charge les politiques d'autorisation basées sur les ressources pour Amazon S3 *buckets*. Les politiques basées sur les ressources vous permettent d'accorder des autorisations d'utilisation à d'autres comptes pour chaque ressource. Vous pouvez également utiliser une politique basée sur les ressources pour autoriser un AWS service à accéder à votre Amazon S3 *buckets*.

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme [principal dans une politique basée sur les ressources](#). L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource se trouvent dans des AWS comptes différents, vous devez également accorder à l'entité principale l'autorisation d'accéder à la ressource. Accordez l'autorisation en attachant une stratégie basée sur les identités à l'entité. Toutefois, si une stratégie basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre stratégie basée sur l'identité n'est requise. Pour plus d'informations, consultez la section En

[quoi IAM les rôles diffèrent des politiques basées sur les ressources](#) dans le Guide de l'AWS Identity and Access Management utilisateur.

Le service Amazon S3 ne prend en charge qu'un seul type de politique basée sur les ressources appelé *bucket* politique, qui est attachée à un *bucket*. Cette politique définit les entités principales (comptes, utilisateurs, rôles et utilisateurs fédérés) qui peuvent effectuer des actions sur l'objet.

Exemples

Pour consulter des exemples de politiques AWS Transfer Family basées sur les ressources, consultez [AWS Transfer Family exemples de politiques basées sur des balises](#)

Autorisation basée sur les balises AWS Transfer Family

Vous pouvez associer des balises aux AWS Transfer Family ressources ou transmettre des balises dans une demande à AWS Transfer Family. Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'[élément de condition](#) d'une politique utilisant les clés de condition `transfer:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`. Pour plus d'informations sur l'utilisation des balises pour contrôler l'accès aux AWS Transfer Family ressources, consultez [AWS Transfer Family exemples de politiques basées sur des balises](#).

AWS Transfer Family IAM rôles

Un [IAM rôle](#) est une entité de votre AWS compte dotée d'autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec AWS Transfer Family

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à la fédération, assumer un IAM rôle ou assumer un rôle entre comptes. Vous obtenez des informations d'identification de sécurité temporaires en appelant AWS STS API des opérations telles que [AssumeRole](#) ou [GetFederationToken](#).

AWS Transfer Family prend en charge l'utilisation d'informations d'identification temporaires.

AWS Transfer Family exemples de politiques basées sur l'identité

Par défaut, IAM les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier AWS Transfer Family des ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide du AWS Management Console AWS CLI, ou AWS API. Un IAM administrateur doit créer des IAM politiques qui accordent aux utilisateurs et aux rôles l'autorisation d'effectuer des API opérations spécifiques sur

les ressources spécifiques dont ils ont besoin. L'administrateur doit ensuite associer ces politiques aux IAM utilisateurs ou aux groupes qui ont besoin de ces autorisations.

Pour savoir comment créer une politique IAM basée sur l'identité à l'aide de ces exemples de documents de JSON stratégie, voir [Création de politiques dans l'JSONonglet du Guide](#) de l'AWS Identity and Access Management utilisateur.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Utilisation de la console AWS Transfer Family](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS Transfer Family des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez [les politiques AWS gérées ou les politiques AWS gérées pour les fonctions professionnelles](#) dans le Guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section [Politiques et autorisations IAM dans](#) le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisant SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique

Service AWS, tel que AWS CloudFormation. Pour plus d'informations, voir [Éléments IAM JSON de politique : Condition](#) dans le guide de IAM l'utilisateur.

- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAM Access Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez la section [Validation des politiques d'IAM Access Analyzer](#) dans le guide de IAM l'utilisateur.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des IAM utilisateurs ou un utilisateur root Compte AWS, activez-le MFA pour une sécurité supplémentaire. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez [la section Configuration de l'API accès MFA protégé](#) dans le Guide de l'IAM utilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de [sécurité IAM](#), consultez la section [Bonnes pratiques en matière](#) de sécurité IAM dans le Guide de IAM l'utilisateur.

Utilisation de la console AWS Transfer Family

Pour accéder à la AWS Transfer Family console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les informations relatives AWS Transfer Family aux ressources de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (IAM utilisateurs ou rôles) dotées de cette politique. Pour plus d'informations, consultez la section [Ajouter des autorisations à un utilisateur](#) dans le Guide de AWS Identity and Access Management l'utilisateur.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui passent des appels uniquement vers le AWS CLI ou le AWS API. Au lieu de cela, autorisez uniquement l'accès aux actions correspondant à l'API opération que vous essayez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI ou. AWS API

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Transfer Family exemples de politiques basées sur des balises

Vous trouverez ci-dessous des exemples de contrôle de l'accès aux AWS Transfer Family ressources à l'aide de balises.

Utilisation de balises pour contrôler l'accès aux ressources AWS Transfer Family

Les conditions figurant dans les IAM politiques font partie de la syntaxe que vous utilisez pour spécifier les autorisations relatives aux AWS Transfer Family ressources. Vous pouvez contrôler

l'accès aux AWS Transfer Family ressources (telles que les utilisateurs, les serveurs, les rôles et autres entités) en fonction des balises associées à ces ressources. Les balises sont des paires clé-valeur. Pour plus d'informations sur le balisage des ressources, consultez la section [Marquage AWS des ressources](#) dans le. Références générales AWS

Dans AWS Transfer Family, les ressources peuvent avoir des balises, et certaines actions peuvent inclure des balises. Lorsque vous créez une IAM politique, vous pouvez utiliser les clés de condition des balises pour contrôler les éléments suivants :

- Quels utilisateurs peuvent effectuer des actions sur une AWS Transfer Family ressource, en fonction des balises que possède la ressource.
- quelles balises peuvent être transmises dans une demande d'action ;
- si des clés de balise spécifiques peuvent être utilisées dans une demande.

En utilisant le contrôle d'accès basé sur des balises, vous pouvez appliquer un contrôle plus fin qu'au API niveau. Vous pouvez également appliquer un contrôle plus dynamique qu'en utilisant le contrôle d'accès basé sur les ressources. Vous pouvez créer des IAM politiques qui autorisent ou refusent une opération en fonction des balises fournies dans la demande (balises de demande). Vous pouvez également créer des IAM politiques basées sur les balises de la ressource utilisée (balises de ressource). En général, les balises de ressources concernent les balises déjà présentes sur les ressources, tandis que les balises de requête sont destinées à être utilisées lorsque vous ajoutez des balises à une ressource ou que vous en supprimez.

Pour connaître la syntaxe et la sémantique complètes des clés de condition des balises, voir [Contrôle de l'accès aux AWS ressources à l'aide des balises de ressources](#) dans le Guide de l'IAMutilisateur. Pour plus de détails sur la définition de IAM politiques avec API Gateway, voir [Contrôler l'accès à et API avec IAM des autorisations](#) dans le Guide du développeur de API Gateway.

Exemple 1 : Refuser les actions en fonction des balises de ressources

Vous pouvez refuser l'exécution d'une action sur une ressource en fonction de balises. L'exemple de politique suivant refuse `TagResource`, `UntagResource`, `StartServer`, `StopServer` `DescribeServer`, et les `DescribeUser` opérations si la ressource utilisateur ou serveur est étiquetée avec la clé `stage` et la valeur `prod`.

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

```

{
  "Effect": "Deny",
  "Action": [
    "transfer:TagResource",
    "transfer:UntagResource",
    "transfer:StartServer",
    "transfer:StopServer",
    "transfer:DescribeServer",
    "transfer:DescribeUser"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/stage": "prod"
    }
  }
}

```

Exemple 2 : Autoriser les actions en fonction des balises de ressources

Vous pouvez autoriser l'exécution d'une action sur une ressource en fonction de balises.

L'exemple de politique suivant autorise les DescribeUser opérations TagResource

UntagResourceStartServer,StopServer,DescribeServer,, et si la ressource utilisateur ou serveur est étiquetée avec la clé stage et la valeurprod.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "transfer:TagResource",
        "transfer:UntagResource",
        "transfer:StartServer",
        "transfer:StopServer",
        "transfer:DescribeServer",
        "transfer:DescribeUser"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {

```

```

        "aws:ResourceTag/stage": "prod"
      }
    }
  ]
}

```

Exemple 3 : refuser la création d'un utilisateur ou d'un serveur en fonction des balises de requête

L'exemple de politique suivant contient deux déclarations. La première instruction refuse l'CreateServeropération sur toutes les ressources si la clé du centre de coûts associée à la balise n'a pas de valeur.

La deuxième instruction refuse l'CreateServeropération si la clé du centre de coûts pour la balise contient une valeur autre que 1, 2 ou 3.

Note

Cette politique permet de créer ou de supprimer une ressource contenant une clé appelée `costcenter` et une valeur de 12, ou 3.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "transfer:CreateServer"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/costcenter": "true"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "transfer:CreateServer",

```

```

    "Resource": [
      "*"
    ],
    "Condition": {
      "ForAnyValue:StringNotEquals": {
        "aws:RequestTag/costcenter": [
          "1",
          "2",
          "3"
        ]
      }
    }
  }
]
}

```

Résolution des problèmes AWS Transfer Family d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS Transfer Family et IAM.

Rubriques

- [Je ne suis pas autorisé à effectuer une action dans AWS Transfer Family](#)
- [Je ne suis pas autorisé à effectuer iam : PassRole](#)
- [Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS Transfer Family ressources](#)

Je ne suis pas autorisé à effectuer une action dans AWS Transfer Family

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojacksonIAMutilisateur` essaie d'utiliser la console pour afficher les détails d'un `widget` mais ne dispose pas d'`transfer:GetWidget` autorisations.

```

User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
transfer: GetWidget on resource: my-example-widget

```


Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *my-example-widget* à l'aide de l'action `transfer:GetWidget`.

Je ne suis pas autorisé à effectuer `iam:PassRole`

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS Transfer Family.

Certains services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un IAM utilisateur nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AWS Transfer Family. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

L'exemple de politique suivant contient l'autorisation de transmettre un rôle à AWS Transfer Family.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/*",
      "Effect": "Allow"
    }
  ]
}
```

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS Transfer Family ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS Transfer Family en charge, consultez [Comment AWS Transfer Family fonctionne avec IAM](#).
- Pour savoir comment donner accès à vos ressources sur un site Comptes AWS qui vous appartient, consultez la section [Fournir l'accès à un IAM utilisateur dans un autre site Compte AWS que vous possédez](#) dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section [Fournir un accès à des ressources Comptes AWS détenues par des tiers](#) dans le Guide de IAM l'utilisateur.
- Pour savoir comment fournir un accès via la fédération d'identité, consultez la section [Fournir un accès aux utilisateurs authentifiés de manière externe \(fédération d'identité\)](#) dans le guide de l'IAM utilisateur.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section En [quoi les IAM rôles diffèrent des politiques basées sur les ressources](#) dans le Guide de l'utilisateur. IAM

Validation de conformité pour AWS Transfer Family

Des auditeurs tiers évaluent la sécurité et AWS Transfer Family la conformité de plusieurs programmes de AWS conformité. Ceux-ci incluent SOC, PCIHIPAA, et d'autres. Pour la liste complète, voir [AWS Services concernés par programme de conformité](#).

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir [AWS Services concernés par programme de conformité](#). Pour obtenir des informations générales, veuillez consulter [Programmes de conformité d'AWS](#).

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez la section [Téléchargement de rapports dans AWS Artifact](#).

Votre responsabilité en matière de conformité lors de l'utilisation AWS Transfer Family est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- [Guides de démarrage rapide sur la sécurité et la conformité](#) : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS
- [Livre blanc sur l'architecture au service de la HIPAA sécurité et de la conformité](#) — Ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes. HIPAA
- [Ressources de conformité d'AWS](#) – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur et à votre emplacement.
- [AWS Config](#)— Ce AWS 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](#)— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans AWS Transfer Family

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. 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.

AWS Transfer Family prend en charge jusqu'à 3 zones de disponibilité et s'appuie sur un parc redondant à évolutivité automatique pour vos demandes de connexion et de transfert.

Notez ce qui suit :

- Pour les points de terminaison publics :

- La redondance au niveau de la zone de disponibilité est intégrée au service
- Il existe des flottes redondantes pour chaque AZ.
- Cette redondance est fournie automatiquement
- Pour les points de terminaison dans un cloud privé virtuel (VPC), voir [Création d'un serveur dans un cloud privé virtuel](#).

Voir aussi

- Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).
 - Pour savoir comment améliorer la redondance et minimiser la latence du réseau en utilisant le routage basé sur la latence, consultez le billet de blog [Minimize network](#) latency with your servers.
- AWS Transfer Family

Sécurité de l'infrastructure dans AWS Transfer Family

En tant que service géré, AWS Transfer Family 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 API les appels AWS publiés pour accéder AWS Transfer Family via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Sécurité de la couche de transport (TLS). Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Des suites de chiffrement parfaitement confidentielles (PFS) telles que (Ephemeral Diffie-Hellman) ou DHE 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 identifiant de clé d'accès et d'une clé d'accès secrète associés à un IAM principal. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Ajouter un pare-feu pour applications Web

AWS WAF est un pare-feu pour applications Web qui aide à protéger les applications Web APIs contre les attaques. Vous pouvez l'utiliser pour configurer un ensemble de règles connu sous le nom de liste de contrôle d'accès Web (WebACL) qui autorise, bloque ou compte les requêtes Web en fonction de règles et de conditions de sécurité Web personnalisables que vous définissez. Pour plus d'informations, consultez la section [Utilisation AWS WAF pour protéger votre APIs](#).

Pour ajouter AWS WAF

1. Ouvrez la console API Gateway à l'adresse <https://console.aws.amazon.com/apigateway/>.
2. Dans le volet APIs de navigation, puis choisissez votre modèle de fournisseur d'identité personnalisé.
3. Choisissez Stages (Étapes).
4. Dans le volet Stages, choisissez le nom de l'étape.
5. Dans le volet Stage Editor, sélectionnez l'onglet Settings.
6. Effectuez l'une des actions suivantes :
 - Sous Web Application Firewall (WAF), pour Web ACL, choisissez le site Web ACL que vous souhaitez associer à cette étape.
 - Si le site Web dont ACL vous avez besoin n'existe pas, vous devez en créer un en procédant comme suit :
 1. Choisissez Create Web ACL.
 2. Sur la page d'accueil du AWS WAF service, choisissez Create web ACL.
 3. Dans ACL Détails du site Web, dans Nom, tapez le nom du site WebACL.
 4. Dans Règles, choisissez Ajouter des règles, puis Ajouter mes propres règles et groupes de règles.
 5. Pour Type de règle, choisissez IP set pour identifier une liste spécifique d'adresses IP.
 6. Pour Règle, entrez le nom de la règle.
 7. Pour un ensemble d'adresses IP, choisissez un ensemble d'adresses IP existant. Pour créer un ensemble d'adresses IP, voir [Création d'un ensemble d'adresses IP](#).
 8. Pour l'adresse IP à utiliser comme adresse d'origine, choisissez l'adresse IP dans l'en-tête.
 9. Pour le nom du champ d'en-tête, entrez SourceIP.
 10. Pour Position dans l'en-tête, choisissez Première adresse IP.

- 11 Pour **Fallback for missing IP address**, choisissez **Match** ou **No Match** en fonction de la manière dont vous souhaitez gérer une adresse IP non valide (ou manquante) dans l'en-tête.
 - 12 Pour **Action**, choisissez l'action de l'ensemble d'adresses IP.
 - 13 Pour l'**ACL action Web** par défaut pour les demandes qui ne répondent à aucune règle, choisissez **Autoriser** ou **Bloquer**, puis cliquez sur **Suivant**.
 - 14 Pour les étapes 4 et 5, choisissez **Next**.
 - 15 Dans **Révision et création**, passez en revue vos choix, puis choisissez **Créer un site Web ACL**.
7. Choisissez **Save Changes** (Enregistrer les modifications).
 8. Sélectionnez **Ressources**.
 9. Pour **Actions**, sélectionnez **Déployer API**.

Pour plus d'informations sur le niveau de sécurité AWS Transfer Family avec AWS le pare-feu d'applications Web, consultez la section [Sécurisation AWS Transfer Family avec le pare-feu d' AWS application et Amazon API Gateway](#) dans le blog sur le AWS stockage.

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 d'appel peut être manipulé pour utiliser ses autorisations afin d'agir sur les ressources d'un autre client d'une manière à laquelle il ne devrait pas être autorisé à 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. Pour une description détaillée de ce problème, voir [le problème de confusion des adjoints](#) dans le guide de IAM l'utilisateur.

Nous recommandons d'utiliser les clés contextuelles de condition [aws:SourceAccount](#) globale [aws:SourceArn](#) et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations accordées à AWS Transfer Family pour la ressource. Si vous utilisez les deux clés de contexte de condition globale, la valeur `aws:SourceAccount` et le compte de la valeur

`aws:SourceArn` doit utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de stratégie.

Le moyen le plus efficace de se protéger contre le problème de confusion des adjoints est d'utiliser le nom de ressource Amazon exact (ARN) de la ressource que vous souhaitez autoriser. Si vous spécifiez plusieurs ressources, utilisez la clé de condition contextuelle `aws:SourceArn` globale avec des caractères génériques (*) pour les parties inconnues du ARN. Par exemple, `arn:aws:transfer::region::account-id:server/*`.

AWS Transfer Family utilise les types de rôles suivants :

- **Rôle utilisateur** — Permet aux utilisateurs gérés par le service d'accéder aux ressources Transfer Family nécessaires. AWS Transfer Family assume ce rôle dans le contexte d'un utilisateur de Transfer FamilyARN.
- **Rôle d'accès** — Permet d'accéder uniquement aux fichiers Amazon S3 en cours de transfert. Pour les AS2 transferts entrants, le rôle d'accès utilise le nom de ressource Amazon (ARN) pour l'accord. Pour les AS2 transferts sortants, le rôle d'accès utilise le ARN pour le connecteur.
- **Rôle d'invocation** : à utiliser avec Amazon API Gateway en tant que fournisseur d'identité personnalisé du serveur. Transfer Family assume ce rôle dans le contexte d'un serveur Transfer FamilyARN.
- **Rôle de journalisation** : utilisé pour enregistrer les entrées sur Amazon CloudWatch. Transfer Family utilise ce rôle pour enregistrer les informations relatives aux réussites et aux échecs ainsi que les informations relatives aux transferts de fichiers. Transfer Family assume ce rôle dans le contexte d'un serveur Transfer FamilyARN. Pour les AS2 transferts sortants, le rôle de journalisation utilise le connecteurARN.
- **Rôle d'exécution** — Permet à un utilisateur de Transfer Family d'appeler et de lancer des flux de travail. Transfer Family assume ce rôle dans le contexte d'un flux de travail Transfer FamilyARN.

Pour plus d'informations, consultez la section [Politiques et autorisations IAM dans](#) le guide de IAM l'utilisateur.

 Note

Dans les exemples suivants, remplacez chaque *user input placeholder* avec vos propres informations.

 Note

Dans nos exemples, nous utilisons à la fois `ArnLike` et `ArnEquals`. Ils sont fonctionnellement identiques, et vous pouvez donc utiliser l'un ou l'autre lorsque vous élaborez vos politiques. La documentation Transfer Family `ArnLike` est utilisée lorsque la condition contient un caractère générique et `ArnEquals` pour indiquer une condition de correspondance exacte.

AWS Transfer Family : rôle d'utilisateur, interservices, prévention des adjoints confus

L'exemple de politique suivant permet à n'importe quel utilisateur de n'importe quel serveur du compte d'assumer le rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:region:account-id:user/*"
        }
      }
    }
  ]
}
```

L'exemple de politique suivant permet à n'importe quel utilisateur d'un serveur spécifique d'assumer le rôle.


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/*"
        }
      }
    }
  ]
}
```

L'exemple de politique suivant permet à un utilisateur spécifique d'un serveur spécifique d'assumer le rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/user-name"
        }
      }
    }
  ]
}
```

```
    ]
  }
}
```

AWS Transfer Family Workflow, rôle, interservices, prévention des adjoints confus

L'exemple de politique suivant permet à n'importe quel flux de travail du compte d'assumer le rôle.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:region:account-id:workflow/*"
        }
      }
    }
  ]
}
```

L'exemple de politique suivant permet à un flux de travail spécifique d'assumer le rôle.

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

```

        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:transfer:region:account-id:workflow/workflow-id"
            }
        }
    ]
}

```

AWS Transfer Family : enregistrement et rôle d'invocation, interservices, prévention des adjoints confus

Note

Les exemples suivants peuvent être utilisés à la fois dans les rôles de journalisation et d'invocation.

Dans ces exemples, vous pouvez supprimer les ARN détails d'un flux de travail si aucun flux de travail n'est associé à votre serveur.

L'exemple de politique de journalisation et d'appel suivant permet à n'importe quel serveur (et flux de travail) du compte d'assumer le rôle.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllServersWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:region:account-id:server/*",

```

```

        "arn:aws:transfer:region:account-id:workflow/*"
      ]
    }
  }
]
}

```

L'exemple de politique de journalisation et d'appel suivant permet à un serveur (et à un flux de travail) spécifiques d'assumer le rôle.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificServerWithWorkflowAttached",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "account-id"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:transfer:region:account-id:server/server-id",
            "arn:aws:transfer:region:account-id:workflow/workflow-id"
          ]
        }
      }
    }
  ]
}

```

AWS politiques gérées pour AWS Transfer Family

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 AWS Identity and Access Management \(IAM\) des politiques gérées par le client](#) qui fournissent

à votre équipe uniquement 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 IAM l'utilisateur. Pour obtenir une liste détaillée de toutes les politiques AWS gérées, consultez le [guide de référence des politiques AWS gérées](#).

AWS les services maintiennent et mettent 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 tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir une liste et une description des politiques relatives aux fonctions de travail, voir [les politiques AWS gérées pour les fonctions de travail](#) dans le Guide de IAM l'utilisateur.

AWS politique gérée : `AWSTransferConsoleFullAccess`

La `AWSTransferConsoleFullAccess` politique fournit un accès complet à Transfer Family via la console AWS de gestion.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `acm:ListCertificates`— Accorde l'autorisation de récupérer la liste des certificats Amazon Resource Names (ARNs) et le nom de domaine de chacun d'euxARN.
- `ec2:DescribeAddresses`— Accorde l'autorisation de décrire une ou plusieurs adresses IP élastiques.
- `ec2:DescribeAvailabilityZones`— Accorde l'autorisation de décrire une ou plusieurs des zones de disponibilité mises à votre disposition.
- `ec2:DescribeNetworkInterfaces`— Accorde l'autorisation de décrire une ou plusieurs interfaces réseau élastiques.

- `ec2:DescribeSecurityGroups`— Accorde l'autorisation de décrire un ou plusieurs groupes de sécurité.
- `ec2:DescribeSubnets`— Accorde l'autorisation de décrire un ou plusieurs sous-réseaux.
- `ec2:DescribeVpcs`— Accorde l'autorisation de décrire un ou plusieurs clouds privés virtuels (VPCs).
- `ec2:DescribeVpcEndpoints`— Accorde l'autorisation de décrire un ou plusieurs VPC points de terminaison.
- `health:DescribeEventAggregates`— Renvoie le nombre d'événements de chaque type d'événement (problème, modification planifiée et notification de compte).
- `iam:GetPolicyVersion`— Accorde l'autorisation de récupérer des informations sur une version de la politique gérée spécifiée, y compris le document de politique.
- `iam:ListPolicies`— Accorde l'autorisation de répertorier toutes les politiques gérées.
- `iam:ListRoles`— Accorde l'autorisation de répertorier les IAM rôles dotés du préfixe de chemin spécifié.
- `iam:PassRole`— Accorde l'autorisation de transmettre un IAM rôle à Transfer Family. Pour plus de détails, consultez la section [Accorder à un utilisateur l'autorisation de transmettre un rôle à un Service AWS](#).
- `route53:ListHostedZones`— Accorde l'autorisation d'obtenir une liste des zones hébergées publiques et privées associées au courant Compte AWS.
- `s3:ListAllMyBuckets`— Accorde l'autorisation de répertorier tous les buckets appartenant à l'expéditeur authentifié de la demande.
- `transfer:*`— Donne accès aux ressources de Transfer Family. L'astérisque (*) donne accès à toutes les ressources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "transfer.amazonaws.com"
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "acm:ListCertificates",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeVpcEndpoints",
      "health:DescribeEventAggregates",
      "iam:GetPolicyVersion",
      "iam:ListPolicies",
      "iam:ListRoles",
      "route53:ListHostedZones",
      "s3:ListAllMyBuckets",
      "transfer:*"
    ],
    "Resource": "*"
  }
]
}

```

AWS politique gérée : AWSTransferFullAccess

La `AWSTransferFullAccess` politique fournit un accès complet aux services Transfer Family.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `transfer:*`— Autorise l'accès aux ressources de Transfer Family. L'astérisque (*) donne accès à toutes les ressources.
- `iam:PassRole`— Accorde l'autorisation de transmettre un IAM rôle à Transfer Family. Pour plus de détails, consultez la section [Accorder à un utilisateur l'autorisation de transmettre un rôle à un Service AWS](#).
- `ec2:DescribeAddresses`— Accorde l'autorisation de décrire une ou plusieurs adresses IP élastiques.

- `ec2:DescribeNetworkInterfaces`— Accorde l'autorisation de décrire une ou plusieurs interfaces réseau.
- `ec2:DescribeVpcEndpoints`— Accorde l'autorisation de décrire un ou plusieurs VPC points de terminaison.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "transfer:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "transfer.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAddresses"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS politique gérée : AWSTransferLoggingAccess

La `AWSTransferLoggingAccess` politique accorde à AWS Transfer Family un accès complet pour créer des flux de journaux et des groupes et pour enregistrer les événements de journal sur votre compte.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes pour Amazon CloudWatch Logs.

- **CreateLogStream**— Autorise les directeurs à créer un flux de journal.
- **DescribeLogStreams**— Autorise les principaux à répertorier les flux de journaux du groupe de journaux.
- **CreateLogGroup**— Autorise les directeurs à créer des groupes de journaux.
- **PutLogEvents**— Autorise les principaux à télécharger un lot d'événements de journal dans un flux de journaux.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS politique gérée : AWSTransferReadOnlyAccess

La **AWSTransferReadOnlyAccess** politique fournit un accès en lecture seule aux services Transfer Family.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes pour Transfer Family.

- **DescribeUser**— Autorise les directeurs à consulter les descriptions des utilisateurs.
- **DescribeServer**— Autorise les principaux à consulter les descriptions des serveurs.
- **ListUsers**— Accorde aux principaux l'autorisation de répertorier les utilisateurs d'un serveur.

- **ListServers**— Autorise les principaux à répertorier les serveurs du compte.
- **TestIdentityProvider**— Accorde des autorisations aux principaux pour vérifier si le fournisseur d'identité configuré est correctement configuré.
- **ListTagsForResource**— Autorise les principaux à répertorier les balises d'une ressource.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "transfer:DescribeUser",
        "transfer:DescribeServer",
        "transfer:ListUsers",
        "transfer:ListServers",
        "transfer:TestIdentityProvider",
        "transfer:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Transfer Family met à jour les politiques AWS gérées

Consultez les détails des mises à jour apportées aux politiques AWS gérées pour AWS Transfer Family depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS fil d'actualité de la [Historique du document pour AWS Transfer Family](#) page.

Modification	Description	Date
Mise à jour de la documentation	Des sections ont été ajoutées pour chacune des politiques gérées par Transfer Family.	27 janvier 2022

Modification	Description	Date
<u>AWSTransferReadOnlyAccess</u> – Mise à jour d'une politique existante	AWS Transfer Family a ajouté de nouvelles autorisations pour permettre la lecture de la politique AWS Managed Microsoft AD.	30 septembre 2021
AWS Transfer Family a commencé à suivre les modifications	AWS Transfer Family a commencé à suivre les modifications apportées AWS à ses politiques gérées.	15 juin 2021

Résolution des problèmes AWS Transfer Family

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pourriez rencontrer lors de votre utilisation AWS Transfer Family.

Pour les problèmes liés IAM à in Transfer Family, consultez [Résolution des problèmes AWS Transfer Family d'identité et d'accès](#).

Rubriques

- [Résoudre les problèmes des utilisateurs gérés par des services](#)
- [Résoudre les problèmes liés à Amazon API Gateway](#)
- [Résoudre les problèmes liés aux compartiments Amazon S3 chiffrés](#)
- [Résoudre les problèmes d'authentification](#)
- [Résoudre les problèmes liés aux flux de travail gérés](#)
- [Résoudre les problèmes de déchiffrement du flux de travail](#)
- [Résoudre les problèmes liés à Amazon EFS](#)
- [Résoudre les problèmes liés au test de votre fournisseur d'identité](#)
- [Résoudre les problèmes liés à l'ajout de clés d'hôte fiables pour votre connecteur SFTP](#)
- [Résoudre les problèmes de téléchargement de fichiers](#)
- [Résolution des problèmes d'exception ResourceNotFound](#)
- [Résoudre les problèmes liés au SFTP connecteur](#)
- [Résolution des problèmes AS2](#)

Résoudre les problèmes des utilisateurs gérés par des services

Cette section décrit les solutions possibles aux problèmes suivants.

Rubriques

- [Résoudre les problèmes des utilisateurs gérés par le EFS service Amazon](#)
- [Résoudre les problèmes liés à un corps de clé publique trop long](#)
- [Résolution des problèmes : échec de l'ajout de la clé SSH publique](#)

Résoudre les problèmes des utilisateurs gérés par le EFS service Amazon

Description

Vous exécutez la `sftp` commande et l'invite ne s'affiche pas. Le message suivant s'affiche à la place :

```
Couldn't canonicalize: Permission denied
Need cwd
```

Cause

Le rôle de votre AWS Identity and Access Management (IAM) utilisateur n'est pas autorisé à accéder à Amazon Elastic File System (AmazonEFS).

Solution

Augmentez les autorisations liées à la politique pour le rôle de votre utilisateur. Vous pouvez ajouter une politique AWS gérée, telle que `AmazonElasticFileSystemClientFullAccess`.

Résoudre les problèmes liés à un corps de clé publique trop long

Description

Lorsque vous essayez de créer un utilisateur géré par un service, le message d'erreur suivant s'affiche :

```
Failed to create user (1 validation error detected:
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or
equal to 2048)
```

Cause

Vous entrez peut-être une PGP clé pour le corps de la clé publique, mais les clés pour les utilisateurs gérés par des services AWS Transfer Family ne sont pas prises en charge PGP.

Solution

Si la PGP clé est RSA basée, vous pouvez la convertir au PEM format. Par exemple, Ubuntu fournit un outil de conversion ici : <https://manpages.ubuntu.com/manpages/xenial/man1/openpgp2ssh.1.html>

Résolution des problèmes : échec de l'ajout de la clé SSH publique

Description

Lorsque vous essayez d'ajouter une clé publique pour un utilisateur géré par un service, le message d'erreur suivant s'affiche :

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

Cause

Vous essayez peut-être d'importer une clé publique SSH2 formatée, mais les clés publiques formatées AWS Transfer Family ne sont pas prises en charge pour les SSH2 utilisateurs gérés par des services.

Solution

Vous devez convertir la clé au SSH format Open. Ce processus est décrit dans [Convertir une clé SSH2 publique au PEM format](#).

Résoudre les problèmes liés à Amazon API Gateway

Cette section décrit les solutions possibles aux problèmes de API passerelle suivants.

Rubriques

- [Trop d'échecs d'authentification](#)
- [Connexion fermée](#)

Trop d'échecs d'authentification

Description

Lorsque vous essayez de vous connecter à votre serveur à l'aide du protocole de transfert de fichiers Secure Shell (SSH/SFTP), le message d'erreur suivant s'affiche :

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures  
Authentication failed.  
Couldn't read packet: Connection reset by peer
```

Cause

Vous avez peut-être saisi un mot de passe incorrect pour votre utilisateur. Réessayez de saisir le mot de passe correct.

Si le mot de passe est correct, le problème peut être dû à un rôle Amazon Resource Name (ARN) non valide. Pour vérifier que c'est bien le problème, testez le fournisseur d'identité de votre serveur. Si vous recevez une réponse similaire à la suivante, le rôle n'ARNest qu'un espace réservé, comme l'indique la valeur d'ID de rôle de tous les zéros :

```
{
  "Response": "{\"Role\": \"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",
  \"HomeDirectory\": \"\"}",
  "StatusCode": 200,
  "Message": "",
  "Url": "https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/
servers/transfer-server-ID/users/myuser/config"
}
```

Solution

Remplacez le rôle ARN d'espace réservé par un rôle réel autorisé à accéder au serveur.

Pour mettre à jour le rôle

1. Ouvrez la AWS CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Dans le volet de navigation de gauche, choisissez Stacks (Piles).
3. Dans la liste des piles, choisissez votre pile, puis cliquez sur l'onglet Paramètres.
4. Choisissez Mettre à jour. Sur la page Mettre à jour la pile, choisissez Utiliser le modèle actuel, puis Next.
5. `UserRoleArn` Remplacez-le par un rôle ARN disposant des autorisations suffisantes pour accéder à votre serveur Transfer Family.

Note

Pour accorder les autorisations nécessaires, vous pouvez ajouter les politiques gérées `AmazonAPIGatewayAdministrator` et les politiques `AmazonS3FullAccess` gérées à votre rôle.

6. Choisissez Next, puis de nouveau Next. À propos de la révision **stack**page, sélectionnez Je reconnais que cela AWS CloudFormation pourrait créer IAM des ressources, puis choisissez Update stack.

Connexion fermée

Description

Lorsque vous essayez de vous connecter à votre serveur à l'aide du protocole de transfert de fichiers Secure Shell (SSH/SFTP), le message d'erreur suivant s'affiche :

```
Connection closed
```

Cause

L'une des causes possibles de ce problème est que votre rôle de CloudWatch journalisation Amazon n'entretient aucune relation de confiance avec Transfer Family.

Solution

Assurez-vous que le rôle de journalisation du serveur entretient une relation de confiance avec Transfer Family. Pour de plus amples informations, veuillez consulter [Étape 1 : Établir une relation d'approbation](#).

Résoudre les problèmes liés aux compartiments Amazon S3 chiffrés

Description

Vous disposez d'un compartiment Amazon S3 chiffré que vous utilisez comme espace de stockage pour votre serveur Transfer Family. Si vous essayez de télécharger un fichier sur le serveur, le message d'erreur s'affiche `Couldn't close file: Permission denied`.

Et si vous consultez les journaux du serveur, les erreurs suivantes s'affichent :

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13  
ERROR Message="Access denied"
```

Cause

La politique de votre IAM utilisateur n'est pas autorisée à accéder au compartiment chiffré.

Solution

Vous devez spécifier des autorisations supplémentaires dans votre politique pour accorder les autorisations requises AWS Key Management Service (AWS KMS). Pour plus de détails, consultez [Chiffrement des données dans Amazon S3](#).

Résoudre les problèmes d'authentification

Cette section décrit les solutions possibles pour les problèmes d'authentification suivants.

Rubriques

- [Défaillances d'authentification—SSH/SFTP](#)
- [Problème de domaines incompatibles avec Managed AD](#)
- [Problèmes d'authentification divers](#)

Défaillances d'authentification—SSH/SFTP

Description

Lorsque vous essayez de vous connecter à votre serveur à l'aide du protocole de transfert de fichiers Secure Shell (SSH/SFTP), vous recevez un message similaire au suivant :

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
Authentication failed.
```

Note

Si vous utilisez une API passerelle et que vous recevez cette erreur, consultez [Trop d'échecs d'authentification](#).

Cause

Vous n'avez pas ajouté de paire de RSA clés pour votre utilisateur, vous devez donc vous authentifier à l'aide d'un mot de passe.

Solution

Lorsque vous exécutez la `sftp` commande, spécifiez l'option `PubkeyAuthentication=nooption`. Cette option force le système à demander votre mot de passe. Par exemple :

```
sftp -o PubkeyAuthentication=no sftp-user@server-id.server.transfer.region-id.amazonaws.com
```

Problème de domaines incompatibles avec Managed AD

Description

Le domaine d'un utilisateur et le domaine de son groupe doivent correspondre. Ils doivent tous deux se trouver dans le domaine par défaut ou dans le domaine de confiance.

Cause

Si un utilisateur et son groupe ne correspondent pas, l'utilisateur ne peut pas être authentifié par Transfer Family. Si vous testez le fournisseur d'identité de l'utilisateur, vous recevez le message d'erreur `Aucun accès associé trouvé pour les groupes d'utilisateurs`.

Solution

Référez un groupe dans le domaine de l'utilisateur qui correspond au domaine du groupe (par défaut ou approuvé).

Problèmes d'authentification divers

Description

Vous recevez une erreur d'authentification et aucun autre dépannage ne fonctionne

Cause

Vous avez peut-être spécifié une cible pour un répertoire logique contenant une barre oblique initiale ou finale (/).

Solution

Mettez à jour la cible de votre répertoire logique pour vous assurer qu'elle commence par une barre oblique et qu'elle ne contient pas de barre oblique finale. Par exemple, `/DOC-EXAMPLE-BUCKET/images` c'est acceptable, mais `/DOC-EXAMPLE-BUCKET/images/` ne `DOC-EXAMPLE-BUCKET/images` l'est pas.

Résoudre les problèmes liés aux flux de travail gérés

Cette section décrit les solutions possibles aux problèmes de flux de travail suivants.

Rubriques

- [Résoudre les erreurs liées au flux de travail à l'aide d'Amazon CloudWatch](#)
- [Résoudre les erreurs de copie du flux de travail](#)

Résoudre les erreurs liées au flux de travail à l'aide d'Amazon CloudWatch

Description

Si vous rencontrez des problèmes avec vos flux de travail, vous pouvez utiliser Amazon CloudWatch pour en rechercher la cause.

Cause

Il peut y avoir plusieurs causes. Utilisez Amazon CloudWatch Logs pour effectuer des recherches.

Solution

Transfer Family transmet le statut d'exécution du flux de travail dans CloudWatch Logs. Les types d'erreurs de flux de travail suivants peuvent apparaître dans CloudWatch les journaux :

- "type": "StepErrored"
- "type": "ExecutionErrored"
- "type": "ExecutionThrottled"
- "Service failure on starting workflow"

Vous pouvez filtrer les journaux d'exécution de votre flux de travail à l'aide de différentes syntaxes de filtre et de modèle. Par exemple, vous pouvez créer un filtre de journal dans vos CloudWatch journaux pour capturer les journaux d'exécution du flux de travail contenant le ExecutionErroredmessage. Pour plus de détails, consultez les [sections Traitement en temps réel des données de journal avec les abonnements](#) et [Syntaxe des filtres et](#) des modèles dans le guide de l'utilisateur Amazon CloudWatch Logs.

StepErrored

```
2021-10-29T12:57:26.272-05:00
```

```

{"type":"StepErrored","details":
{"errorType":"BAD_REQUEST","errorMessage":"Cannot
tag Efs file","stepType":"TAG","stepName":"successful_tag_step"},
"workflowId":"w-
abcdef01234567890","executionId":"1234abcd-56ef-78gh-90ij-1234klmno567",
"transferDetails":
{"serverId":"s-1234567890abcdef0","username":"lhr","sessionId":"1234567890abcdef0"}}

```

Ici, StepErrored indique qu'une étape du flux de travail a généré une erreur. Dans un seul flux de travail, vous pouvez configurer plusieurs étapes. Cette erreur vous indique à quelle étape l'erreur s'est produite et affiche un message d'erreur. Dans cet exemple particulier, l'étape a été configurée pour étiqueter un fichier ; toutefois, le balisage d'un fichier dans un système de fichiers Amazon EFS n'est pas pris en charge, de sorte que l'étape a généré une erreur.

ExecutionErrored

```

2021-10-29T12:57:26.618-05:00
{"type":"ExecutionErrored","details":{},"workflowId":"w-w-
abcdef01234567890",
"executionId":"1234abcd-56ef-78gh-90ij-1234klmno567","transferDetails":
{"serverId":"s-1234567890abcdef0",
"username":"lhr","sessionId":"1234567890abcdef0"}}

```

Lorsqu'un flux de travail ne peut exécuter aucune étape, il génère un ExecutionErrored message. Par exemple, si vous avez configuré une seule étape dans un flux de travail donné et si l'étape ne peut pas s'exécuter, le flux de travail global échoue.

Exécution limitée

L'exécution est limitée si un flux de travail est déclenché à un rythme supérieur à celui que le système peut supporter. Ce message de journal indique que vous devez ralentir le taux d'exécution des flux de travail. [Si vous ne parvenez pas à réduire le taux d'exécution de votre flux de travail, contactez Contact AWS Support . AWS](#)

Défaillance du service au démarrage du flux de travail

Chaque fois que vous supprimez un flux de travail d'un serveur et que vous le remplacez par un nouveau, ou que vous mettez à jour la configuration du serveur (ce qui a un impact sur le rôle d'exécution d'un flux de travail), vous devez attendre environ 10 minutes avant d'exécuter le nouveau flux de travail. Le serveur Transfer Family met en cache les détails du flux de travail et met 10 minutes au serveur pour actualiser son cache.

En outre, vous devez vous déconnecter de toutes les SFTP sessions actives, puis vous reconnecter après la période d'attente de 10 minutes pour voir les modifications.

Résoudre les erreurs de copie du flux de travail

Description

Si vous exécutez un flux de travail contenant une étape permettant de copier le fichier chargé, le message d'erreur suivant peut s'afficher :

```
{
  "type": "StepErrored", "details": {
    "errorType": "BAD_REQUEST", "errorMessage": "Bad Request (Service: Amazon S3;
    Status Code: 400; Error Code: 400 Bad Request;
    Request ID: request-ID; S3 Extended Request ID: request-ID Proxy: null)",
    "stepType": "COPY", "stepName": "copy-step-name" },
    "workflowId": "workflow-ID",
    "executionId": "execution-ID",
    "transferDetails": {
      "serverId": "server-ID",
      "username": "user-name",
      "sessionId": "session-ID"
    }
  }
}
```

Cause

Le fichier source se trouve dans un compartiment Amazon S3 qui se trouve dans un compartiment différent Région AWS de celui de destination.

Solution

Si vous exécutez un flux de travail qui inclut une étape de copie, assurez-vous que les compartiments source et de destination se trouvent dans les mêmes Région AWS compartiments.

Résoudre les problèmes de déchiffrement du flux de travail

Description

Votre flux de déchiffrement échoue et le message du journal ressemble au suivant :

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "File encryption algorithm not supported with FIPS mode
enabled.",
    "stepType": "DECRYPT",
    "stepName": "step-name"
  },
  "workflowId": "workflow-ID",
  "executionId": "execution-ID",
  "transferDetails": {
    "serverId": "server-ID",
    "username": "user-name",
    "sessionId": "session-ID"
  }
}
```

Cause

Le FIPS mode est activé sur votre serveur Transfer Family et dispose d'une étape de flux de travail de déchiffrement associée. Lorsque vous chiffrez les fichiers avant de les télécharger sur votre serveur Transfer Family, le client de chiffrement peut générer des fichiers chiffrés utilisant des algorithmes de chiffrement symétriques non FIPS approuvés. Dans un tel scénario, le flux de travail n'est pas en mesure de déchiffrer les fichiers. Dans l'exemple suivant, la version 2.4.0 de GnuPG OCB utilise (un mode de chiffrement non FIPS par blocs) pour chiffrer des fichiers : cela entraîne l'échec du flux de travail.

Solution

Vous devez modifier la GPG clé que vous avez utilisée pour chiffrer vos fichiers, puis les rechiffrer. La procédure suivante décrit les étapes à suivre.

Pour modifier vos PGP clés

1. Identifiez la clé que vous devez modifier en exécutant `gpg --list-keys`

Cela renvoie une liste de clés. Les détails de chaque clé sont similaires aux suivants :

```
pub   ed25519 2022-07-07 [SC]
      wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

```
uid          [ultimate] Mary Major <marymajor@example.com>
sub    cv25519 2022-07-07 [E]
```

2. Identifiez la clé que vous souhaitez modifier. Dans l'exemple présenté à l'étape précédente, l'ID est `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.
3. Exécutez `gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`.

Le système répond en fournissant des détails sur le programme GnuPG et la clé spécifiée.

4. À l'`gpg>invite`, entrez `showpref`. Les informations suivantes sont renvoyées :

```
[ultimate] (1). Mary Major <marymajor@example.com>
Cipher: AES256, AES192, AES, 3DES
AEAD: OCB
Digest: SHA512, SHA384, SHA256, SHA224, SHA1
Compression: ZLIB, BZIP2, ZIP, Uncompressed
Features: MDC, AEAD, Keyserver no-modify
```

Notez que les algorithmes préférés enregistrés sur la clé sont répertoriés.

5. Nous voulons modifier la clé pour conserver tous les algorithmes à l'exception de OCB. Exécutez la `setpref` commande en spécifiant tous les algorithmes à conserver :

```
gpg> setpref AES256, AES192, AES, 3DES, SHA512, SHA384, SHA256, SHA224, SHA1, ZLIB,
BZIP2, ZIP, Uncompressed
```

Cela renvoie les informations suivantes :

```
Set preference list to:
Cipher: AES256, AES192, AES, 3DES
AEAD:
Digest: SHA512, SHA384, SHA256, SHA224, SHA1
Compression: ZLIB, BZIP2, ZIP, Uncompressed
Features: MDC, Keyserver no-modify
Really update the preferences? (y/N)
```

6. Entrez `y` pour effectuer la mise à jour, puis entrez votre mot de passe lorsque vous êtes invité à confirmer la modification.
7. Enregistrez les Modifications.

```
gpg> save
```

Avant de réexécuter votre flux de travail de déchiffrement, vous devez rechiffrer vos fichiers à l'aide de la clé modifiée.

Résoudre les problèmes liés à Amazon EFS

Cette section décrit les solutions possibles aux EFS problèmes Amazon suivants.

Rubriques

- [Résoudre les problèmes liés au profil manquant POSIX](#)
- [Résoudre les problèmes liés aux annuaires logiques avec Amazon EFS](#)

Résoudre les problèmes liés au profil manquant POSIX

Description

Si vous utilisez le EFS stockage Amazon pour votre serveur et que vous utilisez un fournisseur d'identité personnalisé, vous devez fournir un POSIX profil à votre AWS Lambda fonction.

Cause

L'une des causes possibles est que les modèles que nous fournissons pour créer une méthode Amazon AWS Lambda API Gateway basée sur des données ne contiennent actuellement aucune POSIX information.

Si vous avez fourni des POSIX informations, le format que vous avez utilisé pour les POSIX fournir n'est peut-être pas correctement analysé par Transfer Family.

Solution

Assurez-vous de fournir un JSON élément à Transfer Family pour le `PosixProfile` paramètre.

Par exemple, si vous utilisez Python, vous pouvez ajouter la ligne suivante où vous analysez le `PosixProfile` paramètre :

```
if PosixProfile:
    response_data["PosixProfile"] = json.loads(PosixProfile)
```

Vous pouvez également ajouter la ligne suivante JavaScript, où les *uid-value* et *gid-value* sont des nombres entiers, égaux ou supérieurs à 0, qui représentent respectivement l'ID utilisateur (UID) et l'ID de groupe (GID) :


```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

Ces exemples de code envoient le PosixProfile paramètre à Transfer Family sous forme d'JSONobjet plutôt que sous forme de chaîne.

De plus AWS Secrets Manager, à l'intérieur, vous devez stocker le PosixProfile paramètre comme suit. Remplacez *your-uid* et *your-gid* par vos valeurs réelles pour le GID etUID.

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

Résoudre les problèmes liés aux annuaires logiques avec Amazon EFS

Description

Si le répertoire personnel de l'utilisateur n'existe pas et que celui-ci exécute une `ls` commande, le système répond comme suit :

```
sftp> ls
remote readdir ("/"): No such file or directory
```

Cause

Si votre serveur Transfer Family utilise AmazonEFS, le répertoire personnel de l'utilisateur doit être créé avec un accès en lecture et en écriture pour que l'utilisateur puisse travailler dans son répertoire de base logique. L'utilisateur ne peut pas créer ce répertoire lui-même, car il n'aurait pas les autorisations nécessaires pour `mkdir` accéder à son répertoire de base logique.

Solution

Un utilisateur disposant d'un accès administratif au répertoire parent doit créer le répertoire de base logique de l'utilisateur.

Résoudre les problèmes liés au test de votre fournisseur d'identité

Description

Si vous testez votre fournisseur d'identité à l'aide de la console ou de l'`TestIdentityProviderAPI` appel, le Response champ est vide. Par exemple :

```
{
  "Response": "{}",
  "StatusCode": 200,
  "Message": ""
}
```

Cause

La cause la plus probable est que l'authentification a échoué en raison d'un nom d'utilisateur ou d'un mot de passe incorrect.

Solution

Assurez-vous que vous utilisez les informations d'identification correctes pour votre utilisateur et mettez à jour le nom d'utilisateur ou le mot de passe, si nécessaire.

Résoudre les problèmes liés à l'ajout de clés d'hôte fiables pour votre connecteur SFTP

Description

Lorsque vous créez ou modifiez un SFTP connecteur et que vous ajoutez une clé d'hôte approuvée, le message d'erreur suivant s'affiche : `Failed to edit connector details (Invalid host key format.)`

Cause

Si vous collez une clé publique correcte, le problème vient peut-être du fait que vous avez inclus la comment partie de la clé. AWS Transfer Family n'accepte pas actuellement la partie commentaire de la clé.

Solution

Supprimez la partie commentaire de la clé lorsque vous la collez dans le champ de texte. Supposons, par exemple, que votre clé ressemble à ce qui suit :

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

Supprimez le texte qui suit les `==` caractères et ne collez que la partie de la touche allant jusqu'au `==`.

```
ssh-rsa AAAA...==
```

Résoudre les problèmes de téléchargement de fichiers

Cette section décrit les solutions possibles aux problèmes de téléchargement de fichiers suivants.

Rubriques

- [Résoudre les erreurs de chargement de fichiers Amazon S3](#)
- [Résoudre les problèmes liés aux noms de fichiers illisibles](#)

Résoudre les erreurs de chargement de fichiers Amazon S3

Description

Lorsque vous tentez de charger un fichier vers le stockage Amazon S3 à l'aide de Transfer Family, le message d'erreur suivant s'affiche : AWS Transfer ne prend pas en charge les écritures à accès aléatoire sur des objets S3.

Cause

Lorsque vous utilisez Amazon S3 pour le stockage de votre serveur, Transfer Family ne prend pas en charge les connexions multiples pour un seul transfert.

Solution

Si votre serveur Transfer Family utilise Amazon S3 pour son stockage, désactivez toutes les options de votre logiciel client qui mentionnent l'utilisation de plusieurs connexions pour un seul transfert.

Résoudre les problèmes liés aux noms de fichiers illisibles

Description

Vous voyez des noms de fichiers corrompus dans certains fichiers que vous avez téléchargés. Les utilisateurs rencontrent parfois des problèmes ou FTP des SFTP transferts qui brouillent certains caractères dans les noms de fichiers, tels que les trémas, les lettres accentuées ou certains scripts, tels que le chinois ou l'arabe.

Cause

Bien que les SFTP protocoles FTP and puissent permettre aux clients de négocier le codage des caractères des noms de fichiers, Amazon S3 et Amazon ne EFS le font pas. Au lieu de cela, ils nécessitent un codage de UTF -8 caractères. Par conséquent, certains caractères ne sont pas rendus correctement.

Solution

Pour résoudre ce problème, vérifiez le codage des caractères du nom de fichier dans votre application cliente et assurez-vous qu'il est défini sur UTF -8.

Résolution des problèmes d'exception **ResourceNotFound**

Description

Vous recevez un message d'erreur indiquant que la ressource est introuvable. Par exemple, si vous exécutez `UpdateServer`, le message d'erreur suivant peut s'afficher :

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:  
Unknown server
```

Cause

Plusieurs raisons peuvent expliquer la réception d'un `ResourceNotFoundException` message. Dans la plupart des cas, la ressource que vous avez spécifiée dans votre API commande n'existe pas. Si vous avez indiqué une ressource existante, la cause la plus probable est que votre région par défaut est différente de celle de votre ressource. Par exemple, si votre région par défaut est `us-east-1` et que votre serveur Transfer Family se trouve dans `us-east-2`, vous recevrez une exception de ressource inconnue.

Pour plus de détails sur la définition d'une région par défaut, voir [Configuration rapide avec aws configure](#).

Solution

Ajoutez un paramètre de région à votre API commande pour spécifier explicitement où trouver une ressource particulière.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

Résoudre les problèmes liés au SFTP connecteur

Cette section décrit les solutions possibles aux problèmes de SFTP connecteur suivants.

Rubriques

- [Échec d'une négociation clé](#)
- [Problèmes de SFTP connexion divers](#)

Échec d'une négociation clé

Description

Vous recevez un message d'erreur indiquant l'échec de la négociation de l'échange de clés. Par exemple :

```
Key exchange negotiation failed due to incompatible host key algorithms.  
Client offered: [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,  
ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256] Server offered: [ssh-rsa]
```

Cause

Cette erreur est due au fait qu'il n'y a aucun chevauchement entre les algorithmes de clé d'hôte pris en charge par le serveur et ceux pris en charge par le connecteur.

Solution

Assurez-vous que le serveur distant prend en charge au moins l'un des algorithmes clés de l'hôte client répertoriés dans le message d'erreur. Pour la liste des algorithmes pris en charge, consultez [SFTPalgorithmes de connexion](#).

Problèmes de SFTP connexion divers

Description

Vous recevez un message d'erreur après l'exécution `StartFileTransfer`, mais vous ne connaissez pas la cause du problème, et seul l'ID du connecteur est renvoyé après l'API appel.

Cause

Cette erreur peut avoir plusieurs causes. Pour résoudre le problème, nous vous recommandons de tester votre connecteur et d'effectuer une recherche dans vos CloudWatch journaux.

Solution

- Testez votre connecteur : voir [Tester un SFTP connecteur](#). Si le test échoue, le système affiche un message d'erreur basé sur la raison de l'échec du test. Cette section décrit comment tester votre connecteur depuis la console ou à l'aide du [TestConnection](#) API commande.
- Afficher CloudWatch les journaux de votre connecteur : voir [Exemples d'entrées de journal pour les SFTP connecteurs](#). Cette rubrique fournit des exemples d'entrées de journal de SFTP connecteurs, ainsi que la convention de dénomination pour vous aider à trouver les journaux appropriés.

Résolution des problèmes AS2

Les messages d'erreur et les conseils de dépannage pour les serveurs compatibles avec la déclaration d'applicabilité 2 (AS2) sont décrits ici : [Codes d'erreur AS2](#)

API référence

Les sections suivantes décrivent les appels AWS Transfer Family API de service, les types de données, les paramètres et les erreurs.

Rubriques

- [Bienvenue sur le AWS Transfer Family API](#)
- [Actions](#)
- [Types de données](#)
- [Faire des demandes d'API](#)
- [Paramètres communs](#)
- [Erreurs courantes](#)

Bienvenue sur le AWS Transfer Family API

AWS Transfer Family est un service de transfert sécurisé que vous pouvez utiliser pour transférer des fichiers vers et depuis le stockage Amazon Simple Storage Service (Amazon S3) via les protocoles suivants :

- Protocole de transfert de fichiers Secure Shell (SSHSFTP)
- Protocole de transfert de fichiers sécurisé (FTPS)
- Protocole de transfert de fichiers (FTP)
- Déclaration d'applicabilité (2) AS2

Les protocoles de transfert de fichiers sont utilisés dans les flux de travail d'échange de données dans différents secteurs tels que les services financiers, les soins de santé, la publicité et le commerce de détail, entre autres. AWS Transfer Family simplifie la migration des flux de transfert de fichiers vers AWS.

Pour utiliser le AWS Transfer Family service, vous instanciez un serveur dans la AWS région de votre choix. Vous pouvez créer le serveur, répertorier les serveurs disponibles, mettre à jour et supprimer des serveurs. Le serveur est l'entité qui demande des opérations sur les fichiers AWS Transfer Family. Les serveurs ont un certain nombre de propriétés importantes. Le serveur est une instance nommée identifiée par un identifiant `ServerId` attribué par le système. Vous pouvez éventuellement

attribuer un nom d'hôte à un serveur, voire un nom d'hôte personnalisé. Le service facture tous les serveurs instanciés (même les serveurs OFFLINE) et la quantité de données transférées.

Les utilisateurs doivent être connus du serveur qui demande les opérations sur les fichiers. Un utilisateur identifié par son nom d'utilisateur est affecté à un serveur. Les noms d'utilisateur sont utilisés pour authentifier les demandes. Un serveur ne peut avoir qu'une seule méthode d'authentification : `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA`, ou `API_GATEWAY`.

Vous pouvez utiliser l'un des types de fournisseurs d'identité suivants pour authentifier les utilisateurs :

- En `SERVICE_MANAGED` effet, une clé SSH publique est stockée avec les propriétés de l'utilisateur sur un serveur. Un utilisateur peut avoir une ou plusieurs clés SSH publiques enregistrées pour la méthode `SERVICE_MANAGED` d'authentification. Lorsqu'un client demande une opération de fichier pour une `SERVICE_MANAGED` méthode, le client fournit le nom d'utilisateur et la clé SSH privée, qui sont authentifiés, et l'accès est fourni.
- Vous pouvez gérer l'authentification et l'accès des utilisateurs avec vos groupes Microsoft Active Directory en sélectionnant la méthode `AWS_DIRECTORY_SERVICE` d'authentification.
- Vous pouvez vous connecter à un fournisseur d'identité personnalisé en utilisant AWS Lambda. Choisissez la méthode `AWS_LAMBDA` d'authentification.
- Vous pouvez également authentifier les demandes d'utilisateurs à l'aide d'une méthode d'authentification personnalisée qui fournit à la fois l'authentification et l'accès aux utilisateurs. Cette méthode repose sur Amazon API Gateway pour utiliser votre API appel de votre fournisseur d'identité afin de valider les demandes des utilisateurs. Cette méthode est appelée « `API_GATEWAY` dans les API appels » et « personnalisée » dans la console. Vous pouvez utiliser cette méthode personnalisée pour authentifier les utilisateurs par rapport à un service d'annuaire, une paire nom/mot de passe de base de données ou un autre mécanisme.

Les utilisateurs se voient attribuer une politique établissant une relation de confiance entre eux et un compartiment Amazon S3. Ils peuvent avoir accès à tout ou partie d'un compartiment. Pour qu'un serveur agisse au nom d'un utilisateur, il doit hériter de la relation de confiance de l'utilisateur. Un rôle AWS Identity and Access Management (IAM) contenant la relation de confiance est créé, et une `AssumeRole` action est affectée à ce rôle. Le serveur peut alors effectuer des opérations sur les fichiers comme s'il s'agissait de l'utilisateur.

Les utilisateurs dont les propriétés de home répertoire sont définies verront ce répertoire (ou dossier) servir de cible et de source pour les opérations sur les fichiers. Quand aucun répertoire home n'est défini, le répertoire `root` du compartiment devient le répertoire de destination.

Les serveurs, les utilisateurs et les rôles sont tous identifiés par leur Amazon Resource Name (ARN). Vous pouvez attribuer des balises, qui sont des paires clé-valeur, aux entités dotées d'un ARN. Les balises sont des métadonnées qui peuvent être utilisées pour regrouper ou rechercher ces entités. Les balises s'avèrent utiles dans le domaine de la comptabilité, notamment.

Les conventions suivantes sont respectées dans les formats AWS Transfer Family d'identification :

- Les valeurs `ServerId` se présentent sous la forme `s-01234567890abcdef`.
- Les valeurs `SshPublicKeyId` se présentent sous la forme `key-01234567890abcdef`.

Les formats Amazon Resource Name (ARN) se présentent sous la forme suivante :

- Pour les serveurs, ARNs utilisez le formulaire `arn:aws:transfer:region:account-id:server/server-id`.

Un exemple de serveur ARN est `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

- Pour les utilisateurs, ARNs utilisez le formulaire `arn:aws:transfer:region:account-id:user/server-id/username`.

Par exemple : `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

DNS Les entrées (points de terminaison) utilisées sont les suivantes :

- API Les points de terminaison prennent la forme `transfer.region.amazonaws.com`.
- Les points de terminaison de serveur se présentent sous la forme `server.transfer.region.amazonaws.com`.

Pour obtenir la liste des points de terminaison Transfer Family par AWS région, consultez les [AWS Transfer Family points de terminaison et les quotas](#) dans le. Références générales AWS

Cette référence API d'interface AWS Transfer Family contient la documentation d'une interface de programmation que vous pouvez utiliser pour gérer AWS Transfer Family. La structure du document de référence se présente comme suit :

- Pour la liste alphabétique des API actions, voir [Actions](#).
- Pour la liste alphabétique des types de données, voir [Data Types](#).
- Pour consulter la liste des paramètres de requête courants, reportez-vous à la page [Paramètres courants](#).
- Pour la description des codes d'erreur, consultez la page [Erreurs courantes](#).

 Tip

Plutôt que d'exécuter une commande, vous pouvez utiliser le `--generate-cli-skeleton` paramètre avec n'importe quel API appel pour générer et afficher un modèle de paramètre. Vous pouvez ensuite utiliser le modèle généré pour le personnaliser et l'utiliser comme entrée dans une commande ultérieure. Pour plus de détails, voir [Générer et utiliser un fichier squelette de paramètres](#).

Actions

Les actions suivantes sont prises en charge :

- [CreateAccess](#)
- [CreateAgreement](#)
- [CreateConnector](#)
- [CreateProfile](#)
- [CreateServer](#)
- [CreateUser](#)
- [CreateWorkflow](#)
- [DeleteAccess](#)
- [DeleteAgreement](#)
- [DeleteCertificate](#)
- [DeleteConnector](#)

- [DeleteHostKey](#)
- [DeleteProfile](#)
- [DeleteServer](#)
- [DeleteSshPublicKey](#)
- [DeleteUser](#)
- [DeleteWorkflow](#)
- [DescribeAccess](#)
- [DescribeAgreement](#)
- [DescribeCertificate](#)
- [DescribeConnector](#)
- [DescribeExecution](#)
- [DescribeHostKey](#)
- [DescribeProfile](#)
- [DescribeSecurityPolicy](#)
- [DescribeServer](#)
- [DescribeUser](#)
- [DescribeWorkflow](#)
- [ImportCertificate](#)
- [ImportHostKey](#)
- [ImportSshPublicKey](#)
- [ListAccesses](#)
- [ListAgreements](#)
- [ListCertificates](#)
- [ListConnectors](#)
- [ListExecutions](#)
- [ListHostKeys](#)
- [ListProfiles](#)
- [ListSecurityPolicies](#)
- [ListServers](#)
- [ListTagsForResource](#)

- [ListUsers](#)
- [ListWorkflows](#)
- [SendWorkflowStepState](#)
- [StartFileTransfer](#)
- [StartServer](#)
- [StopServer](#)
- [TagResource](#)
- [TestConnection](#)
- [TestIdentityProvider](#)
- [UntagResource](#)
- [UpdateAccess](#)
- [UpdateAgreement](#)
- [UpdateCertificate](#)
- [UpdateConnector](#)
- [UpdateHostKey](#)
- [UpdateProfile](#)
- [UpdateServer](#)
- [UpdateUser](#)

CreateAccess

Utilisé par les administrateurs pour choisir les groupes du répertoire qui doivent avoir accès au chargement et au téléchargement de fichiers via les protocoles activés à l'aide de AWS Transfer Family. Par exemple, un Microsoft Active Directory peut contenir 50 000 utilisateurs, mais seule une petite partie d'entre eux peut avoir besoin de pouvoir transférer des fichiers vers le serveur. Un administrateur peut utiliser cette CreateAccess option pour limiter l'accès au groupe approprié d'utilisateurs qui ont besoin de cette capacité.

Syntaxe de la requête

```
{
  "ExternalId": "string",
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "Role": "string",
  "ServerId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ExternalId

Identifiant unique requis pour identifier des groupes spécifiques au sein de votre annuaire.

Les utilisateurs du groupe que vous associez ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family. Si vous connaissez le nom du groupe, vous pouvez afficher les SID valeurs en exécutant la commande suivante sous Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties  
* | Select SamAccountName, ObjectSid
```

Dans cette commande, remplacez YourGroupName par le nom de votre groupe Active Directory.

L'expression régulière utilisée pour valider ce paramètre est une chaîne de caractères composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez également inclure des traits de soulignement ou l'un des caractères suivants : =, . @ : /-

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : S-1-[\d-]+

Obligatoire : oui

HomeDirectory

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de HomeDirectory est /bucket_name/home/mydirectory.

Note

Le paramètre HomeDirectory est uniquement utilisé si HomeDirectoryType est défini sur la valeur PATH.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : (| / . *)

Obligatoire : non

[HomeDirectoryMappings](#)

Des mappages de répertoires logiques qui spécifient quels EFS chemins et clés Amazon S3 ou Amazon doivent être visibles par votre utilisateur et comment vous souhaitez les rendre visibles. Vous devez spécifier la Target paire Entry et, qui Entry indique comment le chemin est rendu visible et Target correspond au EFS chemin Amazon S3 ou Amazon réel. Si vous spécifiez uniquement une cible, elle est affichée telle quelle. Vous devez également vous assurer que votre rôle AWS Identity and Access Management (IAM) donne accès aux chemins d'accèsTarget. Cette valeur ne peut être définie que si elle HomeDirectoryType est définie sur LOGICAL.

Voici un exemple de Target paire Entry et.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

Dans la plupart des cas, vous pouvez utiliser cette valeur au lieu de la politique de session pour verrouiller votre utilisateur dans le répertoire de base désigné (« chroot »). Pour ce faire, vous pouvez Entry définir / et Target définir la valeur du HomeDirectory paramètre.

Voici un exemple de Target paire Entry et pourchroot.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Type : tableau d'objets [HomeDirectoryMapEntry](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 50 000 articles.

Obligatoire : non

[HomeDirectoryType](#)

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez surPATH, l'utilisateur verra le bucket Amazon S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez surLOGICAL, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

Note

Dans `HomeDirectoryType` l'affirmative `LOGICAL`, vous devez fournir des mappages à l'aide du `HomeDirectoryMappings` paramètre. Si, par contre, `HomeDirectoryType` c'est le cas `PATH`, vous fournissez un chemin absolu à l'aide du `HomeDirectory` paramètre. Vous ne pouvez pas avoir les deux `HomeDirectory` et `HomeDirectoryMappings` dans votre modèle.

Type : String

Valeurs valides : `PATH` | `LOGICAL`

Obligatoire : non

Policy

Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même rôle AWS Identity and Access Management (IAM) pour plusieurs utilisateurs. Cette politique limite l'accès d'un utilisateur à certaines parties de son compartiment Amazon S3. Les variables que vous pouvez utiliser à l'intérieur de cette politique incluent `${Transfer:UserName}`, `${Transfer:HomeDirectory}` et `${Transfer:HomeBucket}`.

Note

Cette politique s'applique uniquement lorsque le domaine de `ServerId` est Amazon S3. Amazon EFS n'utilise pas de politiques de session.

Pour les politiques de session, AWS Transfer Family stocke la politique sous forme de JSON blob, au lieu du nom de ressource Amazon (ARN) de la politique. Vous enregistrez la politique sous forme de JSON blob et vous la transmettez dans l'`Policy` argument.

Pour obtenir un exemple de politique de session, veuillez consulter la rubrique [Exemple de politique de session](#).

Pour plus d'informations, reportez-vous [AssumeRole](#) à la section `AWS Security Token Service API` Référence.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

PosixProfile

L'POSIX identité complète, y compris l'ID utilisateur (Uid), l'ID de groupe (Gid) et tout groupe secondaire IDs (SecondaryGids), qui contrôle l'accès de vos utilisateurs à vos systèmes de EFS fichiers Amazon. Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Type : objet [PosixProfile](#)

Obligatoire : non

Role

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : oui

ServerId

Identifiant unique attribué par le système pour une instance de serveur. Il s'agit du serveur spécifique auquel vous avez ajouté votre utilisateur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "ExternalId": "string",  
  "ServerId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[ExternalId](#)

L'identifiant externe du groupe dont les utilisateurs ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : S-1-[\d-]+

[ServerId](#)

Identifiant du serveur auquel l'utilisateur est rattaché.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)

- [AWS SDKpour Ruby V3](#)

CreateAgreement

Crée un accord. Un accord est un accord de partenariat commercial bilatéral, ou partenariat, entre un AWS Transfer Family serveur et un AS2 processus. L'accord définit la relation de transfert de fichiers et de messages entre le serveur et le AS2 processus. Pour définir un accord, Transfer Family combine un serveur, un profil local, un profil de partenaire, un certificat et d'autres attributs.

Le partenaire est identifié par le `PartnerProfileId`, et le AS2 processus est identifié par le `LocalProfileId`.

Syntaxe de la requête

```
{
  "AccessRole": "string",
  "BaseDirectory": "string",
  "Description": "string",
  "LocalProfileId": "string",
  "PartnerProfileId": "string",
  "ServerId": "string",
  "Status": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte le JSON format des données suivantes.

[AccessRole](#)

Les connecteurs sont utilisés pour envoyer des fichiers en utilisant le SFTP protocole AS2 or. Pour le rôle d'accès, indiquez le nom de ressource Amazon (ARN) du AWS Identity and Access Management rôle à utiliser.

Pour AS2 connecteurs

AvecAS2, vous pouvez envoyer des fichiers en appelant `StartFileTransfer` et en spécifiant les chemins des fichiers dans le paramètre de requête, `SendFilePaths`. Nous utilisons le répertoire parent du fichier (par exemple, `--send-file-paths /bucket/dir/file.txt`, le répertoire parent est `/bucket/dir/`) pour stocker temporairement un fichier de AS2 message traité, le stocker MDN lorsque nous le recevons du partenaire et écrire un JSON fichier final contenant les métadonnées pertinentes de la transmission. Ainsi, le `AccessRole` doit fournir un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la requête `StartFileTransfer`. En outre, vous devez fournir un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer avec `StartFileTransfer`.

Si vous utilisez l'authentification de base pour votre AS2 connecteur, le rôle d'accès nécessite `secretsmanager:GetSecretValue` autorisation d'accès au secret. Si le secret est chiffré à l'aide d'une clé gérée par le client au lieu de la clé AWS gérée dans Secrets Manager, le rôle doit également disposer d'une `kms:Decrypt` autorisation pour cette clé.

Pour SFTP connecteurs

Assurez-vous que le rôle d'accès fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande. Assurez-vous également que le rôle fournit `secretsmanager:GetSecretValue` autorisation de AWS Secrets Manager.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : oui

BaseDirectory

Le répertoire de destination (dossier) pour les fichiers transférés à l'aide du AS2 protocole.

Un exemple de `BaseDirectory` est `/DOC-EXAMPLE-BUCKET/home/mydirectory`.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `(|/.*)`

Obligatoire : oui

Description

Un nom ou une brève description pour identifier l'accord.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : $[\backslash p\{Graph\}]^+$

Obligatoire : non

LocalProfileId

Identifiant unique pour le profil AS2 local.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : $p-([0-9a-f]\{17\})$

Obligatoire : oui

PartnerProfileId

Un identifiant unique pour le profil de partenaire utilisé dans l'accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : $p-([0-9a-f]\{17\})$

Obligatoire : oui

ServerId

Identifiant unique attribué par le système pour une instance de serveur. Il s'agit du serveur spécifique utilisé par le contrat.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

Status

État de l'accord. L'accord peut être l'un ACTIVE ou l'autre INACTIVE.

Type : String

Valeurs valides : ACTIVE | INACTIVE

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des accords.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
  "AgreementId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

AgreementId

L'identifiant unique de l'accord. Utilisez cet identifiant pour supprimer ou mettre à jour un accord, ainsi que pour tout autre API appel nécessitant que vous spécifiez l'identifiant de l'accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : a - ([0-9a-f] {17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant crée un accord et renvoie l'ID de l'accord.

```
aws transfer create-agreement --server-id s-021345abcdef6789 --local-profile-id p-1234567890abcdef0 --partner-profile-id p-abcdef01234567890 --base-folder /DOC-EXAMPLE-BUCKET/AS2-files --access-role arn:aws:iam::111122223333:role/AS2-role
```

Exemple de réponse

L'API appelle renvoie l'identifiant de l'accord pour le nouvel accord.

```
{
  "AgreementId": "a-11112222333344444"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues 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](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour JavaScript V3](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

CreateConnector

Crée le connecteur, qui capture les paramètres d'une connexion pour le SFTP protocole AS2 or. En AS2 effet, le connecteur est nécessaire pour envoyer des fichiers à un AS2 serveur hébergé en externe. En SFTP effet, le connecteur est nécessaire pour envoyer des fichiers à un SFTP serveur ou recevoir des fichiers d'un SFTP serveur. Pour plus de détails sur les connecteurs, reportez-vous aux [sections Configuration des AS2 connecteurs](#) et [Création de SFTP connecteurs](#).

Note

Vous devez spécifier exactement un objet de configuration : for AS2 (As2Config) ou SFTP (SftpConfig).

Syntaxe de la requête

```
{
  "AccessRole": "string",
  "As2Config": {
    "BasicAuthSecretId": "string",
    "Compression": "string",
    "EncryptionAlgorithm": "string",
    "LocalProfileId": "string",
    "MdnResponse": "string",
    "MdnSigningAlgorithm": "string",
    "MessageSubject": "string",
    "PartnerProfileId": "string",
    "SigningAlgorithm": "string"
  },
  "LoggingRole": "string",
  "SftpConfig": {
    "TrustedHostKeys": [ "string" ],
    "UserSecretId": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Url": "string"
}
```

```
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[AccessRole](#)

Les connecteurs sont utilisés pour envoyer des fichiers en utilisant le SFTP protocole AS2 or. Pour le rôle d'accès, indiquez le nom de ressource Amazon (ARN) du AWS Identity and Access Management rôle à utiliser.

Pour AS2 connecteurs

Avec AS2, vous pouvez envoyer des fichiers en appelant `StartFileTransfer` et en spécifiant les chemins des fichiers dans le paramètre de requête, `SendFilePaths`. Nous utilisons le répertoire parent du fichier (par exemple, `--send-file-paths /bucket/dir/file.txt`, le répertoire parent est `/bucket/dir/`) pour stocker temporairement un fichier de AS2 message traité, le stocker MDN lorsque nous le recevons du partenaire et écrire un JSON fichier final contenant les métadonnées pertinentes de la transmission. Ainsi, le `AccessRole` doit fournir un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la requête `StartFileTransfer`. En outre, vous devez fournir un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer avec `StartFileTransfer`.

Si vous utilisez l'authentification de base pour votre AS2 connecteur, le rôle d'accès nécessite `secretsmanager:GetSecretValue` autorisation d'accès au secret. Si le secret est chiffré à l'aide d'une clé gérée par le client au lieu de la clé AWS gérée dans Secrets Manager, le rôle doit également disposer d'une `kms:Decrypt` autorisation pour cette clé.

Pour SFTP connecteurs

Assurez-vous que le rôle d'accès fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande. Assurez-vous également que le rôle fournit `secretsmanager:GetSecretValue` autorisation de AWS Secrets Manager.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : oui

[As2Config](#)

Structure contenant les paramètres d'un objet AS2 connecteur.

Type : objet [As2ConnectorConfig](#)

Obligatoire : non

[LoggingRole](#)

Nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un connecteur d'activer la CloudWatch journalisation des événements Amazon S3. Lorsque cette option est configurée, vous pouvez consulter l'activité du connecteur dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

[SftpConfig](#)

Structure contenant les paramètres d'un objet SFTP connecteur.

Type : objet [SftpConnectorConfig](#)

Obligatoire : non

[Tags](#)

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des connecteurs. Les balises sont des métadonnées attachées aux connecteurs pour n'importe quel usage.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Url

Celui URL du partenaire AS2 ou du SFTP point final.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 255.

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "ConnectorId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

ConnectorId

Identifiant unique du connecteur, renvoyé une fois l'API appel réussi.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c - ([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant crée un AS2 connecteur. Dans la commande, remplacez les éléments comme suit :

- `url`: fournissez URL le AS2 serveur du partenaire commercial.
- `your-IAM-role-for-bucket-access`: un IAM rôle qui a accès au compartiment Amazon S3 que vous utilisez pour stocker vos fichiers.

- Utilisez le ARN pour votre rôle de journalisation, qui inclut votre Compte AWS identifiant.
- Indiquez le chemin d'un fichier contenant les paramètres de configuration du AS2 connecteur. L'objet de configuration AS2 du connecteur est décrit dans [As2. ConnectorConfig](#)

```
// Listing for testAs2Config.json
{
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "partner-profile-id",
  "MdnResponse": "SYNC",
  "Compression": "ZLIB",
  "EncryptionAlgorithm": "AES256_CBC",
  "SigningAlgorithm": "SHA256",
  "MdnSigningAlgorithm": "DEFAULT",
  "MessageSubject": "Your Message Subject"
}
```

```
aws transfer create-connector --url "http://partner-as2-server-url" \
  --access-role your-IAM-role-for-bucket-access \
  --logging-role arn:aws:iam::your-account-id:role/service-role/
AWSTransferLoggingAccess \
  --as2-config file://path/to/testAS2Config.json
```

Exemple

L'exemple suivant crée un SFTP connecteur. Dans la commande, remplacez les éléments comme suit :

- `sftp-server-url`: indiquez URL le SFTP serveur avec lequel vous échangez des fichiers.
- `your-IAM-role-for-bucket-access`: un IAM rôle qui a accès au compartiment Amazon S3 que vous utilisez pour stocker vos fichiers.
- Utilisez le ARN pour votre rôle de journalisation, qui inclut votre Compte AWS identifiant.
- Indiquez le chemin d'un fichier contenant les paramètres de configuration du SFTP connecteur. L'objet de configuration du SFTP connecteur est décrit dans [SftpConnectorConfig](#).

```
// Listing for testSFTPConfig.json
```



```
{
  "UserSecretId": "arn:aws:secretsmanager:us-east-2:123456789012:secret:aws/transfer/
example-username-key",
  "TrustedHostKeys": [
    "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
  ]
}
```

```
aws transfer create-connector --url "sftp://sftp-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess
\
--sftp-config file:///path/to/testSFTPConfig.json
```

Exemple

L'API appelle renvoie l'ID du nouveau connecteur.

Exemple de réponse

```
{
  "ConnectorId": "a-11112222333344444"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

CreateProfile

Crée le profil local ou partenaire à utiliser pour les AS2 transferts.

Syntaxe de la requête

```
{
  "As2Id": "string",
  "CertificateIds": [ "string" ],
  "ProfileType": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

As2Id

As2Id s'agit du AS2-name, tel que défini dans le [RFC4130](#). Pour les transferts entrants, il s'agit de l'AS2-Fromen-tête des AS2 messages envoyés par le partenaire. Pour les connecteurs sortants, il s'agit de l'AS2-Toen-tête des AS2 messages envoyés au partenaire à l'aide de l'StartFileTransferAPIopération. Cet identifiant ne peut pas inclure d'espaces.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : [\p{Print}\s]*

Obligatoire : oui

CertificateIds

Un tableau d'identifiants pour les certificats importés. Vous utilisez cet identifiant pour travailler avec des profils et des profils de partenaires.

Type : tableau de chaînes

Contraintes de longueur : longueur fixe de 22.

Modèle : `cert-([0-9a-f]{17})`

Obligatoire : non

ProfileType

Détermine le type de profil à créer :

- Spécifiez LOCAL pour créer un profil local. Un profil local représente l'organisation ou le groupe de serveurs Transfer Family AS2 activé.
- Spécifiez PARTNER pour créer un profil de partenaire. Un profil de partenaire représente une organisation distante, externe à Transfer Family.

Type : String

Valeurs valides : LOCAL | PARTNER

Obligatoire : oui

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher AS2 des profils.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{  
  "ProfileId": "string"  
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

ProfileId

Identifiant unique du AS2 profil, renvoyé une fois l'API appel réussi.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant crée un profil et renvoie son ID.

Les certificats IDs sont créés lors de l'exécution `import-certificate`, un pour le certificat de signature et un pour le certificat de chiffrement.

```
aws transfer create-profile --as2-id MYCORP --certificate-ids c-abcdefgh123456hijk  
c-987654aaaa321bbbb
```

Exemple de réponse

L'API appelle renvoie l'ID de profil du nouveau profil.

```
{  
  "ProfileId": "p-11112222333344444"  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues 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](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour JavaScript V3](#)

- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

CreateServer

Instancie un serveur virtuel de scalabilité automatique en se basant sur le protocole de transfert de fichiers sélectionné dans AWS. Lorsque vous effectuez des mises à jour de votre serveur compatible avec le protocole de transfert de fichiers ou lorsque vous travaillez avec des utilisateurs, utilisez la propriété `ServerId` générée par le service qui est attribuée au serveur nouvellement créé.

Syntaxe de la requête

```
{
  "Certificate": "string",
  "Domain": "string",
  "EndpointDetails": {
    "AddressAllocationIds": [ "string" ],
    "SecurityGroupIds": [ "string" ],
    "SubnetIds": [ "string" ],
    "VpcEndpointId": "string",
    "VpcId": "string"
  },
  "EndpointType": "string",
  "HostKey": "string",
  "IdentityProviderDetails": {
    "DirectoryId": "string",
    "Function": "string",
    "InvocationRole": "string",
    "SftpAuthenticationMethods": "string",
    "Url": "string"
  },
  "IdentityProviderType": "string",
  "LoggingRole": "string",
  "PostAuthenticationLoginBanner": "string",
  "PreAuthenticationLoginBanner": "string",
  "ProtocolDetails": {
    "As2Transports": [ "string" ],
    "PassiveIp": "string",
    "SetStatOption": "string",
    "TlsSessionResumptionMode": "string"
  },
  "Protocols": [ "string" ],
  "S3StorageOptions": {
    "DirectoryListingOptimization": "string"
  },
  "SecurityPolicyName": "string",
```



```

"StructuredLogDestinations": [ "string" ],
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"WorkflowDetails": {
  "OnPartialUpload": [
    {
      "ExecutionRole": "string",
      "WorkflowId": "string"
    }
  ],
  "OnUpload": [
    {
      "ExecutionRole": "string",
      "WorkflowId": "string"
    }
  ]
}
}

```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[Certificate](#)

Le nom de ressource Amazon (ARN) du certificat AWS Certificate Manager (ACM). Obligatoire lorsque `Protocol`s est défini sur `FTPS`.

Pour demander un nouveau certificat public, consultez la section [Demander un certificat public](#) dans le guide de AWS Certificate Manager l'utilisateur.

Pour importer un certificat existant dans ACM, consultez la section [Importation de certificats ACM dans](#) le guide de AWS Certificate Manager l'utilisateur.

Pour demander un certificat privé à utiliser FTPS via des adresses IP privées, consultez la section [Demander un certificat privé](#) dans le guide de AWS Certificate Manager l'utilisateur.

Les certificats avec les algorithmes de chiffrement et les tailles de clés suivants sont pris en charge :

- 2048 bits RSA (_2048) RSA
- 4096 bits (_4096RSA) RSA
- Elliptic Prime Curve 256 octets (EC_prime256v1)
- Elliptic Prime Curve 384 octets (EC_secp384r1)
- Elliptic Prime Curve 521 octets (EC_secp521r1)

 Note

Le certificat doit être un SSL TLS certificat/X.509 version 3 valide avec une FQDN adresse IP spécifiée et des informations sur l'émetteur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 1600.

Obligatoire : non

Domain

Domaine du système de stockage utilisé pour les transferts de fichiers. Deux domaines sont disponibles : Amazon Simple Storage Service (Amazon S3) et Amazon Elastic File System (AmazonEFS). La valeur par défaut est S3.

 Note

Une fois le serveur créé, le domaine ne peut pas être modifié.

Type : String

Valeurs valides : S3 | EFS

Obligatoire : non

EndpointDetails

Les paramètres de point de terminaison du cloud privé virtuel (VPC) configurés pour votre serveur. Lorsque vous hébergez votre point de terminaison dans votre environnement VPC, vous

pouvez le rendre accessible uniquement aux ressources qu'il contient, ou vous pouvez associer des adresses IP élastiques et rendre votre point de terminaison accessible aux clients via Internet. Vos groupes VPC de sécurité par défaut sont automatiquement attribués à votre terminal.

Type : objet [EndpointDetails](#)

Obligatoire : non

[EndpointType](#)

Le type de point de terminaison que vous souhaitez que votre serveur utilise. Vous pouvez choisir de rendre le point de terminaison de votre serveur accessible au public (PUBLIC) ou de l'héberger dans votre VPC. Avec un point de terminaison hébergé dans un VPC, vous pouvez restreindre l'accès à votre serveur et à ses ressources uniquement VPC ou choisir de le rendre accessible à Internet en y attachant directement des adresses IP élastiques.

Note

Après le 19 mai 2021, vous ne pourrez plus créer de serveur à l'aide de `EndpointType=VPC_ENDPOINT` in your Compte AWS si votre compte ne l'a pas déjà fait avant le 19 mai 2021. Si vous avez déjà créé des serveurs avec `EndpointType=VPC_ENDPOINT` in Compte AWS your le 19 mai 2021 ou avant, vous ne serez pas concerné. Après cette date, utilisez `EndpointType =VPC`.

Pour de plus amples informations, veuillez consulter [Cessation de l'utilisation de _ VPC ENDPOINT](#).

Il est recommandé d'utiliser VPC comme élément `EndpointType`. Avec ce type de point de terminaison, vous avez la possibilité d'associer directement jusqu'à trois IPv4 adresses élastiques (BYOIP incluses) au point de terminaison de votre serveur et d'utiliser des groupes de VPC sécurité pour restreindre le trafic en fonction de l'adresse IP publique du client. Cela n'est pas possible si `EndpointType` est défini sur `VPC_ENDPOINT`.

Type : String

Valeurs valides : PUBLIC | VPC | VPC_ENDPOINT

Obligatoire : non

HostKey

La RSAECDSA, ou clé ED25519 privée à utiliser pour votre SFTP serveur activé. Vous pouvez ajouter plusieurs clés hôtes, au cas où vous souhaiteriez faire pivoter les clés, ou disposer d'un ensemble de clés actives utilisant différents algorithmes.

Utilisez la commande suivante pour générer une clé de RSA 2048 bits sans phrase secrète :

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

Utilisez une valeur minimale de 2 048 pour l'-boption. Vous pouvez créer une clé plus forte en utilisant 3072 ou 4096.

Utilisez la commande suivante pour générer une clé de ECDSA 256 bits sans phrase secrète :

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

Les valeurs valides pour l'-boption pour ECDSA sont 256, 384 et 521.

Utilisez la commande suivante pour générer une ED25519 clé sans phrase secrète :

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

Pour toutes ces commandes, vous pouvez les remplacer my-new-server-key par une chaîne de votre choix.

Important

Si vous ne prévoyez pas de migrer des utilisateurs existants d'un serveur SFTP compatible existant vers un nouveau serveur, ne mettez pas à jour la clé d'hôte. La modification accidentelle de la clé d'hôte d'un serveur peut être perturbante.

Pour plus d'informations, voir [Mettre à jour les clés d'hôte pour votre SFTP serveur activé](#) dans le Guide de l' AWS Transfer Family utilisateur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Obligatoire : non

[IdentityProviderDetails](#)

Obligatoire lorsque `IdentityProviderType` le paramètre est défini sur `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` ou `API_GATEWAY`. Accepte un tableau contenant toutes les informations requises pour utiliser un répertoire `AWS_DIRECTORY_SERVICE` ou invoquer une authentification fournie par le client API, y compris la API passerelle. URL Facultatif lorsque `IdentityProviderType` est défini sur `SERVICE_MANAGED`.

Type : objet [IdentityProviderDetails](#)

Obligatoire : non

[IdentityProviderType](#)

Le mode d'authentification pour un serveur. La valeur par défaut est `SERVICE_MANAGED`, ce qui vous permet de stocker et d'accéder aux informations d'identification des utilisateurs au sein du AWS Transfer Family service.

`AWS_DIRECTORY_SERVICE` À utiliser pour fournir un accès aux groupes Active Directory AWS Directory Service for Microsoft Active Directory ou à Microsoft Active Directory dans votre environnement local ou à l' AWS aide d'AD Connector. Cette option exige également que vous indiquiez un ID de répertoire en utilisant le paramètre `IdentityProviderDetails`.

Utilisez la valeur `API_GATEWAY` à intégrer au fournisseur d'identité de votre choix. Le `API_GATEWAY` paramètre vous oblige à fournir un point de terminaison Amazon API Gateway URL à appeler pour l'authentification à l'aide du `IdentityProviderDetails` paramètre.

Utilisez la `AWS_LAMBDA` valeur pour utiliser directement une AWS Lambda fonction comme fournisseur d'identité. Si vous choisissez cette valeur, vous devez spécifier la ARN fonction Lambda dans le `Function` paramètre du type de `IdentityProviderDetails` données.

Type : String

Valeurs valides : `SERVICE_MANAGED` | `API_GATEWAY` | `AWS_DIRECTORY_SERVICE` | `AWS_LAMBDA`

Obligatoire : non

[LoggingRole](#)

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un serveur d'activer la CloudWatch journalisation Amazon pour Amazon S3 ou

AmazonEFSevents. Lorsque cette option est configurée, vous pouvez consulter l'activité des utilisateurs dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Modèle : (|arn:.*role/\S+)

Obligatoire : non

PostAuthenticationLoginBanner

Spécifie une chaîne à afficher lorsque les utilisateurs se connectent à un serveur. Cette chaîne s'affiche une fois l'utilisateur authentifié.

Note

Le SFTP protocole ne prend pas en charge les bannières d'affichage après authentification.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Modèle : [\x09-\x0D\x20-\x7E]*

Obligatoire : non

PreAuthenticationLoginBanner

Spécifie une chaîne à afficher lorsque les utilisateurs se connectent à un serveur. Cette chaîne est affichée avant que l'utilisateur ne s'authentifie. Par exemple, la bannière suivante affiche des informations sur l'utilisation du système :

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Modèle : `[\x09-\x0D\x20-\x7E]*`

Obligatoire : non

[ProtocolDetails](#)

Les paramètres du protocole qui sont configurés pour votre serveur.

- Pour indiquer le mode passif (pour FTP et FTPS protocoles), utilisez le `PassiveIp` paramètre. Entrez une seule adresse à quatre points, telle que IPv4 l'adresse IP externe d'un pare-feu, d'un routeur ou d'un équilibreur de charge.
- Pour ignorer l'erreur qui est générée lorsque le client tente d'utiliser la commande SETSTAT sur un fichier que vous téléchargez vers un compartiment Amazon S3, utilisez le paramètre `SetStatOption`. Pour que le AWS Transfer Family serveur ignore la SETSTAT commande et télécharge les fichiers sans avoir à apporter de modifications à votre SFTP client, définissez la valeur sur `ENABLE_NO_OP`. Si vous définissez le `SetStatOption` paramètre sur `ENABLE_NO_OP`, Transfer Family génère une entrée de journal dans Amazon CloudWatch Logs, afin que vous puissiez déterminer à quel moment le client passe un SETSTAT appel.
- Pour déterminer si votre AWS Transfer Family serveur reprend les sessions récemment négociées via un identifiant de session unique, utilisez le `TlsSessionResumptionMode` paramètre.
- `As2Transports` indique le mode de transport des AS2 messages. Actuellement, seul HTTP est pris en charge.

Type : objet [ProtocolDetails](#)

Obligatoire : non

[Protocols](#)

Spécifie le ou les protocoles de transfert de fichiers sur lesquels votre client de protocole de transfert de fichiers peut se connecter au point de terminaison de votre serveur. Les protocoles disponibles sont :

- SFTP(Secure Shell (SSH) File Transfer Protocol) : transfert de fichiers effectué SSH
- FTPS(Protocole de transfert de fichiers sécurisé) : transfert de fichiers avec TLS cryptage
- FTP (Protocole de transfert de fichiers) : Transfert de fichiers non chiffré
- AS2(Déclaration d'applicabilité 2) : utilisé pour le transport de données structurées business-to-business

 Note

- Si vous le sélectionnez FTPS, vous devez choisir un certificat stocké dans AWS Certificate Manager (ACM) qui est utilisé pour identifier votre serveur lorsque des clients s'y connectent FTPS.
- Si Protocol comprend FTP ou FTPS, EndpointType doit être défini sur VPC, et IdentityProviderType sur AWS_DIRECTORY_SERVICE, AWS_LAMBDA ou API_GATEWAY.
- Si Protocol inclut FTP, alors AddressAllocationIds ne peut pas être associé.
- Si Protocol est uniquement défini sur SFTP, EndpointType peut être défini sur PUBLIC, et IdentityProviderType peut être défini comme l'un des types d'identité pris en charge : SERVICE_MANAGED, AWS_DIRECTORY_SERVICE, AWS_LAMBDA ou API_GATEWAY.
- Si Protocol inclut AS2, alors le EndpointType doit être VPC, et le domaine doit être Amazon S3.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Valeurs valides : SFTP | FTP | FTPS | AS2

Obligatoire : non

S3StorageOptions

Spécifie si les performances de vos annuaires Amazon S3 sont optimisées ou non. Par défaut, l'option est désactivée.

Par défaut, les mappages du répertoire de base ont la valeur TYPE de DIRECTORY.

Si vous activez cette option, vous devrez alors définir explicitement la valeur sur HomeDirectoryMapEntry Type FILE si vous souhaitez qu'un mappage ait une cible de fichier.

Type : objet S3StorageOptions

Obligatoire : non

SecurityPolicyName

Spécifie le nom de la politique de sécurité attachée au serveur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 100.

Modèle : TransferSecurityPolicy-.*

Obligatoire : non

[StructuredLogDestinations](#)

Spécifie les groupes de journaux auxquels les journaux de votre serveur sont envoyés.

Pour spécifier un groupe de journaux, vous devez fournir le correspondant ARN à un groupe de journaux existant. Dans ce cas, le format du groupe de logs est le suivant :

```
arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*
```

Par exemple, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Si vous avez déjà spécifié un groupe de journaux pour un serveur, vous pouvez l'effacer, et donc désactiver la journalisation structurée, en fournissant une valeur vide pour ce paramètre dans un `update-server` appel. Par exemple :

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

Type : tableau de chaînes

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : arn:\S+

Obligatoire : non

[Tags](#)

Paires clé-valeur qui peuvent être utilisées pour regrouper et explorer les serveurs.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

[WorkflowDetails](#)

Spécifie l'ID du flux de travail à attribuer et le rôle d'exécution utilisé pour exécuter le flux de travail.

En plus d'un flux de travail à exécuter lorsqu'un fichier est complètement chargé, `WorkflowDetails` peut également contenir un ID de flux de travail (et un rôle d'exécution) pour un flux de travail à exécuter lors d'un chargement partiel. Un téléchargement partiel se produit lorsque la session du serveur se déconnecte alors que le fichier est toujours en cours de téléchargement.

Type : objet [WorkflowDetails](#)

Obligatoire : non

Syntaxe de la réponse

```
{  
  "ServerId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[ServerId](#)

Identifiant attribué par le service au serveur créé.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

HTTPCode de statut : 400

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant crée un nouveau serveur à l'aide d'un VPC_ENDPOINT.

Exemple de demande

```
{
  "EndpointType": "VPC",
  "EndpointDetails": ...,
  "HostKey": "Your RSA private key",
  "IdentityProviderDetails": "IdentityProvider",
  "IdentityProviderType": "SERVICE_MANAGED",
  "LoggingRole": "CloudWatchLoggingRole",
  "Tags": [
    {
      "Key": "Name",
      "Value": "MyServer"
    }
  ]
}
```

Exemple

Voici un exemple de réponse pour cet API appel.

Exemple de réponse

```
{
  "ServerId": "s-01234567890abcdef"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDK pour .NET](#)
- [AWS SDK pour C++](#)

- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

CreateUser

Crée un utilisateur et l'associe à un serveur existant compatible avec le protocole de transfert de fichiers. Vous pouvez uniquement créer et associer les utilisateurs avec des serveurs pour lesquels `IdentityProviderType` est défini sur `SERVICE_MANAGED`. À l'aide des paramètres pour `CreateUser`, vous pouvez spécifier le nom d'utilisateur, définir le répertoire de base, stocker la clé publique de l'utilisateur et attribuer le rôle de l'utilisateur AWS Identity and Access Management (IAM). Vous pouvez également ajouter une politique de session et attribuer les métadonnées avec des balises qui peuvent être utilisées pour regrouper et rechercher des utilisateurs.

Syntaxe de la requête

```
{
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "Role": "string",
  "ServerId": "string",
  "SshPublicKeyBody": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "UserName": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[HomeDirectory](#)

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de HomeDirectory est `/bucket_name/home/mydirectory`.

Note

Le paramètre HomeDirectory est uniquement utilisé si HomeDirectoryType est défini sur la valeur PATH.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : (`|/.*`)

Obligatoire : non

[HomeDirectoryMappings](#)

Des mappages de répertoires logiques qui spécifient quels EFS chemins et clés Amazon S3 ou Amazon doivent être visibles par votre utilisateur et comment vous souhaitez les rendre visibles. Vous devez spécifier la Target paire Entry et, qui Entry indique comment le chemin est rendu visible et Target correspond au EFS chemin Amazon S3 ou Amazon réel. Si vous spécifiez uniquement une cible, elle est affichée telle quelle. Vous devez également vous assurer que votre rôle AWS Identity and Access Management (IAM) donne accès aux chemins d'accèsTarget. Cette valeur ne peut être définie que si elle HomeDirectoryType est définie sur LOGICAL.

Voici un exemple de Target paire Entry et.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

Dans la plupart des cas, vous pouvez utiliser cette valeur au lieu de la politique de session pour verrouiller votre utilisateur dans le répertoire de base désigné (« chroot »). Pour ce faire, vous pouvez Entry définir / et Target définir la valeur que l'utilisateur doit voir pour son répertoire personnel lorsqu'il se connecte.

Voici un exemple de Target paire Entry et pourchroot.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Type : tableau d'objets [HomeDirectoryMapEntry](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 50 000 articles.

Obligatoire : non

[HomeDirectoryType](#)

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez surPATH, l'utilisateur verra le bucket Amazon S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez surLOGICAL, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

Note

Dans HomeDirectoryType l'affirmativeLOGICAL, vous devez fournir des mappages à l'aide du HomeDirectoryMappings paramètre. Si, par contre, HomeDirectoryType c'est le casPATH, vous fournissez un chemin absolu à l'aide du HomeDirectory paramètre. Vous ne pouvez pas avoir les deux HomeDirectory et HomeDirectoryMappings dans votre modèle.

Type : String

Valeurs valides : PATH | LOGICAL

Obligatoire : non

[Policy](#)

Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même rôle AWS Identity and Access Management (IAM) pour plusieurs utilisateurs. Cette politique limite

l'accès d'un utilisateur à certaines parties de son compartiment Amazon S3. Les variables que vous pouvez utiliser à l'intérieur de cette politique incluent `${Transfer:UserName}`, `${Transfer:HomeDirectory}` et `${Transfer:HomeBucket}`.

 Note

Cette politique s'applique uniquement lorsque le domaine de `ServerId` est Amazon S3. Amazon EFS n'utilise pas de politiques de session.

Pour les politiques de session, AWS Transfer Family stocke la politique sous forme de JSON blob, au lieu du nom de ressource Amazon (ARN) de la politique. Vous enregistrez la politique sous forme de JSON blob et vous la transmettez dans l'`PolicyArgument`. Pour obtenir un exemple de politique de session, veuillez consulter la rubrique [Exemple de politique de session](#).

Pour plus d'informations, consultez le [AssumeRole](#) document de API référence du service AWS de jetons de sécurité.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

[PosixProfile](#)

Spécifie l'POSIX identité complète, y compris l'ID utilisateur (`Uid`), l'ID de groupe (`Gid`) et tout groupe secondaire IDs (`SecondaryGids`), qui contrôle l'accès de vos utilisateurs à vos systèmes de EFS fichiers Amazon. Les POSIX autorisations définies sur les fichiers et les répertoires d'Amazon EFS déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Type : objet [PosixProfile](#)

Obligatoire : non

[Role](#)

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment

Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : oui

ServerId

Identifiant unique attribué par le système pour une instance de serveur. Il s'agit du serveur spécifique auquel vous avez ajouté votre utilisateur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

Obligatoire : oui

SshPublicKeyBody

Partie publique de la clé Secure Shell (SSH) utilisée pour authentifier l'utilisateur auprès du serveur.

Les trois éléments de format de clé SSH publique standard sont `<key type><body base64>`, et un facultatif `<comment>`, avec des espaces entre chaque élément.

AWS Transfer Family accepte RSAECDSA, et ED25519 clés.

- Pour RSA les clés, le type de clé est `ssh-rsa`.
- Pour ED25519 les clés, le type de clé est `ssh-ed25519`.
- Pour ECDSA les clés, le type de clé est soit `ecdsa-sha2-nistp256` `ecdsa-sha2-nistp384`, soit `ecdsa-sha2-nistp521`, selon la taille de la clé que vous avez générée.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des utilisateurs. Les balises sont des métadonnées associées aux utilisateurs pour différents motifs.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

UserName

Chaîne unique qui identifie un utilisateur et est associée à un `ServerId`. Ce nom d'utilisateur doit comporter au minimum 3 caractères et au maximum 100 caractères. Les caractères suivants sont valides : a-z, A-Z, 0-9, trait de soulignement '_', tiret '-', point '.', et arobase « @ ». Le nom d'utilisateur ne peut pas commencer par un trait d'union, un point ou un arobase.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "ServerId": "string",
  "UserName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

ServerId

Identifiant du serveur auquel l'utilisateur est rattaché.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

UserName

Chaîne unique qui identifie un utilisateur de Transfer Family.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : [\w][\w@.-]{2,99}

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

Pour créer un utilisateur, vous pouvez d'abord enregistrer les paramètres dans un JSON fichier, par exemple `createUserParameters`, puis exécuter la commande `create-userAPI`.

```
{
  "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
  "HomeDirectoryType": "PATH",
  "Role": "arn:aws:iam::111122223333:role/bob-role",
  "ServerId": "s-1111aaaa2222bbbb3",
  "SshPublicKeyBody": "ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA...
bobusa@mycomputer.us-east-1.amazon.com",
  "UserName": "bobusa-API"
}
```

Exemple de demande

```
aws transfer create-user --cli-input-json file://createUserParameters
```

Exemple de réponse

```
{
  "ServerId": "s-1111aaaa2222bbbb3",
  "UserName": "bobusa-API"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

CreateWorkflow

Vous permet de créer un flux de travail avec des étapes spécifiées et des détails d'étape que le flux de travail appelle une fois le transfert de fichiers terminé. Après avoir créé un flux de travail, vous pouvez associer le flux de travail créé à n'importe quel serveur de transfert en spécifiant le champ `workflow-details` dans les opérations `CreateServer` et `UpdateServer`.

Syntaxe de la requête

```
{
  "Description": "string",
  "OnExceptionSteps": [
    {
      "CopyStepDetails": {
        "DestinationFileLocation": {
          "EfsFileLocation": {
            "FileSystemId": "string",
            "Path": "string"
          },
          "S3FileLocation": {
            "Bucket": "string",
            "Key": "string"
          }
        },
        "Name": "string",
        "OverwriteExisting": "string",
        "SourceFileLocation": "string"
      },
      "CustomStepDetails": {
        "Name": "string",
        "SourceFileLocation": "string",
        "Target": "string",
        "TimeoutSeconds": number
      },
      "DecryptStepDetails": {
        "DestinationFileLocation": {
          "EfsFileLocation": {
            "FileSystemId": "string",
            "Path": "string"
          },
          "S3FileLocation": {
            "Bucket": "string",
            "Key": "string"
          }
        }
      }
    }
  ]
}
```

```

    }
  },
  "Name": "string",
  "OverwriteExisting": "string",
  "SourceFileLocation": "string",
  "Type": "string"
},
"DeleteStepDetails": {
  "Name": "string",
  "SourceFileLocation": "string"
},
"TagStepDetails": {
  "Name": "string",
  "SourceFileLocation": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
},
"Type": "string"
}
],
"Steps": [
  {
    "CopyStepDetails": {
      "DestinationFileLocation": {
        "EfsFileLocation": {
          "FileSystemId": "string",
          "Path": "string"
        },
        "S3FileLocation": {
          "Bucket": "string",
          "Key": "string"
        }
      },
      "Name": "string",
      "OverwriteExisting": "string",
      "SourceFileLocation": "string"
    },
    "CustomStepDetails": {
      "Name": "string",
      "SourceFileLocation": "string",

```



```

    "Target": "string",
    "TimeoutSeconds": number
  },
  "DecryptStepDetails": {
    "DestinationFileLocation": {
      "EfsFileLocation": {
        "FileSystemId": "string",
        "Path": "string"
      },
      "S3FileLocation": {
        "Bucket": "string",
        "Key": "string"
      }
    },
    "Name": "string",
    "OverwriteExisting": "string",
    "SourceFileLocation": "string",
    "Type": "string"
  },
  "DeleteStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string"
  },
  "TagStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  },
  "Type": "string"
}
],
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
]
}

```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[Description](#)

Description textuelle du flux de travail.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : [`\w-`]*

Obligatoire : non

[OnExceptionSteps](#)

Spécifie les étapes (actions) à suivre en cas d'erreur lors de l'exécution du flux de travail.

Note

Pour les étapes personnalisées, la fonction Lambda doit renvoyer FAILURE au rappel pour API lancer les étapes d'exception. De plus, si le Lambda n'envoie pas SUCCESS avant son expiration, les étapes d'exception sont exécutées.

Type : tableau d'objets [WorkflowStep](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 8 articles.

Obligatoire : non

[Steps](#)

Spécifie les détails des étapes qui se trouvent dans le flux de travail spécifié.

TYPE Spécifie laquelle des actions suivantes est entreprise pour cette étape.

- **COPY** : copier le fichier à un autre emplacement.
- **CUSTOM**- Effectuez une étape personnalisée avec une AWS Lambda fonction cible.

- **DECRYPT** : déchiffrer un fichier chiffré avant d'être chargé.
- **DELETE** : supprimer le fichier.
- **TAG** : ajouter une balise au fichier.

 Note

Actuellement, la copie et le balisage ne sont pris en charge que sur S3.

Pour l'emplacement des fichiers, vous spécifiez soit le compartiment et la clé Amazon S3, soit l'ID et le chemin du système de EFS fichiers Amazon.

Type : tableau d'objets [WorkflowStep](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 8 articles.

Obligatoire : oui

[Tags](#)

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des flux de travail. Les balises sont des métadonnées associées aux flux de travail pour différents motifs.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{  
  "WorkflowId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

HTTPCode de statut : 400

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

Vous pouvez enregistrer les informations relatives aux étapes du flux de travail dans un fichier texte, puis utiliser ce fichier pour créer un flux de travail, comme dans l'exemple suivant. L'exemple suivant suppose que vous avez enregistré les étapes de votre flux de travail dans *example-file.json* (dans le même dossier à partir duquel vous exécutez la commande), et que vous souhaitez créer le flux de travail dans la région Virginie du Nord (us-east-1).

```
aws transfer create-workflow --description "example workflow from a file" --steps
file://example-file.json --region us-east-1
```

```
// Example file containing workflow steps
[
  {
    "Type": "TAG",
    "TagStepDetails": {
      "Name": "TagStep",
      "Tags": [
        {
          "Key": "name",
          "Value": "testTag"
        }
      ]
    }
  },
  {
    "Type": "COPY",
    "CopyStepDetails": {
      "Name": "CopyStep",
      "DestinationFileLocation": {
        "S3FileLocation": {
          "Bucket": "DOC-EXAMPLE-BUCKET",
          "Key": "DOC-EXAMPLE-KEY/"
        }
      }
    }
  }
]
```

```
        },
        "OverwriteExisting": "TRUE",
        "SourceFileLocation": "${original.file}"
    }
},
{
    "Type": "DELETE",
    "DeleteStepDetails": {
        "Name": "DeleteStep",
        "SourceFileLocation": "${original.file}"
    }
}
]
```

Exemple

L'CreateWorkflowappel renvoie l'ID du nouveau flux de travail.

Exemple de réponse

```
{
  "WorkflowId": "w-1234abcd5678efghi"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteAccess

Permet de supprimer l'accès spécifié dans les ExternalID paramètres ServerID et.

Syntaxe de la requête

```
{  
  "ExternalId": "string",  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ExternalId

Identifiant unique requis pour identifier des groupes spécifiques au sein de votre annuaire. Les utilisateurs du groupe que vous associez ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family. Si vous connaissez le nom du groupe, vous pouvez afficher les SID valeurs en exécutant la commande suivante sous Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties  
* | Select SamAccountName,ObjectSid
```

Dans cette commande, remplacez YourGroupNamepar le nom de votre groupe Active Directory.

L'expression régulière utilisée pour valider ce paramètre est une chaîne de caractères composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez également inclure des traits de soulignement ou l'un des caractères suivants : =, . @ : /-

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : S-1-[\d-]+

Obligatoire : oui

ServerId

Identifiant unique attribué par le système à un serveur auquel cet utilisateur est assigné.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f] {17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteAgreement

Supprimez l'accord spécifié dans le document fourni `AgreementId`.

Syntaxe de la requête

```
{
  "AgreementId": "string",
  "ServerId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[AgreementId](#)

Identifiant unique pour l'accord. Cet identifiant est renvoyé lorsque vous créez un accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : a - ([0-9a-f]{17})

Obligatoire : oui

[ServerId](#)

L'identifiant du serveur associé à l'accord que vous êtes en train de supprimer.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)

- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteCertificate

Supprime le certificat spécifié dans le `CertificateId` paramètre.

Syntaxe de la requête

```
{  
  "CertificateId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

CertificateId

Identifiant de l'objet de certificat que vous êtes en train de supprimer.

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : `cert-([0-9a-f]{17})`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteConnector

Supprime le connecteur spécifié dans le document fourni `ConnectorId`.

Syntaxe de la requête

```
{  
  "ConnectorId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ConnectorId

Identifiant unique du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c - ([0-9a-f]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteHostKey

Supprime la clé d'hôte spécifiée dans le `HostKeyId` paramètre.

Syntaxe de la requête

```
{  
  "HostKeyId": "string",  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[HostKeyId](#)

Identifiant de la clé d'hôte que vous êtes en train de supprimer.

Type : String

Contraintes de longueur : longueur fixe de 25.

Modèle : `hostkey-[0-9a-f]{17}`

Obligatoire : oui

[ServerId](#)

Identifiant du serveur qui contient la clé d'hôte que vous supprimez.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteProfile

Supprime le profil spécifié dans le `ProfileId` paramètre.

Syntaxe de la requête

```
{  
  "ProfileId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ProfileId

Identifiant du profil que vous êtes en train de supprimer.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteServer

Supprime le serveur compatible avec le protocole de transfert de fichiers que vous spécifiez.

Aucune réponse ne résulte de cette opération.

Syntaxe de la requête

```
{  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ServerId

Identifiant unique attribué par le système à une instance de serveur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

HTTPCode de statut : 400

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant supprime un serveur.

Exemple de demande

```
{
  "ServerId": "s-01234567890abcdef"
}
```

Exemple

En cas de succès, rien n'est renvoyé.

Exemple de réponse

```
{  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteSshPublicKey

Supprime la clé publique Secure Shell (SSH) d'un utilisateur.

Syntaxe de la requête

```
{  
  "ServerId": "string",  
  "SshPublicKeyId": "string",  
  "UserName": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ServerId

Identifiant unique attribué par le système pour une instance de serveur compatible avec le protocole de transfert de fichiers à laquelle l'utilisateur est assigné.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

SshPublicKeyId

Identifiant unique utilisé pour faire référence à la SSH clé spécifique de votre utilisateur.

Type : String

Contraintes de longueur : longueur fixe de 21.

Modèle : key-[0-9a-f]{17}

Obligatoire : oui

UserName

Chaîne unique qui identifie un utilisateur dont la clé publique est supprimée.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant supprime la clé SSH publique d'un utilisateur.

Exemple de demande

```
{
  "ServerId": "s-01234567890abcdef",
  "SshPublicKeyId": "MyPublicKey",
  "UserName": "my_user"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteUser

Supprime l'utilisateur appartenant à un serveur compatible avec le protocole de transfert de fichiers que vous spécifiez.

Aucune réponse n'est renvoyée suite à cette opération.

Note

Lorsque vous supprimez un utilisateur d'un serveur, ses informations sont perdues.

Syntaxe de la requête

```
{
  "ServerId": "string",
  "UserName": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ServerId

Identifiant unique attribué par le système pour une instance de serveur à laquelle l'utilisateur est assigné.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

UserName

Chaîne unique qui identifie un utilisateur en cours de suppression d'un serveur.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant supprime un utilisateur de Transfer Family.

Exemple de demande

```
{
  "ServerId": "s-01234567890abcdef",
  "UserNames": "my_user"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DeleteWorkflow

Supprime le flux de travail spécifié.

Syntaxe de la requête

```
{  
  "WorkflowId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

HTTPCode de statut : 400

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeAccess

Décrit l'accès attribué au serveur compatible avec le protocole de transfert de fichiers spécifique, tel qu'identifié par ses `ServerId` propriétés et ses `ExternalId`.

La réponse de cet appel renvoie les propriétés de l'accès associé à la `ServerId` valeur spécifiée.

Syntaxe de la requête

```
{  
  "ExternalId": "string",  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ExternalId

Identifiant unique requis pour identifier des groupes spécifiques au sein de votre annuaire.

Les utilisateurs du groupe que vous associez ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family. Si vous connaissez le nom du groupe, vous pouvez afficher les SID valeurs en exécutant la commande suivante sous Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties  
* | Select SamAccountName, ObjectSid
```

Dans cette commande, remplacez `YourGroupName` par le nom de votre groupe Active Directory.

L'expression régulière utilisée pour valider ce paramètre est une chaîne de caractères composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez également inclure des traits de soulignement ou l'un des caractères suivants : `=`, `.`, `@` : `/-`

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : S-1-[\d-]+

Obligatoire : oui

ServerId

Identifiant unique attribué par le système à un serveur auquel cet accès est attribué.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{
  "Access": {
    "ExternalId": "string",
    "HomeDirectory": "string",
    "HomeDirectoryMappings": [
      {
        "Entry": "string",
        "Target": "string",
        "Type": "string"
      }
    ],
    "HomeDirectoryType": "string",
    "Policy": "string",
    "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
    },
    "Role": "string"
  },
  "ServerId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Access

Identifiant externe du serveur auquel l'accès est rattaché.

Type : objet [DescribedAccess](#)

ServerId

Identifiant unique attribué par le système à un serveur auquel cet accès est attribué.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f] {17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeAgreement

Décrit l'accord identifié par le `AgreementId`.

Syntaxe de la requête

```
{  
  "AgreementId": "string",  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

AgreementId

Identifiant unique pour l'accord. Cet identifiant est renvoyé lorsque vous créez un accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : a - ([0-9a-f]{17})

Obligatoire : oui

ServerId

L'identifiant du serveur associé à l'accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{
  "Agreement": {
    "AccessRole": "string",
    "AgreementId": "string",
    "Arn": "string",
    "BaseDirectory": "string",
    "Description": "string",
    "LocalProfileId": "string",
    "PartnerProfileId": "string",
    "ServerId": "string",
    "Status": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Agreement

Les détails de l'accord spécifié, renvoyés sous forme d'`DescribedAgreement` objet.

Type : objet [DescribedAgreement](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeCertificate

Décrit le certificat identifié par leCertificateId.

Syntaxe de la requête

```
{  
  "CertificateId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

CertificateId

Un tableau d'identifiants pour les certificats importés. Vous utilisez cet identifiant pour travailler avec des profils et des profils de partenaires.

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : cert-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "Certificate": {  
    "ActiveDate": number,  
    "Arn": "string",  
    "Certificate": "string",  
    "CertificateChain": "string",  
    "CertificateId": "string",  
    "Description": "string",  
    "InactiveDate": number,  
  }
```

```
"NotAfterDate": number,
"NotBeforeDate": number,
"Serial": "string",
"Status": "string",
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"Type": "string",
"Usage": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Certificate

Les détails du certificat spécifié, renvoyés sous forme d'objet.

Type : objet [DescribedCertificate](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeConnector

Décrit le connecteur identifié par ConnectorId.

Syntaxe de la requête

```
{  
  "ConnectorId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ConnectorId

Identifiant unique du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "Connector": {  
    "AccessRole": "string",  
    "Arn": "string",  
    "As2Config": {  
      "BasicAuthSecretId": "string",  
      "Compression": "string",  
      "EncryptionAlgorithm": "string",  
      "LocalProfileId": "string",  
      "MdnResponse": "string",
```

```

    "MdnSigningAlgorithm": "string",
    "MessageSubject": "string",
    "PartnerProfileId": "string",
    "SigningAlgorithm": "string"
  },
  "ConnectorId": "string",
  "LoggingRole": "string",
  "ServiceManagedEgressIpAddresses": [ "string" ],
  "SftpConfig": {
    "TrustedHostKeys": [ "string" ],
    "UserSecretId": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Url": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Connector

Structure contenant les détails du connecteur.

Type : objet [DescribedConnector](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeExecution

Vous pouvez l'utiliser `DescribeExecution` pour vérifier les détails de l'exécution du flux de travail spécifié.

Note

Cet API appel renvoie uniquement les détails des flux de travail en cours.

Si vous fournissez un ID pour une exécution qui n'est pas en cours, ou si l'exécution ne correspond pas à l'ID de flux de travail spécifié, vous recevez une `ResourceNotFound` exception.

Syntaxe de la requête

```
{
  "ExecutionId": "string",
  "WorkflowId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte le JSON format des données suivantes.

ExecutionId

Identifiant unique pour l'exécution d'un flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 36.

Modèle : `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatoire : oui

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Obligatoire : oui

Syntaxe de la réponse

```

{
  "Execution": {
    "ExecutionId": "string",
    "ExecutionRole": "string",
    "InitialFileLocation": {
      "EfsFileLocation": {
        "FileSystemId": "string",
        "Path": "string"
      },
      "S3FileLocation": {
        "Bucket": "string",
        "Etag": "string",
        "Key": "string",
        "VersionId": "string"
      }
    },
    "LoggingConfiguration": {
      "LoggingRole": "string",
      "LogGroupName": "string"
    },
    "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
    },
    "Results": {
      "OnExceptionSteps": [
        {
          "Error": {

```

```

        "Message": "string",
        "Type": "string"
    },
    "Outputs": "string",
    "StepType": "string"
}
],
"Steps": [
    {
        "Error": {
            "Message": "string",
            "Type": "string"
        },
        "Outputs": "string",
        "StepType": "string"
    }
]
},
"ServiceMetadata": {
    "UserDetails": {
        "ServerId": "string",
        "SessionId": "string",
        "UserName": "string"
    }
},
"Status": "string"
},
"WorkflowId": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Execution

Structure qui contient les détails de l'exécution du flux de travail.

Type : objet [DescribedExecution](#)

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeHostKey

Renvoie les détails de la clé d'hôte spécifiée par le `HostKeyId` et `ServerId`.

Syntaxe de la requête

```
{  
  "HostKeyId": "string",  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[HostKeyId](#)

Identifiant de la clé d'hôte que vous souhaitez décrire.

Type : String

Contraintes de longueur : longueur fixe de 25.

Modèle : `hostkey-[0-9a-f]{17}`

Obligatoire : oui

[ServerId](#)

Identifiant du serveur qui contient la clé d'hôte que vous souhaitez décrire.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "HostKey": {
    "Arn": "string",
    "DateImported": number,
    "Description": "string",
    "HostKeyFingerprint": "string",
    "HostKeyId": "string",
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "Type": "string"
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[HostKey](#)

Renvoie les détails de la clé d'hôte spécifiée.

Type : objet [DescribedHostKey](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeProfile

Renvoie les détails du profil spécifié par leProfileId.

Syntaxe de la requête

```
{  
  "ProfileId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ProfileId

Identifiant du profil que vous souhaitez décrire.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "Profile": {  
    "Arn": "string",  
    "As2Id": "string",  
    "CertificateIds": [ "string" ],  
    "ProfileId": "string",  
    "ProfileType": "string",  
    "Tags": [  
      {  
        "Key": "string",  
        "Value": "string"  
      }  
    ]  
  }  
}
```



```
}  
  ]  
}  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Profile

Les détails du profil spécifié, renvoyés sous forme d'objet.

Type : objet [DescribedProfile](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeSecurityPolicy

Décrit la politique de sécurité attachée à votre serveur compatible avec le protocole de transfert de fichiers. La réponse contient une description des propriétés de la politique de sécurité. Pour plus d'informations sur les politiques de sécurité, consultez la section [Utilisation des politiques de sécurité](#).

Syntaxe de la requête

```
{  
  "SecurityPolicyName": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[SecurityPolicyName](#)

Spécifie le nom de la politique de sécurité attachée au serveur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 100.

Modèle : TransferSecurityPolicy-.*

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "SecurityPolicy": {  
    "Fips": boolean,  
    "SecurityPolicyName": "string",  
    "SshCiphers": [ "string" ],  
    "SshKexs": [ "string" ],  
    "SshMacs": [ "string" ],  
    "TlsCiphers": [ "string" ]  
  }  
}
```

```
}  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[SecurityPolicy](#)

Tableau contenant les propriétés de la politique de sécurité.

Type : objet [DescribedSecurityPolicy](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple de commande suivant prend le nom de la politique de sécurité comme argument et renvoie les algorithmes correspondant à la politique de sécurité spécifiée.

Exemple de demande

```
aws transfer describe-security-policy --security-policy-name "TransferSecurityPolicy-FIPS-2023-05"
```

Exemple de réponse

```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

```
}  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeServer

Décrit un serveur compatible avec le protocole de transfert de fichiers que vous spécifiez en transmettant le paramètre. `ServerId`

La réponse contient une description des propriétés d'un serveur. Lorsque vous définissez `EndpointType` sur `VPC`, la réponse contiendra le `EndpointDetails`.

Syntaxe de la requête

```
{  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ServerId

Identifiant unique attribué par le système à un serveur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "Server": {  
    "Arn": "string",  
    "As2ServiceManagedEgressIpAddresses": [ "string" ],  
    "Certificate": "string",  
    "Domain": "string",  
    "EndpointDetails": {
```

```

    "AddressAllocationIds": [ "string" ],
    "SecurityGroupIds": [ "string" ],
    "SubnetIds": [ "string" ],
    "VpcEndpointId": "string",
    "VpcId": "string"
  },
  "EndpointType": "string",
  "HostKeyFingerprint": "string",
  "IdentityProviderDetails": {
    "DirectoryId": "string",
    "Function": "string",
    "InvocationRole": "string",
    "SftpAuthenticationMethods": "string",
    "Url": "string"
  },
  "IdentityProviderType": "string",
  "LoggingRole": "string",
  "PostAuthenticationLoginBanner": "string",
  "PreAuthenticationLoginBanner": "string",
  "ProtocolDetails": {
    "As2Transports": [ "string" ],
    "PassiveIp": "string",
    "SetStatOption": "string",
    "TlsSessionResumptionMode": "string"
  },
  "Protocols": [ "string" ],
  "S3StorageOptions": {
    "DirectoryListingOptimization": "string"
  },
  "SecurityPolicyName": "string",
  "ServerId": "string",
  "State": "string",
  "StructuredLogDestinations": [ "string" ],
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "UserCount": number,
  "WorkflowDetails": {
    "OnPartialUpload": [
      {
        "ExecutionRole": "string",

```



```
        "WorkflowId": "string"
      }
    ],
    "OnUpload": [
      {
        "ExecutionRole": "string",
        "WorkflowId": "string"
      }
    ]
  }
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Server

Tableau contenant les propriétés d'un serveur dont ServerID vous avez spécifié les propriétés.

Type : objet [DescribedServer](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant renvoie les propriétés attribuées à un serveur.

Exemple de demande

```
{
  "ServerId": "s-01234567890abcdef"
}
```

Exemple

Cet exemple illustre une utilisation de DescribeServer.

Exemple de réponse

```
{
  "Server": {
    "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
    "EndpointDetails": {
      "AddressAllocationIds": [
        "eipalloc-01a2eabe3c04d5678",
        "eipalloc-102345be"
      ],
      "SubnetIds": [
        "subnet-047eaa7f0187a7cde",

```

```
        "subnet-0a2d0f474daffde18"  
    ],  
    "VpcEndpointId": "vpce-03fe0080e7cb008b8",  
    "VpcId": "vpc-09047a51f1c8e1634"  
  },  
  "EndpointType": "VPC",  
  "HostKeyFingerprint": "your host key",  
  "IdentityProviderType": "SERVICE_MANAGED",  
  "ServerId": "s-01234567890abcdef",  
  "State": "ONLINE",  
  "Tags": [],  
  "UserCount": 0  
}  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeUser

Décrit l'utilisateur affecté au serveur compatible avec le protocole de transfert de fichiers spécifique, tel qu'identifié par sa propriété. `ServerId`

La réponse de cet appel renvoie les propriétés de l'utilisateur associées à la `ServerId` valeur spécifiée.

Syntaxe de la requête

```
{
  "ServerId": "string",
  "UserName": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ServerId

Identifiant unique attribué par le système à un serveur auquel cet utilisateur est assigné.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

UserName

Nom de l'utilisateur assigné à un ou plusieurs serveurs. Les noms d'utilisateur font partie des informations de connexion permettant d'utiliser le AWS Transfer Family service et d'effectuer des tâches de transfert de fichiers.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "ServerId": "string",
  "User": {
    "Arn": "string",
    "HomeDirectory": "string",
    "HomeDirectoryMappings": [
      {
        "Entry": "string",
        "Target": "string",
        "Type": "string"
      }
    ],
    "HomeDirectoryType": "string",
    "Policy": "string",
    "PosixProfile": {
      "Gid": number,
      "SecondaryGids": [ number ],
      "Uid": number
    },
    "Role": "string",
    "SshPublicKeys": [
      {
        "DateImported": number,
        "SshPublicKeyBody": "string",
        "SshPublicKeyId": "string"
      }
    ],
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "UserName": "string"
  }
}
```

```
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[ServerId](#)

Identifiant unique attribué par le système à un serveur auquel cet utilisateur est assigné.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

[User](#)

Tableau contenant les propriétés de l'utilisateur Transfer Family pour la ServerID valeur que vous avez spécifiée.

Type : objet [DescribedUser](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant montre les détails d'un utilisateur existant.

Exemple de demande

```
aws transfer describe-user --server-id s-1111aaaa2222bbbb3 --user-name bob-test
```

Exemple de réponse

```
{
  "ServerId": "s-1111aaaa2222bbbb3",
  "User": {
    "Arn": "arn:aws:transfer:us-east-1:111122223333:user/s-1111aaaa2222bbbb3/bob-test",
    "HomeDirectory": "/DOC-EXAMPLE-BUCKET",
    "HomeDirectoryType": "PATH",
    "Role": "arn:aws:iam::111122223333:role/bob-role",
    "SshPublicKeys": [
      {
        "DateImported": "2022-03-31T12:27:52.614000-04:00",
        "SshPublicKeyBody": "ssh-rsa AAAAB3NzaC1yc..... bobusa@mycomputer.us-east-1.amazonaws.com",
        "SshPublicKeyId": "key-abcde12345fghik67"
      }
    ],
    "Tags": [],
    "UserName": "bob-test"
  }
}
```

```
}  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

DescribeWorkflow

Décrit le flux de travail spécifié.

Syntaxe de la requête

```
{  
  "WorkflowId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "Workflow": {  
    "Arn": "string",  
    "Description": "string",  
    "OnExceptionSteps": [  
      {  
        "CopyStepDetails": {  
          "DestinationFileLocation": {  
            "EfsFileLocation": {  
              "FileSystemId": "string",  
              "Path": "string"  
            },  
            },  
          },  
        },  
      ],  
    },  
  },  
}
```

```

        "S3FileLocation": {
            "Bucket": "string",
            "Key": "string"
        }
    },
    "Name": "string",
    "OverwriteExisting": "string",
    "SourceFileLocation": "string"
},
"CustomStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string",
    "Target": "string",
    "TimeoutSeconds": number
},
"DecryptStepDetails": {
    "DestinationFileLocation": {
        "EfsFileLocation": {
            "FileSystemId": "string",
            "Path": "string"
        },
        "S3FileLocation": {
            "Bucket": "string",
            "Key": "string"
        }
    },
    "Name": "string",
    "OverwriteExisting": "string",
    "SourceFileLocation": "string",
    "Type": "string"
},
"DeleteStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string"
},
"TagStepDetails": {
    "Name": "string",
    "SourceFileLocation": "string",
    "Tags": [
        {
            "Key": "string",
            "Value": "string"
        }
    ]
}

```

```

    },
    "Type": "string"
  }
],
"Steps": [
  {
    "CopyStepDetails": {
      "DestinationFileLocation": {
        "EfsFileLocation": {
          "FileSystemId": "string",
          "Path": "string"
        },
        "S3FileLocation": {
          "Bucket": "string",
          "Key": "string"
        }
      },
      "Name": "string",
      "OverwriteExisting": "string",
      "SourceFileLocation": "string"
    },
    "CustomStepDetails": {
      "Name": "string",
      "SourceFileLocation": "string",
      "Target": "string",
      "TimeoutSeconds": number
    },
    "DecryptStepDetails": {
      "DestinationFileLocation": {
        "EfsFileLocation": {
          "FileSystemId": "string",
          "Path": "string"
        },
        "S3FileLocation": {
          "Bucket": "string",
          "Key": "string"
        }
      },
      "Name": "string",
      "OverwriteExisting": "string",
      "SourceFileLocation": "string",
      "Type": "string"
    },
    "DeleteStepDetails": {

```

```

        "Name": "string",
        "SourceFileLocation": "string"
    },
    "TagStepDetails": {
        "Name": "string",
        "SourceFileLocation": "string",
        "Tags": [
            {
                "Key": "string",
                "Value": "string"
            }
        ]
    },
    "Type": "string"
},
"Tags": [
    {
        "Key": "string",
        "Value": "string"
    }
],
"WorkflowId": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Workflow

Structure qui contient les détails du flux de travail.

Type : objet [DescribedWorkflow](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ImportCertificate

Importe les certificats de signature et de chiffrement dont vous avez besoin pour créer des profils locaux (AS2) et des profils de partenaires.

Syntaxe de la requête

```
{
  "ActiveDate": number,
  "Certificate": "string",
  "CertificateChain": "string",
  "Description": "string",
  "InactiveDate": number,
  "PrivateKey": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Usage": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ActiveDate

Une date facultative qui indique à quel moment le certificat devient actif.

Type : Timestamp

Obligatoire : non

Certificate

- Pour leCLI, fournissez un chemin de fichier pour un certificat au URI format. Par exemple, `--certificate file://encryption-cert.pem`. Vous pouvez également fournir le contenu brut.

- Pour leSDK, spécifiez le contenu brut d'un fichier de certificat. Par exemple, `--certificate "`cat encryption-cert.pem`"`.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 16384.

Modèle : `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatoire : oui

CertificateChain

Liste facultative de certificats qui constituent la chaîne du certificat en cours d'importation.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2097152.

Modèle : `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatoire : non

Description

Brève description qui permet d'identifier le certificat.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : `[\p{Graph}]+`

Obligatoire : non

InactiveDate

Une date facultative qui indique à quel moment le certificat devient inactif.

Type : Timestamp

Obligatoire : non

PrivateKey

- Pour leCLI, fournissez un chemin de fichier pour une clé privée au URI format. Par exemple, `--private-key file://encryption-key.pem` Vous pouvez également fournir le contenu brut du fichier de clé privée.

- Pour le SDK, spécifiez le contenu brut d'un fichier de clé privée. Par exemple, `--private-key "`cat encryption-key.pem`"`

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 16384.

Modèle : `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des certificats.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Usage

Spécifie si ce certificat est utilisé pour la signature ou le chiffrement.

Type : String

Valeurs valides : SIGNING | ENCRYPTION

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "CertificateId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Certificateld

Un tableau d'identifiants pour les certificats importés. Vous utilisez cet identifiant pour travailler avec des profils et des profils de partenaires.

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : cert-([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant importe un certificat à utiliser pour le chiffrement. Dans la première commande, nous fournissons le contenu du certificat et des fichiers de chaîne de certificats. Utilisez ce format pour SDK les commandes.

```
aws transfer import-certificate --usage ENCRYPTION --certificate "`cat encryption-  
cert.pem`" \  
    --private-key "`cat encryption-key.pem`" --certificate-chain "`cat root-ca.pem`"
```

Exemple

L'exemple suivant est identique à la commande précédente, sauf que nous indiquons les emplacements des fichiers de clé privée, de certificat et de chaîne de certificats. Cette version de la commande ne fonctionne pas si vous utilisez un SDK.

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://encryption-  
cert.pem \  
    --private-key file://encryption-key.pem --certificate-chain file://root-ca.pem
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues 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](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour JavaScript V3](#)
- [AWS SDK pour PHP V3](#)
- [AWS SDK pour Python](#)
- [AWS SDK pour Ruby V3](#)

ImportHostKey

Ajoute une clé d'hôte au serveur spécifiée par le `ServerId` paramètre.

Syntaxe de la requête

```
{
  "Description": "string",
  "HostKeyBody": "string",
  "ServerId": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

Description

Description textuelle identifiant cette clé d'hôte.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `[\p{Print}]*`

Obligatoire : non

HostKeyBody

La partie clé privée d'une paire de SSH clés.

AWS Transfer Family accepte RSAECDSA, et ED25519 clés.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Obligatoire : oui

ServerId

Identifiant du serveur qui contient la clé d'hôte que vous importez.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0 - 9 a - f] { 1 7 })

Obligatoire : oui

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des clés d'hôte.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Syntaxe de la réponse

```
{
  "HostKeyId": "string",
  "ServerId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

HostKeyId

Renvoie l'identifiant de clé d'hôte pour la clé importée.

Type : String

Contraintes de longueur : longueur fixe de 25.

Modèle : hostkey-[0-9a-f]{17}

ServerId

Renvoie l'identifiant du serveur qui contient la clé importée.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ImportSshPublicKey

Ajoute une clé publique Secure Shell (SSH) à un utilisateur de Transfer Family identifié par une `UserName` valeur attribuée au serveur compatible avec le protocole de transfert de fichiers spécifique, identifié par. `ServerId`

La réponse renvoie la `UserName` valeur, la `ServerId` valeur et le nom du `SshPublicKeyId`.

Syntaxe de la requête

```
{
  "ServerId": "string",
  "SshPublicKeyBody": "string",
  "UserName": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ServerId

Identifiant unique attribué par le système à un serveur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

SshPublicKeyBody

La partie clé publique d'une paire de SSH clés.

AWS Transfer Family accepte RSAECDSA, et ED25519 clés.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : oui

UserName

Nom de l'utilisateur Transfer Family attribué à un ou plusieurs serveurs.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "ServerId": "string",
  "SshPublicKeyId": "string",
  "UserName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

ServerId

Identifiant unique attribué par le système à un serveur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

SshPublicKeyId

Nom donné à une clé publique par le système importé.

Type : String

Contraintes de longueur : longueur fixe de 21.

Modèle : key-[0-9a-f]{17}

UserName

Nom d'utilisateur attribué à la ServerID valeur que vous avez spécifiée.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : [\w][\w@.-]{2,99}

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

Cette commande importe une ECDSA clé enregistrée dans le `id_ecdsa.pub` fichier.

```
aws transfer import-ssh-public-key --server-id s-021345abcdef6789 --ssh-public-key-body  
file://id_ecdsa.pub --user-name jane-doe
```

Exemple

Si vous exécutez la commande précédente, le système renvoie les informations suivantes.

```
{  
  "ServerId": "s-021345abcdef6789",  
  "SshPublicKeyId": "key-1234567890abcdef0",  
  "UserName": "jane-doe"  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)

- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListAccesses

Répertorie les détails de tous les accès que vous avez sur votre serveur.

Syntaxe de la requête

```
{
  "MaxResults": number,
  "NextToken": "string",
  "ServerId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Spécifie le nombre maximum d'accès SIDs à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListAccesses` appel, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite transmettre une commande ultérieure au `NextToken` paramètre pour continuer à répertorier les accès supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

[ServerId](#)

Identifiant unique attribué par le système à un serveur auquel des utilisateurs sont assignés.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{
  "Accesses": [
    {
      "ExternalId": "string",
      "HomeDirectory": "string",
      "HomeDirectoryType": "string",
      "Role": "string"
    }
  ],
  "NextToken": "string",
  "ServerId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[Accesses](#)

Renvoie les accès et leurs propriétés pour la `ServerId` valeur que vous spécifiez.

Type : tableau d'objets [ListedAccess](#)

[NextToken](#)

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListAccesses` appel, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite transmettre

une commande ultérieure au NextToken paramètre pour continuer à répertorier les accès supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

ServerId

Identifiant unique attribué par le système à un serveur auquel des utilisateurs sont assignés.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0 - 9 a - f] { 17 })

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListAgreements

Renvoie une liste des accords pour le serveur identifié par celui `ServerId` que vous fournissez. Si vous souhaitez limiter les résultats à un certain nombre, indiquez une valeur pour le `MaxResults` paramètre. Si vous avez déjà exécuté la commande et que vous avez reçu une valeur pour `NextToken`, vous pouvez fournir cette valeur pour continuer à répertorier les accords là où vous vous êtes arrêté.

Syntaxe de la requête

```
{
  "MaxResults": number,
  "NextToken": "string",
  "ServerId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Le nombre maximum d'accords à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListAgreements` appel, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite transmettre une commande ultérieure au `NextToken` paramètre pour continuer à répertorier les accords supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

ServerId

Identifiant du serveur pour lequel vous souhaitez obtenir une liste d'accords.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{
  "Agreements": [
    {
      "AgreementId": "string",
      "Arn": "string",
      "Description": "string",
      "LocalProfileId": "string",
      "PartnerProfileId": "string",
      "ServerId": "string",
      "Status": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Agreements

Renvoie un tableau dans lequel chaque élément contient les détails d'un accord.

Type : tableau d'objets [ListedAgreement](#)

[NextToken](#)

Renvoie un jeton que vous pouvez utiliser pour appeler à `ListAgreements` nouveau et recevoir des résultats supplémentaires, le cas échéant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le `NextToken` paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListCertificates

Renvoie la liste des certificats actuels qui ont été importés dans AWS Transfer Family. Si vous souhaitez limiter les résultats à un certain nombre, indiquez une valeur pour le `MaxResults` paramètre. Si vous avez exécuté la commande précédemment et que vous avez reçu une valeur pour le `NextToken` paramètre, vous pouvez fournir cette valeur pour continuer à répertorier les certificats là où vous vous êtes arrêté.

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](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Le nombre maximum de certificats à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListCertificates` appel, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite transmettre une commande ultérieure au `NextToken` paramètre pour continuer à répertorier les certificats supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

Syntaxe de la réponse

```
{
  "Certificates": [
    {
      "ActiveDate": number,
      "Arn": "string",
      "CertificateId": "string",
      "Description": "string",
      "InactiveDate": number,
      "Status": "string",
      "Type": "string",
      "Usage": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[Certificates](#)

Renvoie un tableau des certificats spécifiés dans l'`ListCertificates` appel.

Type : tableau d'objets [ListedCertificate](#)

[NextToken](#)

Renvoie le jeton suivant, que vous pouvez utiliser pour répertorier le certificat suivant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)

- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListConnectors

Répertorie les connecteurs pour la région spécifiée.

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](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Le nombre maximum de connecteurs à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListConnectors` appel, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite passer une commande suivante au `NextToken` paramètre pour continuer à répertorier les connecteurs supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

Syntaxe de la réponse

```
{
  "Connectors": [
    {
      "Arn": "string",
      "ConnectorId": "string",
      "Url": "string"
    }
  ],
  "NextToken": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[Connectors](#)

Renvoie un tableau dans lequel chaque élément contient les détails d'un connecteur.

Type : tableau d'objets [ListedConnector](#)

[NextToken](#)

Renvoie un jeton que vous pouvez utiliser pour appeler à ListConnectors nouveau et recevoir des résultats supplémentaires, le cas échéant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListExecutions

Répertorie toutes les exécutions en cours pour le flux de travail spécifié.

Note

Si l'ID de flux de travail spécifié est introuvable, `ListExecutions` renvoie une `ResourceNotFound` exception.

Syntaxe de la requête

```
{
  "MaxResults": number,
  "NextToken": "string",
  "WorkflowId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

MaxResults

Spécifie le nombre maximum d'exécutions à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

NextToken

`ListExecutions` renvoie le `NextToken` paramètre dans la sortie. Vous pouvez ensuite transmettre le `NextToken` paramètre dans une commande suivante pour continuer à répertorier les exécutions supplémentaires.

C'est utile pour la pagination, par exemple. Si vous avez 100 exécutions pour un flux de travail, vous souhaitez peut-être n'en répertorier que les 10 premières. Si c'est le cas, appelez le API en spécifiant `max-results` :

```
aws transfer list-executions --max-results 10
```

Cela renvoie les détails des 10 premières exécutions, ainsi que le pointeur (`NextToken`) vers la onzième exécution. Vous pouvez maintenant l'appeler API à nouveau, en fournissant la `NextToken` valeur que vous avez reçue :

```
aws transfer list-executions --max-results 10 --next-token  
$somePointerReturnedFromPreviousListResult
```

Cet appel renvoie les 10 prochaines exécutions, de la 11e à la 20e. Vous pouvez ensuite répéter l'appel jusqu'à ce que les détails des 100 exécutions aient été communiqués.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

[WorkflowId](#)

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `w-([a-z0-9]{17})`

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "Executions": [  
    {  
      "ExecutionId": "string",  
      "InitialFileLocation": {  
        "EfsFileLocation": {  
          "FileSystemId": "string",
```

```

        "Path": "string"
    },
    "S3FileLocation": {
        "Bucket": "string",
        "Etag": "string",
        "Key": "string",
        "VersionId": "string"
    }
},
"ServiceMetadata": {
    "UserDetails": {
        "ServerId": "string",
        "SessionId": "string",
        "UserName": "string"
    }
},
"Status": "string"
}
],
"NextToken": "string",
"WorkflowId": "string"
}

```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[Executions](#)

Renvoie les détails de chaque exécution, sous forme de ListedExecution tableau.

Type : tableau d'objets [ListedExecution](#)

[NextToken](#)

ListExecutions renvoie le NextToken paramètre dans la sortie. Vous pouvez ensuite transmettre le NextToken paramètre dans une commande suivante pour continuer à répertorier les exécutions supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListHostKeys

Renvoie une liste de clés d'hôte pour le serveur spécifiée par le `ServerId` paramètre.

Syntaxe de la requête

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Le nombre maximum de clés d'hôte à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque d'autres résultats n'ont pas été renvoyés, un `NextToken` paramètre est renvoyé. Vous pouvez utiliser cette valeur pour un appel ultérieur afin de continuer `ListHostKeys` à répertorier les résultats.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

[ServerId](#)

Identifiant du serveur qui contient les clés d'hôte que vous souhaitez consulter.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{
  "HostKeys": [
    {
      "Arn": "string",
      "DateImported": number,
      "Description": "string",
      "Fingerprint": "string",
      "HostKeyId": "string",
      "Type": "string"
    }
  ],
  "NextToken": "string",
  "ServerId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

HostKeys

Renvoie un tableau dans lequel chaque élément contient les détails d'une clé d'hôte.

Type : tableau d'objets [ListedHostKey](#)

NextToken

Renvoie un jeton que vous pouvez utiliser pour appeler à ListHostKeys nouveau et recevoir des résultats supplémentaires, le cas échéant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

ServerId

Renvoie l'identifiant du serveur qui contient les clés d'hôte répertoriées.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0 - 9 a - f] { 17 })

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListProfiles

Renvoie la liste des profils de votre système. Si vous souhaitez limiter les résultats à un certain nombre, indiquez une valeur pour le `MaxResults` paramètre. Si vous avez déjà exécuté la commande et que vous avez reçu une valeur pour `NextToken`, vous pouvez fournir cette valeur pour continuer à répertorier les profils là où vous vous êtes arrêté.

Syntaxe de la requête

```
{  
  "MaxResults": number,  
  "NextToken": "string",  
  "ProfileType": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Le nombre maximum de profils à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque d'autres résultats n'ont pas été renvoyés, un `NextToken` paramètre est renvoyé. Vous pouvez utiliser cette valeur pour un appel ultérieur afin de continuer `ListProfiles` à répertorier les résultats.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

[ProfileType](#)

Indique s'il faut répertorier uniquement les profils de type LOCAL ou uniquement les profils de type PARTNER. Si elle n'est pas fournie dans la demande, la commande répertorie tous les types de profils.

Type : String

Valeurs valides : LOCAL | PARTNER

Obligatoire : non

Syntaxe de la réponse

```
{
  "NextToken": "string",
  "Profiles": [
    {
      "Arn": "string",
      "As2Id": "string",
      "ProfileId": "string",
      "ProfileType": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[NextToken](#)

Renvoie un jeton que vous pouvez utiliser pour appeler à ListProfiles nouveau et recevoir des résultats supplémentaires, le cas échéant.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Profiles

Renvoie un tableau dans lequel chaque élément contient les détails d'un profil.

Type : tableau d'objets [ListedProfile](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListSecurityPolicies

Répertorie les politiques de sécurité associées à vos serveurs compatibles avec le protocole de transfert de fichiers.

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](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Spécifie le nombre de politiques de sécurité à renvoyer en réponse à la ListSecurityPolicies requête.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque des résultats supplémentaires sont obtenus à partir de la ListSecurityPolicies commande, un NextToken paramètre est renvoyé dans la sortie. Vous pouvez ensuite transmettre le NextToken paramètre dans une commande suivante pour continuer à répertorier les politiques de sécurité supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

Syntaxe de la réponse

```
{  
  "NextToken": "string",  
  "SecurityPolicyNames": [ "string" ]  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

NextToken

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'ListSecurityPoliciesopération, un NextToken paramètre est renvoyé dans la sortie. Dans une commande suivante, vous pouvez transmettre le NextToken paramètre pour continuer à répertorier les politiques de sécurité.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

SecurityPolicyNames

Un ensemble de politiques de sécurité répertoriées.

Type : tableau de chaînes

Contraintes de longueur : longueur minimale de 0. Longueur maximum de 100.

Modèle : TransferSecurityPolicy-.+

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant répertorie les noms de toutes les politiques de sécurité disponibles.

Exemple de demande

```
aws transfer list-security-policies
```

Exemple de réponse

```
{
  "SecurityPolicyNames": [
    "TransferSecurityPolicy-2022-03",
    "TransferSecurityPolicy-FIPS-2020-06",
    "TransferSecurityPolicy-2018-11",
    "TransferSecurityPolicy-2023-05",
    "TransferSecurityPolicy-FIPS-2023-05",
    "TransferSecurityPolicy-2020-06"
  ]
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListServers

Répertorie les serveurs compatibles avec le protocole de transfert de fichiers associés à votre compte. AWS

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](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Spécifie le nombre de serveurs à renvoyer en réponse à la ListServers requête.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Lorsque des résultats supplémentaires sont obtenus à partir de la ListServers commande, un NextToken paramètre est renvoyé dans la sortie. Vous pouvez ensuite transmettre le NextToken paramètre dans une commande suivante pour continuer à répertorier les serveurs supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

Syntaxe de la réponse

```
{
  "NextToken": "string",
  "Servers": [
    {
      "Arn": "string",
      "Domain": "string",
      "EndpointType": "string",
      "IdentityProviderType": "string",
      "LoggingRole": "string",
      "ServerId": "string",
      "State": "string",
      "UserCount": number
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

NextToken

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListServers` opération, un `NextToken` paramètre est renvoyé dans la sortie. Dans une commande suivante, vous pouvez transmettre le `NextToken` paramètre pour continuer à répertorier les serveurs supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Servers

Un ensemble de serveurs répertoriés.

Type : tableau d'objets [ListedServer](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le `NextToken` paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant répertorie les serveurs qui existent dans votre Compte AWS.

Notez que les `NextToken` valeurs d'exemple ne sont pas réelles : elles sont destinées à indiquer comment utiliser le paramètre.

Exemple de demande

```
{
  "MaxResults": 1,
  "NextToken": "token-from-previous-API-call"
}
```

Exemple de réponse

```
{
  "NextToken": "another-token-to-continue-listing",
  "Servers": [
    {
      "Arn": "arn:aws:transfer:us-east-1:111112222222:server/s-01234567890abcdef",
      "Domain": "S3",
      "IdentityProviderType": "SERVICE_MANAGED",
      "EndpointType": "PUBLIC",
      "LoggingRole": "arn:aws:iam::111112222222:role/my-role",
      "ServerId": "s-01234567890abcdef",
      "State": "ONLINE",
      "UserCount": 3
    }
  ]
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListTagsForResource

Répertorie toutes les balises associées au nom de ressource Amazon (ARN) que vous spécifiez. La ressource peut être un utilisateur, un serveur ou un rôle.

Syntaxe de la requête

```
{  
  "Arn": "string",  
  "MaxResults": number,  
  "NextToken": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

Arn

Demande les balises associées à un nom de ressource Amazon particulier (ARN). An ARN est un identifiant pour une AWS ressource spécifique, telle qu'un serveur, un utilisateur ou un rôle.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

MaxResults

Spécifie le nombre de balises à renvoyer en réponse à la ListTagsForResource demande.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

NextToken

Lorsque vous demandez des résultats supplémentaires à l'`ListTagsForResource` opération, un `NextToken` paramètre est renvoyé dans l'entrée. Vous pouvez ensuite passer une commande suivante au `NextToken` paramètre pour continuer à répertorier les balises supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

Syntaxe de la réponse

```
{
  "Arn": "string",
  "NextToken": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Arn

ARN Vous avez indiqué de répertorier les balises de.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

NextToken

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListTagsForResource` appel, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite passer une commande suivante au `NextToken` paramètre pour continuer à répertorier les balises supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Tags

Paires clé-valeur attribuées à une ressource, généralement dans le but de regrouper et de rechercher des éléments. Les balises sont des métadonnées que vous définissez.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le `NextToken` paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant répertorie les balises de la ressource avec la valeur ARN que vous avez spécifiée.

Exemple de demande

```
{
  "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef"
}
```

Exemple

Cet exemple illustre une utilisation de ListTagsForResource.

Exemple de réponse

```
{
  "Tags": [
    {
      "Key": "Name",
      "Value": "MyServer"
    }
  ]
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)

- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListUsers

Répertorie les utilisateurs d'un serveur compatible avec le protocole de transfert de fichiers que vous spécifiez en transmettant le paramètre. `ServerId`

Syntaxe de la requête

```
{
  "MaxResults": number,
  "NextToken": "string",
  "ServerId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Spécifie le nombre d'utilisateurs à renvoyer en réponse à la `ListUsers` demande.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

Si l'`ListUsers` appel donne des résultats supplémentaires, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite passer la commande `NextToken` à une `ListUsers` commande suivante, pour continuer à répertorier d'autres utilisateurs.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

ServerId

Identifiant unique attribué par le système à un serveur auquel des utilisateurs sont assignés.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{
  "NextToken": "string",
  "ServerId": "string",
  "Users": [
    {
      "Arn": "string",
      "HomeDirectory": "string",
      "HomeDirectoryType": "string",
      "Role": "string",
      "SshPublicKeyCount": number,
      "UserName": "string"
    }
  ]
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

NextToken

Lorsque vous pouvez obtenir des résultats supplémentaires à partir de l'`ListUsers` appel, un `NextToken` paramètre est renvoyé dans la sortie. Vous pouvez ensuite transmettre une commande ultérieure au `NextToken` paramètre pour continuer à répertorier les utilisateurs supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

ServerId

Identifiant unique attribué par le système à un serveur auquel les utilisateurs sont affectés.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Users

Renvoie les utilisateurs de Transfer Family et leurs propriétés pour la `ServerId` valeur que vous spécifiez.

Type : tableau d'objets [ListedUser](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le `NextToken` paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'`ListUsersAPI` renvoie une liste d'utilisateurs associés à un serveur que vous spécifiez.

Exemple de demande

```
{
  "MaxResults": 100,
  "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
  "ServerId": "s-01234567890abcdef"
}
```

Exemple

Voici un exemple de réponse pour cet API appel.

Exemple de réponse

```
{
  "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b1X0cnVuU2F0ZV9hbW91bnQiOiAyfQ==",
  "ServerId": "s-01234567890abcdef",
  "Users": [
    {
      "Arn": "arn:aws:transfer:us-east-1:176354371281:user/s-01234567890abcdef/charlie",
      "HomeDirectory": "/tests/home/charlie",

```

```
    "SshPublicKeyCount": 1,  
    "Role": "arn:aws:iam::176354371281:role/transfer-role1",  
    "Tags": [  
      {  
        "Key": "Name",  
        "Value": "user1"  
      }  
    ],  
    "UserName": "my_user"  
  }  
]  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

ListWorkflows

Répertorie tous les flux de travail associés Compte AWS à votre région actuelle.

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](#).

La demande accepte les données suivantes au JSON format suivant.

[MaxResults](#)

Spécifie le nombre maximum de flux de travail à renvoyer.

Type : entier

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

Obligatoire : non

[NextToken](#)

ListWorkflows renvoie le NextToken paramètre dans la sortie. Vous pouvez ensuite transmettre le NextToken paramètre dans une commande suivante pour continuer à répertorier les flux de travail supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

Obligatoire : non

Syntaxe de la réponse

```
{
```

```
"NextToken": "string",
"Workflows": [
  {
    "Arn": "string",
    "Description": "string",
    "WorkflowId": "string"
  }
]
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[NextToken](#)

ListWorkflows renvoie le NextToken paramètre dans la sortie. Vous pouvez ensuite transmettre le NextToken paramètre dans une commande suivante pour continuer à répertorier les flux de travail supplémentaires.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 6 144.

[Workflows](#)

Renvoie le ArnWorkflowId, et Description pour chaque flux de travail.

Type : tableau d'objets [ListedWorkflow](#)

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidNextTokenException

Le NextToken paramètre transmis n'est pas valide.

HTTPCode de statut : 400

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

SendWorkflowStepState

Envoie un rappel pour les étapes personnalisées asynchrones.

Les `ExecutionIdWorkflowId`, et `Token` sont transmis à la ressource cible lors de l'exécution d'une étape personnalisée d'un flux de travail. Vous devez les inclure dans leur rappel et fournir un statut.

Syntaxe de la requête

```
{
  "ExecutionId": "string",
  "Status": "string",
  "Token": "string",
  "WorkflowId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ExecutionId

Identifiant unique pour l'exécution d'un flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 36.

Modèle : `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatoire : oui

Status

Indique si l'étape spécifiée a réussi ou échoué.

Type : String

Valeurs valides : SUCCESS | FAILURE

Obligatoire : oui

Token

Utilisé pour faire la distinction entre plusieurs rappels pour plusieurs étapes Lambda au cours d'une même exécution.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 64.

Modèle : \w+

Obligatoire : oui

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

HTTPCode de statut : 400

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)

- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

StartFileTransfer

Commence un transfert de fichiers entre le AWS stockage local et une télécommande AS2 ou un SFTP serveur.

- Pour un AS2 connecteur, vous devez spécifier le `ConnectorId` et ou plusieurs `SendFilePaths` pour identifier les fichiers que vous souhaitez transférer.
- Pour un SFTP connecteur, le transfert de fichiers peut être sortant ou entrant. Dans les deux cas, vous spécifiez le `ConnectorId`. En fonction de la direction du transfert, vous spécifiez également les éléments suivants :
 - Si vous transférez un fichier du SFTP serveur d'un partenaire vers le stockage Amazon Web Services, vous devez en spécifier un ou plusieurs `RetrieveFilePaths` pour identifier les fichiers que vous souhaitez transférer, et un `LocalDirectoryPath` pour spécifier le dossier de destination.
 - Si vous transférez un fichier vers le SFTP serveur d'un partenaire depuis le AWS stockage, vous devez en spécifier un ou plusieurs `SendFilePaths` pour identifier les fichiers que vous souhaitez transférer, et un `RemoteDirectoryPath` pour spécifier le dossier de destination.

Syntaxe de la requête

```
{  
  "ConnectorId": "string",  
  "LocalDirectoryPath": "string",  
  "RemoteDirectoryPath": "string",  
  "RetrieveFilePaths": [ "string" ],  
  "SendFilePaths": [ "string" ]  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ConnectorId

Identifiant unique du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c - ([0-9a-f] {17})

Obligatoire : oui

LocalDirectoryPath

Dans le cas d'un transfert entrant, le LocalDirectoryPath spécifie la destination d'un ou de plusieurs fichiers transférés depuis le SFTP serveur du partenaire.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 1024.

Modèle : (.) +

Obligatoire : non

RemoteDirectoryPath

Dans le cas d'un transfert sortant, le RemoteDirectoryPath spécifie la destination d'un ou de plusieurs fichiers transférés vers le SFTP serveur du partenaire. Si vous ne spécifiez pas unRemoteDirectoryPath, la destination des fichiers transférés est le répertoire personnel de SFTP l'utilisateur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 1024.

Modèle : (.) +

Obligatoire : non

RetrieveFilePaths

Un ou plusieurs chemins source pour le SFTP serveur du partenaire. Chaque chaîne représente le chemin du fichier source pour un transfert de fichier entrant.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 1024.

Modèle : (.) +

Obligatoire : non

[SendFilePaths](#)

Un ou plusieurs chemins source pour le stockage Amazon S3. Chaque chaîne représente le chemin du fichier source pour un transfert de fichier sortant. Par exemple, `DOC-EXAMPLE-BUCKET/myfile.txt` .

Note

`DOC-EXAMPLE-BUCKET` Remplacez-le par l'un de vos seaux actuels.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 1024.

Modèle : (.) +

Obligatoire : non

Syntaxe de la réponse

```
{  
  "TransferId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

TransferId

Renvoie l'identifiant unique pour le transfert de fichier.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 512.

Modèle : [0-9a-zA-Z./-]+

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant lance un transfert de AS2 fichier depuis un serveur Transfer Family vers le terminal d'un partenaire commercial distant. *DOC-EXAMPLE-BUCKET* Remplacez-le par l'un de vos seaux actuels.

Exemple de demande

```
{
  "ConnectorId": "c-AAAA1111BBBB2222C",
  "SendFilePaths": [
    "/DOC-EXAMPLE-BUCKET/myfile-1.txt",
    "/DOC-EXAMPLE-BUCKET/myfile-2.txt",
    "/DOC-EXAMPLE-BUCKET/myfile-3.txt"
  ]
}
```

Exemple de réponse

```
{
  "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Exemple

L'exemple suivant lance un transfert de fichier depuis le AWS stockage local vers un SFTP serveur distant.

Exemple de demande

```
{
  "ConnectorId": "c-01234567890abcdef",
  "SendFilePaths": [
    "/DOC-EXAMPLE-BUCKET/myfile-1.txt",
    "/DOC-EXAMPLE-BUCKET/myfile-2.txt",
    "/DOC-EXAMPLE-BUCKET/myfile-3.txt"
  ],
  "RemoteDirectoryPath": "/MySFTPRootFolder/fromTransferFamilyServer"
}
```

Exemple de réponse

```
{
  "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
}
```

Exemple

L'exemple suivant lance un transfert de fichier d'un SFTP serveur distant vers le AWS stockage local.

Exemple de demande

```
{
  "ConnectorId": "c-111122223333AAAAA",
  "RetrieveFilePaths": [
    "/MySFTPFolder/toTransferFamily/myfile-1.txt",
    "/MySFTPFolder/toTransferFamily/myfile-2.txt",
    "/MySFTPFolder/toTransferFamily/myfile-3.txt"
  ],
  "LocalDirectoryPath": "/DOC-EXAMPLE-BUCKET/mySourceFiles"
}
```

Exemple de réponse

```
{
  "TransferId": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)

- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

StartServer

Fait passer l'état d'un serveur compatible avec le protocole de transfert de fichiers de à. OFFLINE
ONLINE Cela n'a aucun impact sur un serveur qui existe déjà à ONLINE. Un ONLINE serveur peut accepter et traiter des tâches de transfert de fichiers.

L'état de STARTING indique que le serveur est dans un état intermédiaire, qu'il n'est pas totalement en mesure de répondre ou qu'il n'est pas entièrement en ligne. Les valeurs de START_FAILED peuvent indiquer une condition d'erreur.

Aucune réponse n'est renvoyée suite à cet appel.

Syntaxe de la requête

```
{  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte le JSON format des données suivantes.

ServerId

Identifiant unique attribué par le système à un serveur que vous démarrez.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant démarre un serveur.

Exemple de demande

```
{
```

```
"ServerId": "s-01234567890abcdef"
}
```

Exemple

Voici un exemple de réponse pour cet API appel.

Exemple de réponse

```
{
  "ServerId": "s-01234567890abcdef"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

StopServer

Fait passer l'état d'un serveur compatible avec le protocole de transfert de fichiers de à. ONLINE
OFFLINE Un OFFLINE serveur ne peut pas accepter et traiter les tâches de transfert de fichiers. Les informations liées à votre serveur, telles que les propriétés du serveur et de l'utilisateur, ne sont pas affectées par l'arrêt de votre serveur.

Note

L'arrêt du serveur ne réduit ni n'a d'impact sur la facturation de votre terminal de protocole de transfert de fichiers ; vous devez supprimer le serveur pour ne plus être facturé.

L'état de STOPPING indique que le serveur est dans un état intermédiaire, qu'il n'est pas totalement en mesure de répondre ou qu'il n'est pas complètement hors ligne. Les valeurs de STOP_FAILED peuvent indiquer une condition d'erreur.

Aucune réponse n'est renvoyée suite à cet appel.

Syntaxe de la requête

```
{  
  "ServerId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte le JSON format des données suivantes.

ServerId

Identifiant unique attribué par le système à un serveur que vous avez arrêté.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant arrête un serveur.

Exemple de demande

```
{  
  "ServerId": "s-01234567890abcdef"  
}
```

Exemple

Voici un exemple de réponse pour cet API appel.

Exemple de réponse

```
{  
  "ServerId": "s-01234567890abcdef"  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

TagResource

Attache une paire clé-valeur à une ressource, telle qu'identifiée par son Amazon Resource Name (ARN). Les ressources sont des utilisateurs, des serveurs, des rôles et d'autres entités.

Aucune réponse n'a été renvoyée à la suite de cet appel.

Syntaxe de la requête

```
{
  "Arn": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[Arn](#)

Nom de ressource Amazon (ARN) pour une AWS ressource spécifique, telle qu'un serveur, un utilisateur ou un rôle.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

[Tags](#)

Paires clé-valeur assignées ARNs que vous pouvez utiliser pour regrouper et rechercher des ressources par type. Vous pouvez associer ces métadonnées à des ressources (serveurs, utilisateurs, flux de travail, etc.) pour n'importe quel usage.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant ajoute une balise à un serveur compatible avec le protocole de transfert de fichiers.

Exemple de demande

```
{
  "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
  "Tags": [
    {
      "Key": "Group",
      "Value": "Europe"
    }
  ]
}
```

Exemple

Cet exemple illustre une utilisation de TagResource.

Exemple de réponse

HTTP 200 response with an empty HTTP body.

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)

- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

TestConnection

Teste si votre SFTP connecteur est correctement configuré. Nous vous recommandons vivement d'effectuer cette opération pour tester votre capacité à transférer des fichiers entre le AWS stockage local et le SFTP serveur d'un partenaire commercial.

Syntaxe de la requête

```
{  
  "ConnectorId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[ConnectorId](#)

Identifiant unique du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c - ([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "ConnectorId": "string",  
  "Status": "string",  
  "StatusMessage": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

ConnectorId

Renvoie l'identifiant de l'objet connecteur que vous testez.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c - ([0 - 9 a - f] { 17 })

Status

Retourne OK en cas de réussite du test ou en ERROR cas d'échec du test.

Type : String

StatusMessage

Renvoie Connection succeeded si le test est réussi. Ou renvoie un message d'erreur descriptif en cas d'échec du test. La liste suivante fournit des informations de dépannage, en fonction du message d'erreur que vous recevez.

- Vérifiez que votre nom secret correspond à celui indiqué dans les autorisations Transfer Role.
- Vérifiez le serveur URL dans la configuration du connecteur et vérifiez que les informations de connexion fonctionnent correctement en dehors du connecteur.
- Vérifiez que le secret existe et qu'il est correctement formaté.
- Vérifiez que la clé d'hôte approuvée dans la configuration du connecteur correspond à la ssh-keyscan sortie.

Type : String

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant teste la connexion à un serveur distant.

```
aws transfer test-connection --connector-id c-abcd1234567890fff
```

Exemple de réponse

En cas de succès, l'API appelle renvoie les informations suivantes.

```
{
  "Status": "OK",
  "StatusMessage": "Connection succeeded"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

TestIdentityProvider

Si le serveur compatible avec le protocole `IdentityProviderType` de transfert de fichiers est `AWS_DIRECTORY_SERVICE` ou `API_Gateway`, teste si votre fournisseur d'identité est correctement configuré. Nous vous recommandons vivement d'appeler cette opération pour tester votre méthode d'authentification dès la création de votre serveur. Ce faisant, vous pouvez résoudre les problèmes liés à l'intégration du fournisseur d'identité afin de garantir que vos utilisateurs peuvent utiliser le service avec succès.

Les paramètres `ServerId` et `UserName` sont obligatoires. Les `ServerProtocolSourceIp`, et `UserPassword` sont tous facultatifs.

Notez ce qui suit :

- Vous ne pouvez pas l'utiliser `TestIdentityProvider` si le `IdentityProviderType` de votre serveur l'est `SERVICE_MANAGED`.
- `TestIdentityProvider` ne fonctionne pas avec les clés : il n'accepte que les mots de passe.
- `TestIdentityProvider` peut tester le fonctionnement du mot de passe pour un fournisseur d'identité personnalisé qui gère les clés et les mots de passe.
- Si vous fournissez des valeurs incorrectes pour un paramètre, le `Response` champ est vide.
- Si vous fournissez un ID de serveur pour un serveur qui utilise des utilisateurs gérés par des services, le message d'erreur suivant s'affiche :

```
An error occurred (InvalidRequestException) when calling the
TestIdentityProvider operation: s-server-ID not configured for external
auth
```

- Si vous entrez un ID de serveur pour le `--server-id` paramètre qui n'identifie pas un véritable serveur de transfert, le message d'erreur suivant s'affiche :

```
An error occurred (ResourceNotFoundException) when calling the
TestIdentityProvider operation: Unknown server.
```

Il est possible que votre serveur se trouve dans une autre région. Vous pouvez spécifier une région en ajoutant ce qui suit : `--region region-code`, par exemple `--region us-east-2` pour spécifier un serveur dans l'est des États-Unis (Ohio).

Syntaxe de la requête

```
{  
  "ServerId": "string",  
  "ServerProtocol": "string",  
  "SourceIp": "string",  
  "UserName": "string",  
  "UserPassword": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte le JSON format des données suivantes.

ServerId

Identifiant attribué par le système à un serveur spécifique. La méthode d'authentification utilisateur de ce serveur est testée avec un nom d'utilisateur et un mot de passe.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

ServerProtocol

Type de protocole de transfert de fichiers à tester.

Les protocoles disponibles sont :

- Protocole de transfert de fichiers Secure Shell (SSHSFTP)
- Protocole de transfert de fichiers sécurisé (FTPS)
- Protocole de transfert de fichiers (FTP)
- Déclaration d'applicabilité (2) AS2

Type : String

Valeurs valides : SFTP | FTP | FTPS | AS2

Obligatoire : non

SourceIp

Adresse IP source du compte à tester.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 32.

Modèle : \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}

Obligatoire : non

UserName

Nom du compte à tester.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : [\w][\w@.-]{2,99}

Obligatoire : oui

UserPassword

Le mot de passe du compte à tester.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 1024.

Obligatoire : non

Syntaxe de la réponse

```
{  
  "Message": "string",  
  "Response": "string",  
  "StatusCode": number,  
  "Url": "string"
```

```
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

Message

Message indiquant si le test a réussi ou non.

Note

Si une chaîne vide est renvoyée, la cause la plus probable est que l'authentification a échoué en raison d'un nom d'utilisateur ou d'un mot de passe incorrect.

Type : String

Response

La réponse renvoyée par votre API passerelle ou votre fonction Lambda.

Type : String

StatusCode

Le code HTTP d'état qui est la réponse de votre API passerelle ou de votre fonction Lambda.

Type : entier

Url

Point de terminaison du service utilisé pour authentifier un utilisateur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 255.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

La demande suivante renvoie un message d'un fournisseur d'identité indiquant qu'une combinaison nom d'utilisateur et mot de passe constitue une identité valide à utiliser AWS Transfer Family.

Exemple de demande

```
{
  "ServerID": "s-01234567890abcdef",
  "UserName": "my_user",
  "UserPassword": "MyPassword-1"
}
```

Exemple

La réponse suivante montre un exemple de réponse pour un test réussi.

Exemple de réponse

```
"Response": "{
  \"homeDirectory\": \"\\mybucket001\\\", \"homeDirectoryDetails\": null,
  \"homeDirectoryType\": \"PATH\\\", \"posixProfile\": null,
  \"publicKeys\": \"[ssh-rsa-key]\\\", \"role\": \"arn:aws:iam::123456789012:role/
my_role\\\", \"policy\": null, \"username\": \"transferuser002\\\",
  \"identityProviderType\": null, \"userConfigMessage\": null)}\"
\"StatusCode\": \"200\",
\"Message\": \"\"
```

Exemple

La réponse suivante indique que l'utilisateur spécifié appartient à plusieurs groupes ayant accès.

```
"Response": "",
"StatusCode": 200,
"Message": "More than one associated access found for user's groups."
```

Exemple

Si vous avez créé et configuré un fournisseur d'identité personnalisé à l'aide d'une API passerelle, vous pouvez entrer la commande suivante pour tester votre utilisateur :

```
aws transfer test-identity-provider --server-id s-0123456789abcdefg --user-
name myuser
```

où s-0123456789abcdefg est votre serveur de transfert et myuser est le nom d'utilisateur de votre utilisateur personnalisé.

Si la commande aboutit, votre réponse est similaire à la suivante, où :

- Compte AWS L'identifiant est 012345678901
- Le rôle de l'utilisateur est user-role-api-gateway
- Le répertoire de base est myuser-bucket
- La clé publique est une clé publique

- L'invocation URL est une invocation... URL

```
{
  "Response": "{\"Role\": \"arn:aws:iam::012345678901:role/user-role-api-gateway\",
  \"HomeDirectory\": \"~/myuser-bucket\", \"PublicKeys\": \"[public-key]\"}\",
  \"StatusCode\": 200,
  \"Message\": \"\",
  \"Url\": \"https://invocation-URL/servers/s-0123456789abcdefg/users/myuser/config\"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UntagResource

Détache une paire clé-valeur d'une ressource, telle qu'identifiée par son Amazon Resource Name (ARN). Les ressources sont des utilisateurs, des serveurs, des rôles et d'autres entités.

Aucune réponse n'est renvoyée suite à cet appel.

Syntaxe de la requête

```
{
  "Arn": "string",
  "TagKeys": [ "string" ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[Arn](#)

La valeur de la ressource dont la balise sera supprimée. Un Amazon Resource Name (ARN) est l'identifiant d'une AWS ressource spécifique, telle qu'un serveur, un utilisateur ou un rôle.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

[TagKeys](#)

TagKeys sont des paires clé-valeur attribuées ARNs qui peuvent être utilisées pour regrouper et rechercher des ressources par type. Ces métadonnées peuvent être associées à des ressources pour n'importe quel usage.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 128.

Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un HTTP corps vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

Exemples

Exemple

L'exemple suivant supprime une balise d'un serveur compatible avec le protocole de transfert de fichiers.

Exemple de demande

```
{
  "Arn": "arn:aws:transfer:us-east-1:176354371281:server/s-01234567890abcdef",
  "TagKeys": "Europe" ]
}
```

Exemple

Cet exemple illustre une utilisation de UntagResource.

Exemple de réponse

HTTP 200 response with an empty HTTP body.

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateAccess

Vous permet de mettre à jour les paramètres d'accès spécifiés dans les ExternalID paramètres ServerID et.

Syntaxe de la requête

```
{
  "ExternalId": "string",
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
  "Role": "string",
  "ServerId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

ExternalId

Identifiant unique requis pour identifier des groupes spécifiques au sein de votre annuaire.

Les utilisateurs du groupe que vous associez ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family. Si vous connaissez le nom du groupe, vous pouvez afficher les SID valeurs en exécutant la commande suivante sous Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties  
* | Select SamAccountName,ObjectSid
```

Dans cette commande, remplacez `YourGroupName` par le nom de votre groupe Active Directory.

L'expression régulière utilisée pour valider ce paramètre est une chaîne de caractères composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez également inclure des traits de soulignement ou l'un des caractères suivants : `=`, `.`, `@` : `/-`

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `S-1-[\d-]+`

Obligatoire : oui

[HomeDirectory](#)

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de `HomeDirectory` est `/bucket_name/home/mydirectory`.

Note

Le paramètre `HomeDirectory` est uniquement utilisé si `HomeDirectoryType` est défini sur la valeur `PATH`.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `(|/.*)`

Obligatoire : non

[HomeDirectoryMappings](#)

Des mappages de répertoires logiques qui spécifient quels EFS chemins et clés Amazon S3 ou Amazon doivent être visibles par votre utilisateur et comment vous souhaitez les rendre visibles. Vous devez spécifier la `Target` paire `Entry` et, qui `Entry` indique comment le chemin est rendu

visible et Target correspond au EFS chemin Amazon S3 ou Amazon réel. Si vous spécifiez uniquement une cible, elle est affichée telle quelle. Vous devez également vous assurer que votre rôle AWS Identity and Access Management (IAM) donne accès aux chemins d'accèsTarget. Cette valeur ne peut être définie que si elle HomeDirectoryType est définie sur LOGICAL.

Voici un exemple de Target paire Entry et.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

Dans la plupart des cas, vous pouvez utiliser cette valeur au lieu de la politique de session pour verrouiller votre utilisateur dans le répertoire de base désigné (« chroot »). Pour ce faire, vous pouvez Entry définir / et Target définir la valeur du HomeDirectory paramètre.

Voici un exemple de Target paire Entry et pourchroot.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Type : tableau d'objets [HomeDirectoryMapEntry](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 50 000 articles.

Obligatoire : non

[HomeDirectoryType](#)

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez surPATH, l'utilisateur verra le bucket Amazon S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez surLOGICAL, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

Note

Dans HomeDirectoryType l'affirmativeLOGICAL, vous devez fournir des mappages à l'aide du HomeDirectoryMappings paramètre. Si, par contre, HomeDirectoryType c'est le casPATH, vous fournissez un chemin absolu à l'aide du HomeDirectory paramètre. Vous ne pouvez pas avoir les deux HomeDirectory et HomeDirectoryMappings dans votre modèle.

Type : String

Valeurs valides : PATH | LOGICAL

Obligatoire : non

Policy

Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même rôle AWS Identity and Access Management (IAM) pour plusieurs utilisateurs. Cette politique limite l'accès d'un utilisateur à certaines parties de son compartiment Amazon S3. Les variables que vous pouvez utiliser à l'intérieur de cette politique incluent `${Transfer:UserName}`, `${Transfer:HomeDirectory}` et `${Transfer:HomeBucket}`.

Note

Cette politique s'applique uniquement lorsque le domaine de `ServerId` est Amazon S3. Amazon EFS n'utilise pas de politiques de session.

Pour les politiques de session, AWS Transfer Family stocke la politique sous forme de JSON blob, au lieu du nom de ressource Amazon (ARN) de la politique. Vous enregistrez la politique sous forme de JSON blob et vous la transmettez dans l'`Policy` argument. Pour obtenir un exemple de politique de session, veuillez consulter la rubrique [Exemple de politique de session](#).

Pour plus d'informations, consultez le [AssumeRole](#) document de API référence du service AWS de jetons de sécurité.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

PosixProfile

L'POSIX identité complète, y compris l'ID utilisateur (`Uid`), l'ID de groupe (`Gid`) et tout groupe secondaire IDs (`SecondaryGids`), qui contrôle l'accès de vos utilisateurs à vos systèmes de EFS fichiers Amazon. Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Type : objet [PosixProfile](#)

Obligatoire : non

[Role](#)

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

[ServerId](#)

Identifiant unique attribué par le système pour une instance de serveur. Il s'agit du serveur spécifique auquel vous avez ajouté votre utilisateur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "ExternalId": "string",
  "ServerId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

ExternalId

L'identifiant externe du groupe dont les utilisateurs ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : S-1-[\d-]+

ServerId

Identifiant du serveur auquel l'utilisateur est rattaché.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateAgreement

Met à jour certains paramètres d'un accord existant. Indiquez le `AgreementId` et le `ServerId` pour l'accord que vous souhaitez mettre à jour, ainsi que les nouvelles valeurs des paramètres à mettre à jour.

Syntaxe de la requête

```
{
  "AccessRole": "string",
  "AgreementId": "string",
  "BaseDirectory": "string",
  "Description": "string",
  "LocalProfileId": "string",
  "PartnerProfileId": "string",
  "ServerId": "string",
  "Status": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

AccessRole

Les connecteurs sont utilisés pour envoyer des fichiers en utilisant le SFTP protocole AS2 or. Pour le rôle d'accès, indiquez le nom de ressource Amazon (ARN) du AWS Identity and Access Management rôle à utiliser.

Pour AS2 connecteurs

AvecAS2, vous pouvez envoyer des fichiers en appelant `StartFileTransfer` et en spécifiant les chemins des fichiers dans le paramètre de requête, `SendFilePaths`. Nous utilisons le répertoire parent du fichier (par exemple, `car--send-file-paths /bucket/dir/file.txt`, le répertoire parent est `/bucket/dir/`) pour stocker temporairement un fichier de AS2 message traité, le stocker MDN lorsque nous le recevons du partenaire et écrire un JSON fichier final contenant les métadonnées pertinentes de la transmission. Ainsi, le `AccessRole` doit fournir un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la

requête `StartFileTransfer`. En outre, vous devez fournir un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer avec `StartFileTransfer`.

Si vous utilisez l'authentification de base pour votre AS2 connecteur, le rôle d'accès nécessite `secretsmanager:GetSecretValue` autorisation d'accès au secret. Si le secret est chiffré à l'aide d'une clé gérée par le client au lieu de la clé AWS gérée dans Secrets Manager, le rôle doit également disposer d'une `kms:Decrypt` autorisation pour cette clé.

Pour SFTP connecteurs

Assurez-vous que le rôle d'accès fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande. En outre, assurez-vous que le rôle fournit `secretsmanager:GetSecretValue` l'autorisation de AWS Secrets Manager.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

[AgreementId](#)

Identifiant unique pour l'accord. Cet identifiant est renvoyé lorsque vous créez un accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `a-([0-9a-f]{17})`

Obligatoire : oui

[BaseDirectory](#)

Pour modifier le répertoire de destination (dossier) des fichiers transférés, indiquez le dossier de compartiment que vous souhaitez utiliser, par exemple, `/DOC-EXAMPLE-BUCKET/home/mydirectory` .

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `(|/.*)`

Obligatoire : non

Description

Pour remplacer la description existante, fournissez une brève description de l'accord.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : $[\backslash p\{Graph\}]^+$

Obligatoire : non

LocalProfileId

Identifiant unique pour le profil AS2 local.

Pour modifier l'identifiant de profil local, entrez une nouvelle valeur ici.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : $p-([\emptyset-9a-f]\{17\})$

Obligatoire : non

PartnerProfileId

Identifiant unique pour le profil du partenaire. Pour modifier l'identifiant du profil du partenaire, entrez une nouvelle valeur ici.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : $p-([\emptyset-9a-f]\{17\})$

Obligatoire : non

ServerId

Identifiant unique attribué par le système pour une instance de serveur. Il s'agit du serveur spécifique utilisé par le contrat.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f] {17})

Obligatoire : oui

[Status](#)

Vous pouvez mettre à jour le statut de l'accord, soit en activant un accord inactif, soit en inversant.

Type : String

Valeurs valides : ACTIVE | INACTIVE

Obligatoire : non

Syntaxe de la réponse

```
{  
  "AgreementId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[AgreementId](#)

Identifiant unique pour l'accord. Cet identifiant est renvoyé lorsque vous créez un accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : a - ([0-9a-f] {17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateCertificate

Met à jour les dates d'activité et d'inactivité d'un certificat.

Syntaxe de la requête

```
{  
  "ActiveDate": number,  
  "CertificateId": "string",  
  "Description": "string",  
  "InactiveDate": number  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte le JSON format des données suivantes.

[ActiveDate](#)

Une date facultative qui indique à quel moment le certificat devient actif.

Type : Timestamp

Obligatoire : non

[CertificateId](#)

Identifiant de l'objet de certificat que vous mettez à jour.

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : cert-([0-9a-f]{17})

Obligatoire : oui

[Description](#)

Brève description pour aider à identifier le certificat.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : $[\backslash p\{Graph\}]^+$

Obligatoire : non

[InactiveDate](#)

Une date facultative qui indique à quel moment le certificat devient inactif.

Type : Timestamp

Obligatoire : non

Syntaxe de la réponse

```
{  
  "CertificateId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[CertificateId](#)

Renvoie l'identifiant de l'objet de certificat que vous mettez à jour.

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : $cert-([0-9a-f]\{17\})$

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant met à jour la date d'activité d'un certificat, en la fixant au 16 janvier 2022 à 16:12:07 UTC -5 heures.

Exemple de demande

```
aws transfer update-certificate --certificate-id c-abcdefgh123456hijk --active-date 2022-01-16T16:12:07-05:00
```

Exemple

Voici un exemple de réponse à cet API appel.

Exemple de réponse

```
"CertificateId": "c-abcdefg123456hijk"
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateConnector

Met à jour certains paramètres d'un connecteur existant. Indiquez le `ConnectorId` connecteur que vous souhaitez mettre à jour, ainsi que les nouvelles valeurs des paramètres à mettre à jour.

Syntaxe de la requête

```
{
  "AccessRole": "string",
  "As2Config": {
    "BasicAuthSecretId": "string",
    "Compression": "string",
    "EncryptionAlgorithm": "string",
    "LocalProfileId": "string",
    "MdnResponse": "string",
    "MdnSigningAlgorithm": "string",
    "MessageSubject": "string",
    "PartnerProfileId": "string",
    "SigningAlgorithm": "string"
  },
  "ConnectorId": "string",
  "LoggingRole": "string",
  "SftpConfig": {
    "TrustedHostKeys": [ "string" ],
    "UserSecretId": "string"
  },
  "Url": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[AccessRole](#)

Les connecteurs sont utilisés pour envoyer des fichiers en utilisant le SFTP protocole AS2 or. Pour le rôle d'accès, indiquez le nom de ressource Amazon (ARN) du AWS Identity and Access Management rôle à utiliser.

Pour AS2 connecteurs

Avec AS2, vous pouvez envoyer des fichiers en appelant `StartFileTransfer` et en spécifiant les chemins des fichiers dans le paramètre de requête, `SendFilePaths`. Nous utilisons le répertoire parent du fichier (par exemple, `--send-file-paths /bucket/dir/file.txt`, le répertoire parent est `/bucket/dir/`) pour stocker temporairement un fichier de AS2 message traité, le stocker MDN lorsque nous le recevons du partenaire et écrire un JSON fichier final contenant les métadonnées pertinentes de la transmission. Ainsi, le `AccessRole` doit fournir un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la requête `StartFileTransfer`. En outre, vous devez fournir un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer avec `StartFileTransfer`.

Si vous utilisez l'authentification de base pour votre AS2 connecteur, le rôle d'accès nécessite `secretsmanager:GetSecretValue` autorisation d'accès au secret. Si le secret est chiffré à l'aide d'une clé gérée par le client au lieu de la clé AWS gérée dans Secrets Manager, le rôle doit également disposer d'une `kms:Decrypt` autorisation pour cette clé.

Pour SFTP connecteurs

Assurez-vous que le rôle d'accès fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande. Assurez-vous également que le rôle fournit `secretsmanager:GetSecretValue` autorisation de AWS Secrets Manager.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

[As2Config](#)

Structure contenant les paramètres d'un objet AS2 connecteur.

Type : objet [As2ConnectorConfig](#)

Obligatoire : non

[ConnectorId](#)

Identifiant unique du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c-([0-9a-f]{17})

Obligatoire : oui

[LoggingRole](#)

Nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un connecteur d'activer la CloudWatch journalisation des événements Amazon S3. Lorsque cette option est configurée, vous pouvez consulter l'activité du connecteur dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : arn:.*role/\S+

Obligatoire : non

[SftpConfig](#)

Structure contenant les paramètres d'un objet SFTP connecteur.

Type : objet [SftpConnectorConfig](#)

Obligatoire : non

[Url](#)

Celui URL du partenaire AS2 ou du SFTP point final.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 255.

Obligatoire : non

Syntaxe de la réponse

```
{
```

```
"ConnectorId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[ConnectorId](#)

Renvoie l'identifiant de l'objet connecteur que vous mettez à jour.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : c - ([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour .NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateHostKey

Met à jour la description de la clé d'hôte spécifiée par les HostKeyId paramètres ServerId et.

Syntaxe de la requête

```
{
  "Description": "string",
  "HostKeyId": "string",
  "ServerId": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

Description

Description mise à jour de la clé d'hôte.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `[\p{Print}]*`

Obligatoire : oui

HostKeyId

Identifiant de la clé d'hôte que vous mettez à jour.

Type : String

Contraintes de longueur : longueur fixe de 25.

Modèle : `hostkey-[0-9a-f]{17}`

Obligatoire : oui

[ServerId](#)

Identifiant du serveur qui contient la clé d'hôte que vous mettez à jour.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{
  "HostKeyId": "string",
  "ServerId": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[HostKeyId](#)

Renvoie l'identifiant de clé d'hôte pour la clé d'hôte mise à jour.

Type : String

Contraintes de longueur : longueur fixe de 25.

Modèle : hostkey - [0-9a-f]{17}

[ServerId](#)

Renvoie l'identifiant du serveur qui contient la clé d'hôte mise à jour.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f] {17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)

- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateProfile

Met à jour certains paramètres d'un profil existant. Indiquez le `ProfileId` profil que vous souhaitez mettre à jour, ainsi que les nouvelles valeurs des paramètres à mettre à jour.

Syntaxe de la requête

```
{  
  "CertificateIds": [ "string" ],  
  "ProfileId": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[CertificateIds](#)

Un tableau d'identifiants pour les certificats importés. Vous utilisez cet identifiant pour travailler avec des profils et des profils de partenaires.

Type : tableau de chaînes

Contraintes de longueur : longueur fixe de 22.

Modèle : cert-([0-9a-f]{17})

Obligatoire : non

[ProfileId](#)

Identifiant de l'objet de profil que vous mettez à jour.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : oui

Syntaxe de la réponse

```
{  
  "ProfileId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[ProfileId](#)

Renvoie l'identifiant du profil en cours de mise à jour.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateServer

Met à jour les propriétés du serveur compatible avec le protocole de transfert de fichiers après sa création.

L'UpdateServerappel renvoie le ServerId serveur que vous avez mis à jour.

Syntaxe de la requête

```
{
  "Certificate": "string",
  "EndpointDetails": {
    "AddressAllocationIds": [ "string" ],
    "SecurityGroupIds": [ "string" ],
    "SubnetIds": [ "string" ],
    "VpcEndpointId": "string",
    "VpcId": "string"
  },
  "EndpointType": "string",
  "HostKey": "string",
  "IdentityProviderDetails": {
    "DirectoryId": "string",
    "Function": "string",
    "InvocationRole": "string",
    "SftpAuthenticationMethods": "string",
    "Url": "string"
  },
  "LoggingRole": "string",
  "PostAuthenticationLoginBanner": "string",
  "PreAuthenticationLoginBanner": "string",
  "ProtocolDetails": {
    "As2Transports": [ "string" ],
    "PassiveIp": "string",
    "SetStatOption": "string",
    "TlsSessionResumptionMode": "string"
  },
  "Protocols": [ "string" ],
  "S3StorageOptions": {
    "DirectoryListingOptimization": "string"
  },
  "SecurityPolicyName": "string",
  "ServerId": "string",
  "StructuredLogDestinations": [ "string" ],
```

```
"WorkflowDetails": {
  "OnPartialUpload": [
    {
      "ExecutionRole": "string",
      "WorkflowId": "string"
    }
  ],
  "OnUpload": [
    {
      "ExecutionRole": "string",
      "WorkflowId": "string"
    }
  ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte le JSON format des données suivantes.

[Certificate](#)

Amazon Resource Name (ARN) du AWS certificat Certificate Manager (ACM). Obligatoire lorsque `Protocols` est défini sur `FTPS`.

Pour demander un nouveau certificat public, consultez la section [Request a public certificate](#) dans le guide de l'utilisateur de AWS Certificate Manager.

Pour importer un certificat existant dans ACM, consultez la section [Importation de certificats ACM](#) dans le guide de l'utilisateur de AWS Certificate Manager.

Pour demander un certificat privé à utiliser FTPS via des adresses IP privées, consultez la section [Request a private certificate](#) dans le guide de l'utilisateur de AWS Certificate Manager.

Les certificats avec les algorithmes de chiffrement et les tailles de clés suivants sont pris en charge :

- 2048 bits RSA (`_2048`) RSA
- 4096 bits (`_4096RSA`) RSA
- Elliptic Prime Curve 256 octets (`EC_prime256v1`)

- Elliptic Prime Curve 384 octets (EC_secp384r1)
- Elliptic Prime Curve 521 octets (EC_secp521r1)

 Note

Le certificat doit être un SSL TLS certificat/X.509 version 3 valide avec une FQDN adresse IP spécifiée et des informations sur l'émetteur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 1600.

Obligatoire : non

EndpointDetails

Les paramètres de point de terminaison du cloud privé virtuel (VPC) configurés pour votre serveur. Lorsque vous hébergez votre point de terminaison dans votre environnement VPC, vous pouvez le rendre accessible uniquement aux ressources qu'il contient, ou vous pouvez associer des adresses IP élastiques et rendre votre point de terminaison accessible aux clients via Internet. Vos groupes VPC de sécurité par défaut sont automatiquement attribués à votre terminal.

Type : objet [EndpointDetails](#)

Obligatoire : non

EndpointType

Le type de point de terminaison que vous souhaitez que votre serveur utilise. Vous pouvez choisir de rendre le point de terminaison de votre serveur accessible au public (PUBLIC) ou de l'héberger dans votre VPC. Avec un point de terminaison hébergé dans un VPC, vous pouvez restreindre l'accès à votre serveur et à ses ressources uniquement VPC ou choisir de le rendre accessible à Internet en y attachant directement des adresses IP élastiques.

 Note

Après le 19 mai 2021, vous ne pourrez plus créer de serveur `EndpointType=VPC_ENDPOINT` à l'aide de votre AWS compte si celui-ci ne l'a pas déjà fait avant le 19 mai 2021. Si vous avez déjà créé des serveurs

EndpointType=VPC_ENDPOINT dans votre AWS compte le 19 mai 2021 ou avant, vous ne serez pas concerné. Après cette date, utilisez EndpointType =VPC.

Pour de plus amples informations, veuillez consulter [Cessation de l'utilisation de _ VPC ENDPOINT](#).

Il est recommandé d'utiliser VPC comme élément EndpointType. Avec ce type de point de terminaison, vous avez la possibilité d'associer directement jusqu'à trois IPv4 adresses élastiques (BYOIP incluses) au point de terminaison de votre serveur et d'utiliser des groupes de VPC sécurité pour restreindre le trafic en fonction de l'adresse IP publique du client. Cela n'est pas possible si EndpointType est défini sur VPC_ENDPOINT.

Type : String

Valeurs valides : PUBLIC | VPC | VPC_ENDPOINT

Obligatoire : non

HostKey

La RSAECDSA, ou clé ED25519 privée à utiliser pour votre SFTP serveur activé. Vous pouvez ajouter plusieurs clés hôtes, au cas où vous souhaiteriez faire pivoter les clés, ou disposer d'un ensemble de clés actives utilisant différents algorithmes.

Utilisez la commande suivante pour générer une clé de RSA 2048 bits sans phrase secrète :

```
ssh-keygen -t rsa -b 2048 -N "" -m PEM -f my-new-server-key.
```

Utilisez une valeur minimale de 2 048 pour l'-boption. Vous pouvez créer une clé plus forte en utilisant 3072 ou 4096.

Utilisez la commande suivante pour générer une clé de ECDSA 256 bits sans phrase secrète :

```
ssh-keygen -t ecdsa -b 256 -N "" -m PEM -f my-new-server-key.
```

Les valeurs valides pour l'-boption pour ECDSA sont 256, 384 et 521.

Utilisez la commande suivante pour générer une ED25519 clé sans phrase secrète :

```
ssh-keygen -t ed25519 -N "" -f my-new-server-key.
```

Pour toutes ces commandes, vous pouvez les remplacer my-new-server-key par une chaîne de votre choix.

⚠ Important

Si vous ne prévoyez pas de migrer des utilisateurs existants d'un serveur SFTP compatible existant vers un nouveau serveur, ne mettez pas à jour la clé d'hôte. La modification accidentelle de la clé d'hôte d'un serveur peut être perturbante.

Pour plus d'informations, voir [Mettre à jour les clés d'hôte pour votre SFTP serveur activé](#) dans le Guide de l' AWS Transfer Family utilisateur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Obligatoire : non

[IdentityProviderDetails](#)

Tableau contenant toutes les informations requises pour appeler la API méthode d'authentification d'un client.

Type : objet [IdentityProviderDetails](#)

Obligatoire : non

[LoggingRole](#)

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un serveur d'activer la CloudWatch journalisation Amazon pour Amazon S3 ou AmazonEFS events. Lorsque cette option est configurée, vous pouvez consulter l'activité des utilisateurs dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Modèle : (|arn:.*role/\S+)

Obligatoire : non

[PostAuthenticationLoginBanner](#)

Spécifie une chaîne à afficher lorsque les utilisateurs se connectent à un serveur. Cette chaîne s'affiche une fois l'utilisateur authentifié.

 Note

Le SFTP protocole ne prend pas en charge les bannières d'affichage après authentification.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Modèle : `[\x09-\x0D\x20-\x7E]*`

Obligatoire : non

PreAuthenticationLoginBanner

Spécifie une chaîne à afficher lorsque les utilisateurs se connectent à un serveur. Cette chaîne est affichée avant que l'utilisateur ne s'authentifie. Par exemple, la bannière suivante affiche des informations sur l'utilisation du système :

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel.
```

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Modèle : `[\x09-\x0D\x20-\x7E]*`

Obligatoire : non

ProtocolDetails

Les paramètres du protocole qui sont configurés pour votre serveur.

- Pour indiquer le mode passif (pour FTP et FTPS protocoles), utilisez le `PassiveIp` paramètre. Entrez une seule adresse à quatre points, telle que IPv4 l'adresse IP externe d'un pare-feu, d'un routeur ou d'un équilibreur de charge.
- Pour ignorer l'erreur qui est générée lorsque le client tente d'utiliser la commande `SETSTAT` sur un fichier que vous téléchargez vers un compartiment Amazon S3, utilisez le paramètre

`SetStatOption`. Pour que le AWS Transfer Family serveur ignore la SETSTAT commande et télécharge les fichiers sans avoir à apporter de modifications à votre SFTP client, définissez la valeur `surENABLE_NO_OP`. Si vous définissez le `SetStatOption` paramètre `surENABLE_NO_OP`, Transfer Family génère une entrée de journal dans Amazon CloudWatch Logs, afin que vous puissiez déterminer à quel moment le client passe un SETSTAT appel.

- Pour déterminer si votre AWS Transfer Family serveur reprend les sessions récemment négociées via un identifiant de session unique, utilisez le `TlsSessionResumptionMode` paramètre.
- `As2Transports` indique le mode de transport des AS2 messages. Actuellement, seul HTTP est pris en charge.

Type : objet [ProtocolDetails](#)

Obligatoire : non

[Protocols](#)

Spécifie le ou les protocoles de transfert de fichiers sur lesquels votre client de protocole de transfert de fichiers peut se connecter au point de terminaison de votre serveur. Les protocoles disponibles sont :

- SFTP(Secure Shell (SSH) File Transfer Protocol) : transfert de fichiers effectué SSH
- FTPS(Protocole de transfert de fichiers sécurisé) : transfert de fichiers avec TLS cryptage
- FTP (Protocole de transfert de fichiers) : Transfert de fichiers non chiffré
- AS2(Déclaration d'applicabilité 2) : utilisé pour le transport de données structurées business-to-business

Note

- Si vous le sélectionnez FTPS, vous devez choisir un certificat stocké dans AWS Certificate Manager (ACM) qui est utilisé pour identifier votre serveur lorsque des clients s'y connectent FTPS.
- Si `Protocol` comprend FTP ou FTPS, `EndpointType` doit être défini sur VPC, et `IdentityProviderType` sur `AWS_DIRECTORY_SERVICE`, `AWS_LAMBDA` ou `API_GATEWAY`.
- Si `Protocol` inclut FTP, alors `AddressAllocationIds` ne peut pas être associé.
- Si `Protocol` est uniquement défini sur SFTP, `EndpointType` peut être défini sur `PUBLIC`, et `IdentityProviderType` peut être défini comme l'un des types d'identité

pris en charge : SERVICE_MANAGED, AWS_DIRECTORY_SERVICE, AWS_LAMBDA ou API_GATEWAY.

- Si Protocol inclut AS2, alors le EndpointType doit être VPC, et le domaine doit être Amazon S3.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Valeurs valides : SFTP | FTP | FTPS | AS2

Obligatoire : non

S3StorageOptions

Spécifie si les performances de vos annuaires Amazon S3 sont optimisées ou non. Par défaut, l'option est désactivée.

Par défaut, les mappages du répertoire de base ont la valeur TYPE de DIRECTORY.

Si vous activez cette option, vous devrez alors définir explicitement la valeur sur HomeDirectoryMapEntry Type FILE si vous souhaitez qu'un mappage ait une cible de fichier.

Type : objet S3StorageOptions

Obligatoire : non

SecurityPolicyName

Spécifie le nom de la politique de sécurité attachée au serveur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 100.

Modèle : TransferSecurityPolicy-.*

Obligatoire : non

ServerId

Identifiant unique attribué par le système pour une instance de serveur à laquelle l'utilisateur Transfer Family est affecté.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : oui

[StructuredLogDestinations](#)

Spécifie les groupes de journaux auxquels les journaux de votre serveur sont envoyés.

Pour spécifier un groupe de journaux, vous devez fournir le correspondant ARN à un groupe de journaux existant. Dans ce cas, le format du groupe de logs est le suivant :

```
arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*
```

Par exemple, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Si vous avez déjà spécifié un groupe de journaux pour un serveur, vous pouvez l'effacer, et donc désactiver la journalisation structurée, en fournissant une valeur vide pour ce paramètre dans un `update-server` appel. Par exemple :

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

Type : tableau de chaînes

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : arn:\S+

Obligatoire : non

[WorkflowDetails](#)

Spécifie l'ID du flux de travail à attribuer et le rôle d'exécution utilisé pour exécuter le flux de travail.

En plus d'un flux de travail à exécuter lorsqu'un fichier est complètement chargé, `WorkflowDetails` peut également contenir un ID de flux de travail (et un rôle d'exécution) pour un flux de travail à exécuter lors d'un chargement partiel. Un téléchargement partiel se

produit lorsque la session du serveur se déconnecte alors que le fichier est toujours en cours de téléchargement.

Pour supprimer un flux de travail associé d'un serveur, vous pouvez fournir un objet `OnUpload` vide, comme dans l'exemple suivant.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-  
details '{"OnUpload":[]}'
```

Type : objet [WorkflowDetails](#)

Obligatoire : non

Syntaxe de la réponse

```
{  
  "ServerId": "string"  
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

[ServerId](#)

Identifiant unique attribué par le système à un serveur auquel l'utilisateur de Transfer Family est affecté.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

HTTPCode de statut : 400

ConflictException

Cette exception est levée lorsqu'un serveur compatible avec le protocole de transfert de fichiers UpdateServer est appelé et dont VPC le type de point de terminaison n'VpcEndpointIDest pas disponible.

HTTPCode de statut : 400

InternalServerError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceExistsException

La ressource demandée n'existe pas ou existe dans une région autre que celle spécifiée pour la commande.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant met à jour le rôle d'un serveur.

Exemple de demande

```
{
  "EndpointDetails": {
    "VpcEndpointId": "vpce-01234f056f3g13",
    "LoggingRole": "CloudWatchS3Events",
    "ServerId": "s-01234567890abcdef"
  }
}
```

Exemple

L'exemple suivant supprime tous les flux de travail associés du serveur.

Exemple de demande

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
'{"OnUpload":[]}'
```

Exemple

Voici un exemple de réponse pour cet API appel.

Exemple de réponse

```
{
  "ServerId": "s-01234567890abcdef"
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

UpdateUser

Affecte de nouvelles propriétés à un utilisateur. Les paramètres que vous transmettez modifient tout ou partie des éléments suivants : le répertoire de base, le rôle et la politique du UserName et ServerId que vous spécifiez.

La réponse renvoie le ServerId et le UserName pour l'utilisateur mis à jour.

Dans la console, vous pouvez sélectionner Restreint lorsque vous créez ou mettez à jour un utilisateur. Cela garantit que l'utilisateur ne peut accéder à rien en dehors de son répertoire personnel. La méthode programmatique pour configurer ce comportement consiste à mettre à jour l'utilisateur. Définissez leur valeur HomeDirectoryType sur LOGICAL et HomeDirectoryMappings spécifiez-les Entry en tant que root (/) et Target en tant que répertoire personnel.

Par exemple, si c'est le répertoire personnel de l'utilisateur/test/admin-user, la commande suivante met à jour l'utilisateur afin que sa configuration dans la console affiche l'indicateur Restricted tel qu'il est sélectionné.

```
aws transfer update-user --server-id <server-id> --user-name admin-user --
home-directory-type LOGICAL --home-directory-mappings "[{\"Entry\":\"/\",
\"Target\":\"/test/admin-user\"}]"
```

Syntaxe de la requête

```
{
  "HomeDirectory": "string",
  "HomeDirectoryMappings": [
    {
      "Entry": "string",
      "Target": "string",
      "Type": "string"
    }
  ],
  "HomeDirectoryType": "string",
  "Policy": "string",
  "PosixProfile": {
    "Gid": number,
    "SecondaryGids": [ number ],
    "Uid": number
  },
}
```

```
"Role": "string",  
"ServerId": "string",  
"UserName": "string"  
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez [Paramètres courants](#).

La demande accepte les données suivantes au JSON format suivant.

[HomeDirectory](#)

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de HomeDirectory est /bucket_name/home/mydirectory.

Note

Le paramètre HomeDirectory est uniquement utilisé si HomeDirectoryType est défini sur la valeur PATH.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : (| / . *)

Obligatoire : non

[HomeDirectoryMappings](#)

Des mappages de répertoires logiques qui spécifient quels EFS chemins et clés Amazon S3 ou Amazon doivent être visibles par votre utilisateur et comment vous souhaitez les rendre visibles. Vous devez spécifier la Target paire Entry et, qui Entry indique comment le chemin est rendu visible et Target correspond au EFS chemin Amazon S3 ou Amazon réel. Si vous spécifiez uniquement une cible, elle est affichée telle quelle. Vous devez également vous assurer que votre rôle AWS Identity and Access Management (IAM) donne accès aux chemins d'accèsTarget. Cette valeur ne peut être définie que si elle HomeDirectoryType est définie sur LOGICAL.

Voici un exemple de Target paire Entry et.

```
[ { "Entry": "/directory1", "Target": "/bucket_name/home/mydirectory" } ]
```

Dans la plupart des cas, vous pouvez utiliser cette valeur au lieu de la politique de session pour verrouiller votre utilisateur dans le répertoire de base désigné (« chroot »). Pour ce faire, vous pouvez Entry régler sur «/» et Target définir la valeur du HomeDirectory paramètre.

Voici un exemple de Target paire Entry et pourchroot.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Type : tableau d'objets [HomeDirectoryMapEntry](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 50 000 articles.

Obligatoire : non

[HomeDirectoryType](#)

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez surPATH, l'utilisateur verra le bucket Amazon S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez surLOGICAL, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

Note

Dans HomeDirectoryType l'affirmativeLOGICAL, vous devez fournir des mappages à l'aide du HomeDirectoryMappings paramètre. Si, en revanche, HomeDirectoryType c'est le casPATH, vous fournissez un chemin absolu à l'aide du HomeDirectory paramètre. Vous ne pouvez pas avoir les deux HomeDirectory et HomeDirectoryMappings dans votre modèle.

Type : String

Valeurs valides : PATH | LOGICAL

Obligatoire : non

Policy

Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même rôle AWS Identity and Access Management (IAM) pour plusieurs utilisateurs. Cette politique limite l'accès d'un utilisateur à certaines parties de son compartiment Amazon S3. Les variables que vous pouvez utiliser à l'intérieur de cette politique incluent `${Transfer:UserName}`, `${Transfer:HomeDirectory}` et `${Transfer:HomeBucket}`.

Note

Cette politique s'applique uniquement lorsque le domaine de `ServerId` est Amazon S3. Amazon EFS n'utilise pas de politiques de session.

Pour les politiques de session, AWS Transfer Family stocke la politique sous forme de JSON blob, au lieu du nom de ressource Amazon (ARN) de la politique. Vous enregistrez la politique sous forme de JSON blob et vous la transmettez dans l'`Policy` argument.

Pour obtenir un exemple de politique de session, veuillez consulter la rubrique [Exemple de politique de session](#).

Pour plus d'informations, consultez le [AssumeRole](#) document de API référence du service AWS de jetons de sécurité.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

PosixProfile

Spécifie l'POSIX identité complète, y compris l'ID utilisateur (`Uid`), l'ID de groupe (`Gid`) et tout groupe secondaire IDs (`SecondaryGids`), qui contrôle l'accès de vos utilisateurs à vos systèmes de fichiers Amazon Elastic (AmazonEFS). Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Type : objet [PosixProfile](#)

Obligatoire : non

Role

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

ServerId

Identifiant unique attribué par le système pour une instance de serveur Transfer Family à laquelle l'utilisateur est affecté.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

Obligatoire : oui

UserName

Chaîne unique qui identifie un utilisateur et est associée à un serveur, comme spécifié par le `ServerId`. Ce nom d'utilisateur doit comporter au minimum 3 caractères et au maximum 100 caractères. Les caractères suivants sont valides : a-z, A-Z, 0-9, trait de soulignement '_', tiret '-', point '.', et arobase « @ ». Le nom d'utilisateur ne peut pas commencer par un trait d'union, un point ou un arobase.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : oui

Syntaxe de la réponse

```
{
  "ServerId": "string",
  "UserName": "string"
}
```

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées sous JSON forme formatée par le service.

ServerId

Identifiant unique attribué par le système pour une instance de serveur Transfer Family à laquelle le compte est attribué.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `s-([0-9a-f]{17})`

UserName

Identifiant unique d'un utilisateur attribué à une instance de serveur spécifiée dans la demande.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez [Erreurs courantes](#).

InternalServiceError

Cette exception est levée lorsqu'une erreur se produit dans le AWS Transfer Family service.

HTTPCode de statut : 500

InvalidRequestException

Cette exception est levée lorsque le client soumet une demande mal formée.

HTTPCode de statut : 400

ResourceNotFoundException

Cette exception est levée lorsqu'aucune ressource n'est trouvée par le service AWS Transfer Family.

HTTPCode de statut : 400

ServiceUnavailableException

La demande a échoué car le service AWS Transfer Family n'est pas disponible.

HTTPCode de statut : 500

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

HTTPCode de statut : 400

Exemples

Exemple

L'exemple suivant met à jour un utilisateur de Transfer Family.

Exemple de demande

```
{
  "HomeDirectory": "/bucket2/documentation",
  "HomeDirectoryMappings": [
    {
      "Entry": "/directory1",
      "Target": "/bucket_name/home/mydirectory"
    }
  ]
}
```

```
    }  
  ],  
  "HomeDirectoryType": "PATH",  
  "Role": "AssumeRole",  
  "ServerId": "s-01234567890abcdef",  
  "UserName": "my_user"  
}
```

Exemple

Il s'agit d'un exemple de réponse pour cet API appel.

Exemple de réponse

```
{  
  "ServerId": "s-01234567890abcdef",  
  "UserName": "my_user"  
}
```

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [Interface de ligne de commande AWS](#)
- [AWS SDKpour. NET](#)
- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour JavaScript V3](#)
- [AWS SDKpour PHP V3](#)
- [AWS SDKpour Python](#)
- [AWS SDKpour Ruby V3](#)

Types de données

Les types de données suivants sont pris en charge :

- [As2ConnectorConfig](#)
- [CopyStepDetails](#)
- [CustomStepDetails](#)
- [DecryptStepDetails](#)
- [DeleteStepDetails](#)
- [DescribedAccess](#)
- [DescribedAgreement](#)
- [DescribedCertificate](#)
- [DescribedConnector](#)
- [DescribedExecution](#)
- [DescribedHostKey](#)
- [DescribedProfile](#)
- [DescribedSecurityPolicy](#)
- [DescribedServer](#)
- [DescribedUser](#)
- [DescribedWorkflow](#)
- [EfsFileLocation](#)
- [EndpointDetails](#)
- [ExecutionError](#)
- [ExecutionResults](#)
- [ExecutionStepResult](#)
- [FileLocation](#)
- [HomeDirectoryMapEntry](#)
- [IdentityProviderDetails](#)
- [InputFileLocation](#)
- [ListedAccess](#)
- [ListedAgreement](#)
- [ListedCertificate](#)
- [ListedConnector](#)
- [ListedExecution](#)

- [ListedHostKey](#)
- [ListedProfile](#)
- [ListedServer](#)
- [ListedUser](#)
- [ListedWorkflow](#)
- [LoggingConfiguration](#)
- [PosixProfile](#)
- [ProtocolDetails](#)
- [S3FileLocation](#)
- [S3InputFileLocation](#)
- [S3StorageOptions](#)
- [S3Tag](#)
- [ServiceMetadata](#)
- [SftpConnectorConfig](#)
- [SshPublicKey](#)
- [Tag](#)
- [TagStepDetails](#)
- [UserDetails](#)
- [WorkflowDetail](#)
- [WorkflowDetails](#)
- [WorkflowStep](#)

As2ConnectorConfig

Contient les détails d'un objet AS2 connecteur. L'objet connecteur est utilisé pour les processus AS2 sortants, afin de connecter le AWS Transfer Family client au partenaire commercial.

Table des matières

BasicAuthSecretId

Fournit un support d'authentification de base aux AS2 connecteursAPI. Pour utiliser l'authentification de base, vous devez fournir le nom ou le nom de ressource Amazon (ARN) d'un secret dans AWS Secrets Manager.

La valeur par défaut de ce paramètre est `null`, ce qui indique que l'authentification de base n'est pas activée pour le connecteur.

Si le connecteur doit utiliser l'authentification de base, le secret doit être au format suivant :

```
{ "Username": "user-name", "Password": "user-password" }
```

Remplacez `user-name` et `user-password` par les informations d'identification de l'utilisateur réel qui est authentifié.

Notez ce qui suit :

- Vous stockez ces informations d'identification dans Secrets Manager, et vous ne les transmettez pas directement dans celui-ciAPI.
- Si vous utilisez le connecteur APISDKs, ou CloudFormation pour configurer votre connecteur, vous devez créer le secret avant de pouvoir activer l'authentification de base. Toutefois, si vous utilisez la console AWS de gestion, le système peut créer le secret pour vous.

Si vous avez déjà activé l'authentification de base pour un connecteur, vous pouvez la désactiver en utilisant l'`UpdateConnectorAPI` appel. Par exemple, si vous utilisez leCLI, vous pouvez exécuter la commande suivante pour supprimer l'authentification de base :

```
update-connector --connector-id my-connector-id --as2-config  
'BasicAuthSecretId=""'
```

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

Compression

Spécifie si le AS2 fichier est compressé.

Type : String

Valeurs valides : ZLIB | DISABLED

Obligatoire : non

EncryptionAlgorithm

Algorithme utilisé pour chiffrer le fichier.

Notez ce qui suit :

- N'utilisez pas l'DES_EDE3_CBCalgorithme sauf si vous devez prendre en charge un ancien client qui en a besoin, car il s'agit d'un algorithme de chiffrement faible.
- Vous pouvez uniquement spécifier NONE si le URL pour votre connecteur utiliseHTTPS. L'utilisation HTTPS garantit qu'aucun trafic n'est envoyé en texte clair.

Type : String

Valeurs valides : AES128_CBC | AES192_CBC | AES256_CBC | DES_EDE3_CBC | NONE

Obligatoire : non

LocalProfileId

Identifiant unique pour le profil AS2 local.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : non

MdnResponse

Utilisé pour les demandes sortantes (d'un AWS Transfer Family serveur vers un AS2 serveur partenaire) afin de déterminer si la réponse du partenaire pour les transferts est synchrone ou asynchrone. Spécifiez l'une des valeurs suivantes :

- SYNC: Le système attend une MDN réponse synchrone confirmant que le fichier a été transféré avec succès (ou non).
- NONE: indique qu'aucune MDN réponse n'est requise.

Type : String

Valeurs valides : SYNC | NONE

Obligatoire : non

MdnSigningAlgorithm

Algorithme de signature de la MDN réponse.

Note

S'il est défini sur DEFAULT (ou pas défini du tout), la valeur pour SigningAlgorithm est utilisée.

Type : String

Valeurs valides : SHA256 | SHA384 | SHA512 | SHA1 | NONE | DEFAULT

Obligatoire : non

MessageSubject

Utilisé comme attribut Subject HTTP d'en-tête dans les AS2 messages envoyés avec le connecteur.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 1024.

Modèle : `[\p{Print}\p{Blank}]+`

Obligatoire : non

PartnerProfileId

Identifiant unique pour le profil de partenaire du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : non

SigningAlgorithm

Algorithme utilisé pour signer les AS2 messages envoyés avec le connecteur.

Type : String

Valeurs valides : SHA256 | SHA384 | SHA512 | SHA1 | NONE

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

CopyStepDetails

Chaque type d'étape possède sa propre `StepDetails` structure.

Table des matières

DestinationFileLocation

Spécifie l'emplacement du fichier copié. Utilisez `${Transfer:UserName}` ou `${Transfer:UploadDate}` dans ce champ pour paramétrer le préfixe de destination par nom d'utilisateur ou date de téléchargement.

- Définissez la valeur de `DestinationFileLocation` `${Transfer:UserName}` to pour copier les fichiers téléchargés dans un compartiment Amazon S3 préfixé par le nom de l'utilisateur de Transfer Family qui a chargé le fichier.
- Définissez la valeur de `DestinationFileLocation` `${Transfer:UploadDate}` to pour copier les fichiers téléchargés dans un compartiment Amazon S3 préfixé par la date du téléchargement.



Note

Le système adopte le format `UploadDate` de date `YYYY-MM-DD`, en fonction de la date à laquelle le fichier est chargé. UTC

Type : objet [InputFileLocation](#)

Obligatoire : non

Name

Le nom de l'étape, utilisé comme identifiant.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 30.

Modèle : `[\w-]*`

Obligatoire : non

OverwriteExisting

Un indicateur qui indique s'il faut écraser un fichier existant portant le même nom. L'argument par défaut est FALSE.

Si le flux de travail traite un fichier portant le même nom qu'un fichier existant, le comportement est le suivant :

- Dans l'`OverwriteExisting` affirmative TRUE, le fichier existant est remplacé par le fichier en cours de traitement.
- Si tel `OverwriteExisting` est FALSE le cas, rien ne se passe et le traitement du flux de travail s'arrête.

Type : String

Valeurs valides : TRUE | FALSE

Obligatoire : non

SourceFileLocation

Spécifie le fichier à utiliser comme entrée pour l'étape du flux de travail : soit le résultat de l'étape précédente, soit le fichier initialement chargé pour le flux de travail.

- Pour utiliser le fichier précédent comme entrée, entrez `${previous.file}`. Dans ce cas, cette étape du flux de travail utilise le fichier de sortie de l'étape précédente du flux de travail comme entrée. C'est la valeur par défaut.
- Pour utiliser l'emplacement du fichier initialement chargé comme entrée pour cette étape, entrez `${original.file}`.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `\$\{(\w+.\w+)\}`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

CustomStepDetails

Chaque type d'étape possède sa propre `StepDetails` structure.

Table des matières

Name

Le nom de l'étape, utilisé comme identifiant.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 30

Modèle : `[\w-]*`

Obligatoire : non

SourceFileLocation

Spécifie le fichier à utiliser comme entrée pour l'étape du flux de travail : soit le résultat de l'étape précédente, soit le fichier initialement chargé pour le flux de travail.

- Pour utiliser le fichier précédent comme entrée, entrez `${previous.file}`. Dans ce cas, cette étape du flux de travail utilise le fichier de sortie de l'étape précédente du flux de travail comme entrée. C'est la valeur par défaut.
- Pour utiliser l'emplacement du fichier initialement chargé comme entrée pour cette étape, entrez `${original.file}`.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `\$\{(\w+.\w+)\}`

Obligatoire : non

Target

ARN Pour la fonction Lambda qui est appelée.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 170.

Modèle : `arn:[a-z-]+:lambda:.*`

Obligatoire : non

TimeoutSeconds

Délai d'expiration, en secondes, pour l'étape.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 1800.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

DecryptStepDetails

Chaque type d'étape possède sa propre `StepDetails` structure.

Table des matières

DestinationFileLocation

Spécifie l'emplacement du fichier en cours de déchiffrement. Utilisez `${Transfer:UserName}` ou `${Transfer:UploadDate}` dans ce champ pour paramétrer le préfixe de destination par nom d'utilisateur ou date de téléchargement.

- Définissez la valeur de `DestinationFileLocation` `${Transfer:UserName}` to pour déchiffrer les fichiers téléchargés dans un compartiment Amazon S3 préfixé par le nom de l'utilisateur de Transfer Family qui a chargé le fichier.
- Définissez la valeur de `DestinationFileLocation` `${Transfer:UploadDate}` to pour déchiffrer les fichiers téléchargés dans un compartiment Amazon S3 préfixé par la date du téléchargement.

Note

Le système adopte le format `UploadDate` de date `YYYY-MM-DD`, en fonction de la date à laquelle le fichier est chargé. UTC

Type : objet [InputFileLocation](#)

Obligatoire : oui

Type

Type de cryptage utilisé. Actuellement, cette valeur doit être PGP.

Type : String

Valeurs valides : PGP

Obligatoire : oui

Name

Le nom de l'étape, utilisé comme identifiant.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 30

Modèle : `[\w-]*`

Obligatoire : non

OverwriteExisting

Un indicateur qui indique s'il faut écraser un fichier existant portant le même nom. L'argument par défaut est FALSE.

Si le flux de travail traite un fichier portant le même nom qu'un fichier existant, le comportement est le suivant :

- Si tel `OverwriteExisting` est le cas `TRUE`, le fichier existant est remplacé par le fichier en cours de traitement.
- Si tel `OverwriteExisting` est `FALSE` le cas, rien ne se passe et le traitement du flux de travail s'arrête.

Type : String

Valeurs valides : `TRUE` | `FALSE`

Obligatoire : non

SourceFileLocation

Spécifie le fichier à utiliser comme entrée pour l'étape du flux de travail : soit le résultat de l'étape précédente, soit le fichier initialement chargé pour le flux de travail.

- Pour utiliser le fichier précédent comme entrée, entrez `${previous.file}`. Dans ce cas, cette étape du flux de travail utilise le fichier de sortie de l'étape précédente du flux de travail comme entrée. C'est la valeur par défaut.
- Pour utiliser l'emplacement du fichier initialement chargé comme entrée pour cette étape, entrez `${original.file}`.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `\$\{(\w+.\w+)\}`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DeleteStepDetails

Nom de l'étape, utilisé pour identifier l'étape de suppression.

Table des matières

Name

Le nom de l'étape, utilisé comme identifiant.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 30

Modèle : `[\w-]*`

Obligatoire : non

SourceFileLocation

Spécifie le fichier à utiliser comme entrée pour l'étape du flux de travail : soit le résultat de l'étape précédente, soit le fichier initialement chargé pour le flux de travail.

- Pour utiliser le fichier précédent comme entrée, entrez `${previous.file}`. Dans ce cas, cette étape du flux de travail utilise le fichier de sortie de l'étape précédente du flux de travail comme entrée. C'est la valeur par défaut.
- Pour utiliser l'emplacement du fichier initialement chargé comme entrée pour cette étape, entrez `${original.file}`.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `\$\{(\w+.\w+)\}`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedAccess

Décrit les propriétés de l'accès spécifié.

Table des matières

ExternalId

Identifiant unique requis pour identifier des groupes spécifiques au sein de votre annuaire.

Les utilisateurs du groupe que vous associez ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family. Si vous connaissez le nom du groupe, vous pouvez afficher les SID valeurs en exécutant la commande suivante sous Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties  
* | Select SamAccountName, ObjectSid
```

Dans cette commande, remplacez YourGroupName par le nom de votre groupe Active Directory.

L'expression régulière utilisée pour valider ce paramètre est une chaîne de caractères composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez également inclure des traits de soulignement ou l'un des caractères suivants : =, . @ : /-

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : S-1-[\d-]+

Obligatoire : non

HomeDirectory

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de HomeDirectory est /bucket_name/home/mydirectory.

Note

Le paramètre HomeDirectory est uniquement utilisé si HomeDirectoryType est défini sur la valeur PATH.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : (| / . *)

Obligatoire : non

HomeDirectoryMappings

Des mappages de répertoires logiques qui spécifient quels EFS chemins et clés Amazon S3 ou Amazon doivent être visibles par votre utilisateur et comment vous souhaitez les rendre visibles. Vous devez spécifier la Target paire Entry et, qui Entry indique comment le chemin est rendu visible et Target correspond au EFS chemin Amazon S3 ou Amazon réel. Si vous spécifiez uniquement une cible, elle est affichée telle quelle. Vous devez également vous assurer que votre rôle AWS Identity and Access Management (IAM) donne accès aux chemins d'accèsTarget. Cette valeur ne peut être définie que si elle HomeDirectoryType est définie sur LOGICAL.

Dans la plupart des cas, vous pouvez utiliser cette valeur au lieu de la politique de session pour verrouiller l'accès associé au répertoire de base désigné (« chroot »). Pour ce faire, vous pouvez Entry régler sur «/» et Target définir la valeur du HomeDirectory paramètre.

Type : tableau d'objets [HomeDirectoryMapEntry](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 50 000 articles.

Obligatoire : non

HomeDirectoryType

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez surPATH, l'utilisateur verra le bucket Amazon S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez surLOGICAL, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

Note

Dans HomeDirectoryType l'affirmativeLOGICAL, vous devez fournir des mappages à l'aide du HomeDirectoryMappings paramètre. Si, en revanche, HomeDirectoryType c'est le casPATH, vous fournissez un chemin absolu à l'aide du

HomeDirectory paramètre. Vous ne pouvez pas avoir les deux HomeDirectory et HomeDirectoryMappings dans votre modèle.

Type : String

Valeurs valides : PATH | LOGICAL

Obligatoire : non

Policy

Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même rôle AWS Identity and Access Management (IAM) pour plusieurs utilisateurs. Cette politique limite l'accès d'un utilisateur à certaines parties de son compartiment Amazon S3. Les variables que vous pouvez utiliser à l'intérieur de cette politique incluent `${Transfer:UserName}`, `${Transfer:HomeDirectory}` et `${Transfer:HomeBucket}`.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

PosixProfile

L'POSIXidentité complète, y compris l'ID utilisateur (Uid), l'ID de groupe (Gid) et tout groupe secondaire IDs (SecondaryGids), qui contrôle l'accès de vos utilisateurs à vos systèmes de EFS fichiers Amazon. Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Type : objet [PosixProfile](#)

Obligatoire : non

Role

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une

relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

DescribedAgreement

Décrit les propriétés d'un accord.

Table des matières

Arn

Le nom unique de la ressource Amazon (ARN) pour le contrat.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

AccessRole

Les connecteurs sont utilisés pour envoyer des fichiers en utilisant le SFTP protocole AS2 or. Pour le rôle d'accès, indiquez le nom de ressource Amazon (ARN) du AWS Identity and Access Management rôle à utiliser.

Pour AS2 connecteurs

AvecAS2, vous pouvez envoyer des fichiers en appelant `StartFileTransfer` et en spécifiant les chemins des fichiers dans le paramètre de requête, `SendFilePaths`. Nous utilisons le répertoire parent du fichier (par exemple, `--send-file-paths /bucket/dir/file.txt`, le répertoire parent est `/bucket/dir/`) pour stocker temporairement un fichier de AS2 message traité, le stocker MDN lorsque nous le recevons du partenaire et écrire un JSON fichier final contenant les métadonnées pertinentes de la transmission. Ainsi, le `AccessRole` doit fournir un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la requête `StartFileTransfer`. En outre, vous devez fournir un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer avec `StartFileTransfer`.

Si vous utilisez l'authentification de base pour votre AS2 connecteur, le rôle d'accès nécessite `secretsmanager:GetSecretValue` autorisation d'accès au secret. Si le secret est chiffré à l'aide d'une clé gérée par le client au lieu de la clé AWS gérée dans Secrets Manager, le rôle doit également disposer d'une `kms:Decrypt` autorisation pour cette clé.

Pour SFTP connecteurs

Assurez-vous que le rôle d'accès fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande. En outre, assurez-vous que le rôle fournit `secretsmanager:GetSecretValue` l'autorisation de AWS Secrets Manager.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

AgreementId

Identifiant unique pour l'accord. Cet identifiant est renvoyé lorsque vous créez un accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `a-([0-9a-f]{17})`

Obligatoire : non

BaseDirectory

Le répertoire de destination (dossier) pour les fichiers transférés à l'aide du AS2 protocole.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `(|/.*)`

Obligatoire : non

Description

Le nom ou la brève description qui est utilisé pour identifier l'accord.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : `[\p{Graph}]+`

Obligatoire : non

LocalProfileId

Identifiant unique pour le profil AS2 local.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : non

PartnerProfileId

Un identifiant unique pour le profil de partenaire utilisé dans l'accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : non

ServerId

Identifiant unique attribué par le système pour une instance de serveur. Cet identifiant indique le serveur spécifique utilisé par l'accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : non

Status

L'état actuel de l'accord, soit ACTIVE ou INACTIVE.

Type : String

Valeurs valides : ACTIVE | INACTIVE

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des accords.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedCertificate

Décrit les propriétés d'un certificat.

Table des matières

Arn

Nom de ressource Amazon unique (ARN) pour le certificat.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

ActiveDate

Une date facultative qui indique à quel moment le certificat devient actif.

Type : Timestamp

Obligatoire : non

Certificate

Le nom du fichier du certificat.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 16384.

Modèle : `[\u0009\u000A\u000D\u0020-\u00FF]*`

Obligatoire : non

CertificateChain

La liste des certificats qui constituent la chaîne du certificat.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2097152.

Modèle : [\u0009\u000A\u000D\u0020-\u00FF]*

Obligatoire : non

CertificateId

Un tableau d'identifiants pour les certificats importés. Vous utilisez cet identifiant pour travailler avec des profils et des profils de partenaires.

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : cert-([0-9a-f]{17})

Obligatoire : non

Description

Le nom ou la description utilisé pour identifier le certificat.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : [\p{Graph}]+

Obligatoire : non

InactiveDate

Une date facultative qui indique à quel moment le certificat devient inactif.

Type : Timestamp

Obligatoire : non

NotAfterDate

La date limite de validité du certificat.

Type : Timestamp

Obligatoire : non

NotBeforeDate

La date la plus proche à laquelle le certificat est valide.

Type : Timestamp

Obligatoire : non

Serial

Le numéro de série du certificat.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 48

Modèle : `[\p{XDigit}{2}:?]*`

Obligatoire : non

Status

Le certificat peut être soit ACTIVE, PENDING_ROTATION, ou INACTIVE. PENDING_ROTATION signifie que ce certificat remplacera le certificat actuel à son expiration.

Type : String

Valeurs valides : ACTIVE | PENDING_ROTATION | INACTIVE

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des certificats.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Type

Si une clé privée a été spécifiée pour le certificat, son type est CERTIFICATE_WITH_PRIVATE_KEY. S'il n'y a pas de clé privée, le type est CERTIFICATE.

Type : String

Valeurs valides : CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY

Obligatoire : non

Usage

Spécifie si ce certificat est utilisé pour la signature ou le chiffrement.

Type : String

Valeurs valides : SIGNING | ENCRYPTION

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedConnector

Décrit les paramètres du connecteur, tels qu'identifiés par leConnectorId.

Table des matières

Arn

Nom de ressource Amazon unique (ARN) pour le connecteur.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : arn:\S+

Obligatoire : oui

AccessRole

Les connecteurs sont utilisés pour envoyer des fichiers en utilisant le SFTP protocole AS2 or. Pour le rôle d'accès, indiquez le nom de ressource Amazon (ARN) du AWS Identity and Access Management rôle à utiliser.

Pour AS2 connecteurs

AvecAS2, vous pouvez envoyer des fichiers en appelant StartFileTransfer et en spécifiant les chemins des fichiers dans le paramètre de requête,SendFilePaths. Nous utilisons le répertoire parent du fichier (par exemple, car--send-file-paths /bucket/dir/file.txt, le répertoire parent est/bucket/dir/) pour stocker temporairement un fichier de AS2 message traité, le stocker MDN lorsque nous le recevons du partenaire et écrire un JSON fichier final contenant les métadonnées pertinentes de la transmission. Ainsi, le AccessRole doit fournir un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la requête StartFileTransfer. En outre, vous devez fournir un accès en lecture et en écriture au répertoire parent des fichiers que vous souhaitez envoyer avec StartFileTransfer.

Si vous utilisez l'authentification de base pour votre AS2 connecteur, le rôle d'accès nécessite l'secretsmanager:GetSecretValueautorisation d'accès au secret. Si le secret est chiffré à l'aide d'une clé gérée par le client au lieu de la clé AWS gérée dans Secrets Manager, le rôle doit également disposer d'une kms:Decrypt autorisation pour cette clé.

Pour SFTP connecteurs

Assurez-vous que le rôle d'accès fournit un accès en lecture et en écriture au répertoire parent de l'emplacement du fichier utilisé dans la `StartFileTransfer` demande. Assurez-vous également que le rôle fournit l'`secretsmanager:GetSecretValue` autorisation de AWS Secrets Manager.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

As2Config

Structure contenant les paramètres d'un objet AS2 connecteur.

Type : objet [As2ConnectorConfig](#)

Obligatoire : non

ConnectorId

Identifiant unique du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `c-([0-9a-f]{17})`

Obligatoire : non

LoggingRole

Nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un connecteur d'activer la CloudWatch journalisation des événements Amazon S3. Lorsque cette option est configurée, vous pouvez consulter l'activité du connecteur dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

ServiceManagedEgressIpAddresses

Liste des adresses IP de sortie de ce connecteur. Ces adresses IP sont attribuées automatiquement lorsque vous créez le connecteur.

Type : tableau de chaînes

Modèle : \d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}

Obligatoire : non

SftpConfig

Structure contenant les paramètres d'un objet SFTP connecteur.

Type : objet [SftpConnectorConfig](#)

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des connecteurs.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Url

Celui URL du partenaire AS2 ou du SFTP point final.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 255.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedExecution

Détails d'un objet d'exécution.

Table des matières

ExecutionId

Identifiant unique pour l'exécution d'un flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 36.

Modèle : `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatoire : non

ExecutionRole

IAM Rôle associé à l'exécution.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

InitialFileLocation

Structure qui décrit l'Amazon S3 ou l'emplacement EFS du fichier. Il s'agit de l'emplacement du fichier lorsque l'exécution commence : si le fichier est copié, il s'agit de l'emplacement du fichier initial (et non de destination).

Type : objet [FileLocation](#)

Obligatoire : non

LoggingConfiguration

Rôle de IAM journalisation associé à l'exécution.

Type : objet [LoggingConfiguration](#)

Obligatoire : non

PosixProfile

L'POSIXidentité complète, y compris l'ID utilisateur (Uid), l'ID de groupe (Gid) et tout groupe secondaire IDs (SecondaryGids), qui contrôle l'accès de vos utilisateurs à vos systèmes de EFS fichiers Amazon. Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Type : objet [PosixProfile](#)

Obligatoire : non

Results

Structure qui décrit les résultats de l'exécution. Cela inclut une liste des étapes ainsi que les détails de chaque étape, le type d'erreur et le message (le cas échéant), ainsi que la OnExceptionSteps structure.

Type : objet [ExecutionResults](#)

Obligatoire : non

ServiceMetadata

Objet conteneur pour les détails de session associés à un flux de travail.

Type : objet [ServiceMetadata](#)

Obligatoire : non

Status

Le statut est celui de l'exécution. Peut être en cours, terminé, une exception rencontrée ou être en cours de traitement.

Type : String

Valeurs valides : IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedHostKey

Les détails d'une clé d'hôte de serveur.

Table des matières

Arn

Nom de ressource Amazon unique (ARN) pour la clé d'hôte.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

DateImported

Date à laquelle la clé d'hôte a été ajoutée au serveur.

Type : Timestamp

Obligatoire : non

Description

Description textuelle de cette clé d'hôte.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `[\p{Print}]*`

Obligatoire : non

HostKeyFingerprint

L'empreinte de clé publique, qui est une courte séquence d'octets utilisée pour identifier la clé publique la plus longue.

Type : chaîne

Obligatoire : non

HostKeyId

Identifiant unique pour la clé d'hôte.

Type : String

Contraintes de longueur : longueur fixe de 25.

Modèle : `hostkey-[0-9a-f]{17}`

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des clés d'hôte.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Type

Algorithme de chiffrement utilisé pour la clé d'hôte. Le Type paramètre est spécifié à l'aide de l'une des valeurs suivantes :

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedProfile

Informations relatives à un profil local ou à un AS2 profil de partenaire.

Table des matières

Arn

Nom de ressource Amazon unique (ARN) pour le profil.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

As2Id

As2Id s'agit du AS2-name, tel que défini dans le [RFC4130](#). Pour les transferts entrants, il s'agit de l'AS2-Fromen-tête des AS2 messages envoyés par le partenaire. Pour les connecteurs sortants, il s'agit de l'AS2-Toen-tête des AS2 messages envoyés au partenaire à l'aide de l'`StartFileTransferAPI`opération. Cet identifiant ne peut pas inclure d'espaces.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : `[\p{Print}\s]*`

Obligatoire : non

CertificateIds

Un tableau d'identifiants pour les certificats importés. Vous utilisez cet identifiant pour travailler avec des profils et des profils de partenaires.

Type : tableau de chaînes

Contraintes de longueur : longueur fixe de 22.

Modèle : `cert-([0-9a-f]{17})`

Obligatoire : non

ProfileId

Identifiant unique pour le profil local ou le AS2 profil du partenaire.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : non

ProfileType

Indique s'il faut répertorier uniquement les profils de type LOCAL ou uniquement les profils de type PARTNER. Si elle n'est pas fournie dans la demande, la commande répertorie tous les types de profils.

Type : String

Valeurs valides : LOCAL | PARTNER

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des profils.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)

- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedSecurityPolicy

Décrit les propriétés d'une politique de sécurité spécifiée. Pour plus d'informations sur les politiques de sécurité, consultez la section [Utilisation des politiques de sécurité](#).

Table des matières

SecurityPolicyName

Spécifie le nom de la politique de sécurité attachée au serveur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 100.

Modèle : TransferSecurityPolicy-.+

Obligatoire : oui

Fips

Spécifie si cette politique active les normes fédérales de traitement de l'information (FIPS).

Type : booléen

Obligatoire : non

SshCiphers

Spécifie les algorithmes de chiffrement Secure Shell (SSH) activés dans la politique de sécurité attachée au serveur.

Type : tableau de chaînes

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 50.

Obligatoire : non

SshKexs

Spécifie les algorithmes de chiffrement par échange de SSH clés (KEX) activés dans la politique de sécurité attachée au serveur.

Type : tableau de chaînes

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 50.

Obligatoire : non

SshMacs

Spécifie les algorithmes de chiffrement du code d'authentification des SSH messages (MAC) activés dans la politique de sécurité attachée au serveur.

Type : tableau de chaînes

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 50.

Obligatoire : non

TlsCiphers

Spécifie les algorithmes de chiffrement Transport Layer Security (TLS) activés dans la politique de sécurité attachée au serveur.

Type : tableau de chaînes

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 50.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

DescribedServer

Décrit les propriétés d'un serveur compatible avec le protocole de transfert de fichiers spécifié.

Table des matières

Arn

Spécifie le nom de ressource Amazon unique (ARN) du serveur.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

As2ServiceManagedEgressIpAddresses

La liste des adresses IP de sortie de ce serveur. Ces adresses IP ne sont pertinentes que pour les serveurs qui utilisent le AS2 protocole. Ils sont utilisés pour l'envoi asynchroneMDNs.

Ces adresses IP sont attribuées automatiquement lorsque vous créez un AS2 serveur. En outre, si vous mettez à jour un serveur existant et ajoutez le AS2 protocole, des adresses IP statiques sont également attribuées.

Type : tableau de chaînes

Modèle : `\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`

Obligatoire : non

Certificate

Spécifie ARN le AWS certificat Certificate Manager (ACM). Obligatoire lorsque `Protocols` est défini sur `FTPS`.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 1600.

Obligatoire : non

Domain

Spécifie le domaine du système de stockage utilisé pour les transferts de fichiers.

Type : String

Valeurs valides : S3 | EFS

Obligatoire : non

EndpointDetails

Les paramètres de point de terminaison du cloud privé virtuel (VPC) configurés pour votre serveur. Lorsque vous hébergez votre point de terminaison dans votre environnement VPC, vous pouvez le rendre accessible uniquement aux ressources qu'il contient, ou vous pouvez associer des adresses IP élastiques et rendre votre point de terminaison accessible aux clients via Internet. Les groupes VPC de sécurité par défaut de votre choix sont automatiquement attribués à votre terminal.

Type : objet [EndpointDetails](#)

Obligatoire : non

EndpointType

Définit le type de point de terminaison auquel votre serveur est connecté. Si votre serveur est connecté à un VPC point de terminaison, il n'est pas accessible via l'Internet public.

Type : String

Valeurs valides : PUBLIC | VPC | VPC_ENDPOINT

Obligatoire : non

HostKeyFingerprint

Spécifie l'empreinte SHA256 codée en Base64 de la clé d'hôte du serveur. Cette valeur est équivalente à la sortie de la commande `ssh-keygen -l -f my-new-server-key`.

Type : chaîne

Obligatoire : non

IdentityProviderDetails

Spécifie les informations permettant d'appeler une authentification fournie par le client.

API Ce champ n'est pas renseigné lorsque le IdentityProviderType d'un serveur est AWS_DIRECTORY_SERVICE ou SERVICE_MANAGED.

Type : objet [IdentityProviderDetails](#)

Obligatoire : non

IdentityProviderType

Le mode d'authentification pour un serveur. La valeur par défaut est SERVICE_MANAGED, ce qui vous permet de stocker et d'accéder aux informations d'identification des utilisateurs au sein du AWS Transfer Family service.

AWS_DIRECTORY_SERVICE À utiliser pour fournir un accès aux groupes Active Directory AWS Directory Service for Microsoft Active Directory ou à Microsoft Active Directory dans votre environnement local ou à l' AWS aide d'AD Connector. Cette option exige également que vous indiquiez un ID de répertoire en utilisant le paramètre IdentityProviderDetails.

Utilisez la valeur API_GATEWAY à intégrer au fournisseur d'identité de votre choix. Le API_GATEWAY paramètre vous oblige à fournir un point de terminaison Amazon API Gateway URL à appeler pour l'authentification à l'aide du IdentityProviderDetails paramètre.

Utilisez la AWS_LAMBDA valeur pour utiliser directement une AWS Lambda fonction en tant que fournisseur d'identité. Si vous choisissez cette valeur, vous devez spécifier la ARN fonction Lambda dans le Function paramètre du type de IdentityProviderDetails données.

Type : String

Valeurs valides : SERVICE_MANAGED | API_GATEWAY | AWS_DIRECTORY_SERVICE | AWS_LAMBDA

Obligatoire : non

LoggingRole

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un serveur d'activer la CloudWatch journalisation Amazon pour Amazon S3 ou AmazonEFS events. Lorsque cette option est configurée, vous pouvez consulter l'activité des utilisateurs dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Modèle : (|arn:.*role/\S+)

Obligatoire : non

PostAuthenticationLoginBanner

Spécifie une chaîne à afficher lorsque les utilisateurs se connectent à un serveur. Cette chaîne s'affiche une fois l'utilisateur authentifié.

Note

Le SFTP protocole ne prend pas en charge les bannières d'affichage après authentification.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Modèle : [\x09-\x0D\x20-\x7E]*

Obligatoire : non

PreAuthenticationLoginBanner

Spécifie une chaîne à afficher lorsque les utilisateurs se connectent à un serveur. Cette chaîne est affichée avant que l'utilisateur ne s'authentifie. Par exemple, la bannière suivante affiche des informations sur l'utilisation du système :

```
This system is for the use of authorized users only. Individuals using  
this computer system without authority, or in excess of their authority,  
are subject to having all of their activities on this system monitored  
and recorded by system personnel.
```

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 4096.

Modèle : `[\x09-\x0D\x20-\x7E]*`

Obligatoire : non

ProtocolDetails

Les paramètres du protocole qui sont configurés pour votre serveur.

- Pour indiquer le mode passif (pour FTP et FTPS protocoles), utilisez le `PassiveIp` paramètre. Entrez une seule adresse à quatre points, telle que IPv4 l'adresse IP externe d'un pare-feu, d'un routeur ou d'un équilibreur de charge.
- Pour ignorer l'erreur qui est générée lorsque le client tente d'utiliser la commande `SETSTAT` sur un fichier que vous téléchargez vers un compartiment Amazon S3, utilisez le paramètre `SetStatOption`. Pour que le AWS Transfer Family serveur ignore la `SETSTAT` commande et télécharge les fichiers sans avoir à apporter de modifications à votre SFTP client, définissez la valeur sur `ENABLE_NO_OP`. Si vous définissez le `SetStatOption` paramètre sur `ENABLE_NO_OP`, Transfer Family génère une entrée de journal dans Amazon CloudWatch Logs, afin que vous puissiez déterminer à quel moment le client passe un `SETSTAT` appel.
- Pour déterminer si votre AWS Transfer Family serveur reprend les sessions récemment négociées via un identifiant de session unique, utilisez le `TlsSessionResumptionMode` paramètre.
- `As2Transports` indique le mode de transport des AS2 messages. Actuellement, seul HTTP est pris en charge.

Type : objet [ProtocolDetails](#)

Obligatoire : non

Protocols

Spécifie le ou les protocoles de transfert de fichiers sur lesquels votre client de protocole de transfert de fichiers peut se connecter au point de terminaison de votre serveur. Les protocoles disponibles sont :

- SFTP(Secure Shell (SSH) File Transfer Protocol) : transfert de fichiers effectué SSH
- FTPS(Protocole de transfert de fichiers sécurisé) : transfert de fichiers avec TLS cryptage
- FTP (Protocole de transfert de fichiers) : Transfert de fichiers non chiffré
- AS2(Déclaration d'applicabilité 2) : utilisé pour le transport de données structurées business-to-business

 Note

- Si vous le sélectionnez FTPS, vous devez choisir un certificat stocké dans AWS Certificate Manager (ACM) qui est utilisé pour identifier votre serveur lorsque des clients s'y connectent FTPS.
- Si Protocol comprend FTP ou FTPS, EndpointType doit être défini sur VPC, et IdentityProviderType sur AWS_DIRECTORY_SERVICE, AWS_LAMBDA ou API_GATEWAY.
- Si Protocol inclut FTP, alors AddressAllocationIds ne peut pas être associé.
- Si Protocol est uniquement défini sur SFTP, EndpointType peut être défini sur PUBLIC, et IdentityProviderType peut être défini comme l'un des types d'identité pris en charge : SERVICE_MANAGED, AWS_DIRECTORY_SERVICE, AWS_LAMBDA ou API_GATEWAY.
- Si Protocol inclut AS2, alors le EndpointType doit être VPC, et le domaine doit être Amazon S3.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 4 articles.

Valeurs valides : SFTP | FTP | FTPS | AS2

Obligatoire : non

S3StorageOptions

Spécifie si les performances de vos annuaires Amazon S3 sont optimisées ou non. Par défaut, l'option est désactivée.

Par défaut, les mappages du répertoire de base ont la valeur TYPE de DIRECTORY.

Si vous activez cette option, vous devrez alors définir explicitement la valeur sur HomeDirectoryMapEntry Type FILE si vous souhaitez qu'un mappage ait une cible de fichier.

Type : objet [S3StorageOptions](#)

Obligatoire : non

SecurityPolicyName

Spécifie le nom de la politique de sécurité attachée au serveur.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 100.

Modèle : TransferSecurityPolicy-.+

Obligatoire : non

ServerId

Spécifie l'identifiant unique attribué par le système à un serveur que vous instanciez.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : non

State

État du serveur décrit. La valeur de ONLINE indique que le serveur peut accepter des tâches et transférer des fichiers. StateLa valeur de OFFLINE signifie que le serveur ne peut pas effectuer d'opérations de transfert de fichiers.

Les états de STARTING et STOPPING indiquent que le serveur est dans un état intermédiaire, qu'il n'est pas totalement en mesure de répondre ou qu'il n'est pas complètement hors ligne. Les valeurs de START_FAILED ou STOP_FAILED peuvent indiquer une condition d'erreur.

Type : String

Valeurs valides : OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED

Obligatoire : non

StructuredLogDestinations

Spécifie les groupes de journaux auxquels les journaux de votre serveur sont envoyés.

Pour spécifier un groupe de journaux, vous devez fournir le correspondant ARN à un groupe de journaux existant. Dans ce cas, le format du groupe de logs est le suivant :

arn:aws:logs:region-name:amazon-account-id:log-group:log-group-name:*

Par exemple, `arn:aws:logs:us-east-1:111122223333:log-group:mytestgroup:*`

Si vous avez déjà spécifié un groupe de journaux pour un serveur, vous pouvez l'effacer, et donc désactiver la journalisation structurée, en fournissant une valeur vide pour ce paramètre dans un `update-server` appel. Par exemple :

```
update-server --server-id s-1234567890abcdef0 --structured-log-destinations
```

Type : tableau de chaînes

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : non

Tags

Spécifie les paires clé-valeur que vous pouvez utiliser pour rechercher et regrouper les serveurs assignés au serveur décrit.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

UserCount

Spécifie le nombre d'utilisateurs affectés à un serveur que vous avez spécifié avec `leServerId`.

Type : entier

Obligatoire : non

WorkflowDetails

Spécifie l'ID du flux de travail à attribuer et le rôle d'exécution utilisé pour exécuter le flux de travail.

En plus d'un flux de travail à exécuter lorsqu'un fichier est complètement chargé, `WorkflowDetails` peut également contenir un ID de flux de travail (et un rôle d'exécution)

pour un flux de travail à exécuter lors d'un chargement partiel. Un téléchargement partiel se produit lorsque la session du serveur se déconnecte alors que le fichier est toujours en cours de téléchargement.

Type : objet [WorkflowDetails](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedUser

Décrit les propriétés d'un utilisateur spécifié.

Table des matières

Arn

Spécifie le nom unique de la ressource Amazon (ARN) pour l'utilisateur dont la description a été demandée.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

HomeDirectory

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de HomeDirectory est `/bucket_name/home/mydirectory`.

Note

Le paramètre HomeDirectory est uniquement utilisé si HomeDirectoryType est défini sur la valeur PATH.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `(|/.*)`

Obligatoire : non

HomeDirectoryMappings

Des mappages de répertoires logiques qui spécifient quels EFS chemins et clés Amazon S3 ou Amazon doivent être visibles par votre utilisateur et comment vous souhaitez les rendre visibles.

Vous devez spécifier la Target paire Entry et, qui Entry indique comment le chemin est rendu visible et Target correspond au EFS chemin Amazon S3 ou Amazon réel. Si vous spécifiez uniquement une cible, elle est affichée telle quelle. Vous devez également vous assurer que votre rôle AWS Identity and Access Management (IAM) donne accès aux chemins d'accèsTarget. Cette valeur ne peut être définie que si elle HomeDirectoryType est définie sur LOGICAL.

Dans la plupart des cas, vous pouvez utiliser cette valeur au lieu de la politique de session pour verrouiller votre utilisateur dans le répertoire de base désigné (« chroot »). Pour ce faire, vous pouvez Entry régler sur «/» et Target définir la valeur du HomeDirectory paramètre.

Type : tableau d'objets [HomeDirectoryMapEntry](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 50 000 articles.

Obligatoire : non

HomeDirectoryType

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez surPATH, l'utilisateur verra le bucket Amazon S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez surLOGICAL, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

 Note

Dans HomeDirectoryType l'affirmativeLOGICAL, vous devez fournir des mappages à l'aide du HomeDirectoryMappings paramètre. Si, en revanche, HomeDirectoryType c'est le casPATH, vous fournissez un chemin absolu à l'aide du HomeDirectory paramètre. Vous ne pouvez pas avoir les deux HomeDirectory et HomeDirectoryMappings dans votre modèle.

Type : String

Valeurs valides : PATH | LOGICAL

Obligatoire : non

Policy

Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même rôle AWS Identity and Access Management (IAM) pour plusieurs utilisateurs. Cette politique limite l'accès d'un utilisateur à certaines parties de son compartiment Amazon S3. Les variables que vous pouvez utiliser à l'intérieur de cette politique incluent `${Transfer:UserName}`, `${Transfer:HomeDirectory}` et `${Transfer:HomeBucket}`.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : non

PosixProfile

Spécifie l'POSIXidentité complète, y compris l'ID utilisateur (Uid), l'ID de groupe (Gid) et tout groupe secondaire IDs (SecondaryGids), qui contrôle l'accès de vos utilisateurs à vos systèmes de fichiers Amazon Elastic File System (AmazonEFS). Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Type : objet [PosixProfile](#)

Obligatoire : non

Role

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

SshPublicKeys

Spécifie la partie clé publique des clés Secure Shell (SSH) stockées pour l'utilisateur décrit.

Type : tableau d'objets [SshPublicKey](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 5 éléments.

Obligatoire : non

Tags

Spécifie les paires clé-valeur pour l'utilisateur demandé. Le tag peut être utilisé pour rechercher et regrouper des utilisateurs à diverses fins.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

UserName

Spécifie le nom de l'utilisateur dont la description a été demandée. Les noms d'utilisateur sont utilisés à des fins d'authentification. Il s'agit de la chaîne qui sera utilisée par votre utilisateur lorsqu'il se connectera à votre serveur.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)

- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

DescribedWorkflow

Décrit les propriétés du flux de travail spécifié

Table des matières

Arn

Spécifie le nom unique de la ressource Amazon (ARN) pour le flux de travail.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

Description

Spécifie la description textuelle pour le flux de travail.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `[\w- ]*`

Obligatoire : non

OnExceptionSteps

Spécifie les étapes (actions) à suivre en cas d'erreur lors de l'exécution du flux de travail.

Type : tableau d'objets [WorkflowStep](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 8 articles.

Obligatoire : non

Steps

Spécifie les détails des étapes qui se trouvent dans le flux de travail spécifié.

Type : tableau d'objets [WorkflowStep](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 8 articles.

Obligatoire : non

Tags

Paires clé-valeur qui peuvent être utilisées pour regrouper et rechercher des flux de travail. Les balises sont des métadonnées associées aux flux de travail pour différents motifs.

Type : tableau d'objets [Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : w-([a-z0-9]{17})

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

EfsFileLocation

Spécifie les détails de l'emplacement du fichier utilisé dans le flux de travail. Applicable uniquement si vous utilisez Amazon Elastic File Systems (AmazonEFS) pour le stockage.

Table des matières

FileSystemId

L'identifiant du système de fichiers, attribué par AmazonEFS.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 128.

Modèle : (arn:aws[-a-z]*:elasticfilesystem:[0-9a-z-:]+:(access-point/fsap|file-system/fs)-[0-9a-f]{8,40}|fs(ap)?-[0-9a-f]{8,40})

Obligatoire : non

Path

Le nom du chemin du dossier utilisé par un flux de travail.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 65536.

Modèle : [^\x00]+

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

EndpointDetails

Les paramètres de point de terminaison du cloud privé virtuel (VPC) configurés pour votre serveur compatible avec le protocole de transfert de fichiers. Avec un VPC point de terminaison, vous pouvez restreindre l'accès à votre serveur et aux ressources uniquement au sein de votre VPC. Pour contrôler le trafic Internet entrant, invoquez l'adresse IP élastique UpdateServer API et associez une adresse IP élastique au point de terminaison de votre serveur.

Note

Après le 19 mai 2021, vous ne pourrez plus créer de serveur `EndpointType=VPC_ENDPOINT` à l'aide de votre AWS compte si celui-ci ne l'a pas déjà fait avant le 19 mai 2021. Si vous avez déjà créé des serveurs `EndpointType=VPC_ENDPOINT` dans votre AWS compte le 19 mai 2021 ou avant, vous ne serez pas concerné. Après cette date, utilisez `EndpointType =VPC`.

Pour de plus amples informations, veuillez consulter [Cessation de l'utilisation de _ VPC ENDPOINT](#).

Table des matières

AddressAllocationIds

Liste des allocations IDs d'adresses requises pour associer une adresse IP élastique au point de terminaison de votre serveur.

Un ID d'allocation d'adresse correspond à l'ID d'allocation d'une adresse IP Elastic. Cette valeur peut être extraite du `allocationId` champ à partir du type de données Amazon EC2 [Address](#). Une façon de récupérer cette valeur est d'appeler le EC2 [DescribeAddresses](#) API.

Ce paramètre est facultatif. Définissez ce paramètre si vous souhaitez rendre votre VPC point de terminaison accessible au public. Pour plus de détails, voir [Création d'un point de terminaison connecté à Internet pour votre serveur](#).

Note

Cette propriété ne peut être définie que comme suit :

- `EndpointType` doit être réglé sur VPC
- Le serveur Transfer Family doit être hors ligne.

- Vous ne pouvez pas définir ce paramètre pour les serveurs Transfer Family qui utilisent le FTP protocole.
- Le serveur doit déjà être SubnetIds renseigné (SubnetIdset AddressAllocationIds ne peut pas être mis à jour simultanément).
- AddressAllocationIds ne peut pas contenir de doublons et doit être d'une longueur égale à SubnetIds. Par exemple, si vous avez trois sous-réseauxIDs, vous devez également spécifier trois allocations IDs d'adresses.
- Appelez le UpdateServer API pour définir ou modifier ce paramètre.

Type : tableau de chaînes

Obligatoire : non

SecurityGroupIds

Liste des groupes de sécurité IDs que vous pouvez associer au point de terminaison de votre serveur.

 Note

Cette propriété ne peut être définie que lorsque EndpointType est défini sur VPC. Vous ne pouvez modifier la SecurityGroupIds propriété [UpdateServerAPI](#) que si vous modifiez le EndpointType de PUBLIC ou le VPC_ENDPOINT vers VPC. Pour modifier les groupes de sécurité associés au VPC point de terminaison de votre serveur après sa création, utilisez Amazon EC2 [ModifyVpcEndpointAPI](#).

Type : tableau de chaînes

Contraintes de longueur : longueur minimale de 11. Longueur maximale de 20.

Modèle : sg-[0-9a-f]{8,17}

Obligatoire : non

SubnetIds

Liste des IDs sous-réseaux nécessaires pour héberger le point de terminaison de votre serveur dans votre VPC.

 Note

Cette propriété ne peut être définie que lorsque `EndpointType` est défini sur VPC.

Type : tableau de chaînes

Obligatoire : non

`VpcEndpointId`

Identifiant du VPC point de terminaison.

 Note

Cette propriété ne peut être définie que lorsque `EndpointType` est défini sur `VPC_ENDPOINT`.

Pour de plus amples informations, veuillez consulter [Cessation de l'utilisation de _ VPC ENDPOINT](#).

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : `vpce-[0-9a-f]{17}`

Obligatoire : non

`VpcId`

L'ID d'identification VPC dans lequel le point de terminaison d'un serveur sera hébergé.

 Note

Cette propriété ne peut être définie que lorsque `EndpointType` est défini sur VPC.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ExecutionError

Spécifie le message et le type d'erreur pour une erreur survenue lors de l'exécution du flux de travail.

Table des matières

Message

Spécifie le message descriptif correspondant au `ErrorType`.

Type : String

Obligatoire : oui

Type

Spécifie le type d'erreur.

- `ALREADY_EXISTS`: se produit lors d'une étape de copie, si l'option de remplacement n'est pas sélectionnée et qu'un fichier portant le même nom existe déjà dans l'emplacement cible.
- `BAD_REQUEST`: une mauvaise demande générale : par exemple, une étape qui tente de baliser un EFS fichier renvoie `BAD_REQUEST`, car seuls les fichiers S3 peuvent être balisés.
- `CUSTOM_STEP_FAILED`: se produit lorsque l'étape personnalisée fournit un rappel indiquant un échec.
- `INTERNAL_SERVER_ERROR`: une erreur fourre-tout qui peut survenir pour diverses raisons.
- `NOT_FOUND`: se produit lorsqu'une entité demandée, par exemple un fichier source pour une étape de copie, n'existe pas.
- `PERMISSION_DENIED`: se produit si votre politique ne contient pas les autorisations appropriées pour effectuer une ou plusieurs étapes du flux de travail.
- `TIMEOUT`: se produit lorsque le délai d'exécution est expiré.

Note

Vous pouvez définir une étape personnalisée, comprise entre 1 seconde et 1 800 secondes (30 minutes). `TimeoutSeconds`

- `THROTTLED`: se produit si vous dépassez le nouveau taux de recharge d'exécution d'un flux de travail par seconde.

Type : String

Valeurs valides : PERMISSION_DENIED | CUSTOM_STEP_FAILED | THROTTLED
| ALREADY_EXISTS | NOT_FOUND | BAD_REQUEST | TIMEOUT |
INTERNAL_SERVER_ERROR

Obligatoire : oui

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ExecutionResults

Spécifie les étapes du flux de travail, ainsi que les étapes à exécuter en cas d'erreur lors de l'exécution du flux de travail.

Table des matières

OnExceptionSteps

Spécifie les étapes (actions) à suivre en cas d'erreur lors de l'exécution du flux de travail.

Type : tableau d'objets [ExecutionStepResult](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

Steps

Spécifie les détails des étapes qui se trouvent dans le flux de travail spécifié.

Type : tableau d'objets [ExecutionStepResult](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 50 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ExecutionStepResult

Spécifie les détails suivants pour l'étape : erreur (le cas échéant), sorties (le cas échéant) et type d'étape.

Table des matières

Error

Spécifie les détails d'une erreur, si elle s'est produite lors de l'exécution de l'étape de flux de travail spécifiée.

Type : objet [ExecutionError](#)

Obligatoire : non

Outputs

Les valeurs de la paire clé/valeur appliquées sous forme de balise au fichier. Applicable uniquement si le type d'étape est TAG.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 65536

Obligatoire : non

StepType

L'un des types d'étapes disponibles.

- **COPY** : copier le fichier à un autre emplacement.
- **CUSTOM**- Effectuez une étape personnalisée avec une AWS Lambda fonction cible.
- **DECRYPT** : déchiffrer un fichier chiffré avant d'être chargé.
- **DELETE** : supprimer le fichier.
- **TAG** : ajouter une balise au fichier.

Type : String

Valeurs valides : COPY | CUSTOM | TAG | DELETE | DECRYPT

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

FileLocation

Spécifie l'Amazon S3 ou les détails EFS du fichier à utiliser dans l'étape.

Table des matières

EfsFileLocation

Spécifie l'EFSidentifiant Amazon et le chemin du fichier utilisé.

Type : objet [EfsFileLocation](#)

Obligatoire : non

S3FileLocation

Spécifie les détails S3 du fichier utilisé, tels que le bucketETag, etc.

Type : objet [S3FileLocation](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

HomeDirectoryMapEntry

Représente un objet qui contient des entrées et des cibles pour HomeDirectoryMappings.

Voici un exemple de Target paire Entry et pourchroot.

```
[ { "Entry": "/", "Target": "/bucket_name/home/mydirectory" } ]
```

Table des matières

Entry

Représente une entrée pour HomeDirectoryMappings.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : /. *

Obligatoire : oui

Target

Représente la cible de carte utilisée dans un élément HomeDirectoryMapEntry.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : /. *

Obligatoire : oui

Type

Spécifie le type de mappage. Définissez le type sur FILE si vous souhaitez que le mappage pointe vers un fichier ou DIRECTORY que le répertoire pointe vers un répertoire.

Note

Par défaut, les mappages du répertoire de base ont un Type de DIRECTORY lorsque vous créez un serveur Transfer Family. Vous devez définir explicitement sur Type FILE si vous souhaitez qu'un mappage ait une cible de fichier.

Type : String

Valeurs valides : FILE | DIRECTORY

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

IdentityProviderDetails

Renvoie les informations relatives au type d'authentification utilisateur utilisé pour les utilisateurs d'un serveur compatible avec le protocole de transfert de fichiers. Un serveur ne peut avoir qu'une seule méthode d'authentification.

Table des matières

DirectoryId

Identifiant de l' AWS Directory Service annuaire que vous souhaitez utiliser comme fournisseur d'identité.

Type : String

Contraintes de longueur : longueur fixe de 12.

Modèle : d-[0-9a-f]{10}

Obligatoire : non

Function

La ARN fonction Lambda à utiliser pour le fournisseur d'identité.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 170.

Modèle : arn:[a-z-]+:lambda:.*

Obligatoire : non

InvocationRole

Ce paramètre n'est applicable que si vous IdentityProviderType l'êtesAPI_GATEWAY. Le paramètre fournit le type de InvocationRole utilisé pour authentifier le compte d'utilisateur.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : arn:.*role/\S+

Obligatoire : non

SftpAuthenticationMethods

Pour les serveurs SFTP compatibles, et pour les fournisseurs d'identité personnalisés uniquement, vous pouvez spécifier si vous souhaitez vous authentifier à l'aide d'un mot de passe, d'une paire de SSH clés ou des deux.

- **PASSWORD**- les utilisateurs doivent fournir leur mot de passe pour se connecter.
- **PUBLIC_KEY**- les utilisateurs doivent fournir leur clé privée pour se connecter.
- **PUBLIC_KEY_OR_PASSWORD**- les utilisateurs peuvent s'authentifier à l'aide de leur mot de passe ou de leur clé. C'est la valeur par défaut.
- **PUBLIC_KEY_AND_PASSWORD**- les utilisateurs doivent fournir à la fois leur clé privée et leur mot de passe pour se connecter. Le serveur vérifie d'abord la clé, puis si la clé est valide, le système demande un mot de passe. Si la clé privée fournie ne correspond pas à la clé publique stockée, l'authentification échoue.

Type : String

Valeurs valides : **PASSWORD** | **PUBLIC_KEY** | **PUBLIC_KEY_OR_PASSWORD** | **PUBLIC_KEY_AND_PASSWORD**

Obligatoire : non

Url

Fournit l'emplacement du point de terminaison de service utilisé pour authentifier les utilisateurs.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 255.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)

- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

InputFileLocation

Spécifie l'emplacement du fichier en cours de traitement.

Table des matières

EfsFileLocation

Spécifie les détails du fichier Amazon Elastic File System (AmazonEFS) en cours de déchiffrement.

Type : objet [EfsFileLocation](#)

Obligatoire : non

S3FileLocation

Spécifie les détails du fichier Amazon S3 qui est copié ou déchiffré.

Type : objet [S3InputFileLocation](#)

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedAccess

Répertorie les propriétés d'un ou de plusieurs accès associés spécifiés.

Table des matières

ExternalId

Identifiant unique requis pour identifier des groupes spécifiques au sein de votre annuaire.

Les utilisateurs du groupe que vous associez ont accès à vos EFS ressources Amazon S3 ou Amazon via les protocoles activés à l'aide de AWS Transfer Family. Si vous connaissez le nom du groupe, vous pouvez afficher les SID valeurs en exécutant la commande suivante sous Windows PowerShell.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties  
* | Select SamAccountName, ObjectSid
```

Dans cette commande, remplacez YourGroupName par le nom de votre groupe Active Directory.

L'expression régulière utilisée pour valider ce paramètre est une chaîne de caractères composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez également inclure des traits de soulignement ou l'un des caractères suivants : =, . @ : /-

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : S-1-[\d-]+

Obligatoire : non

HomeDirectory

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de HomeDirectory est /bucket_name/home/mydirectory.

Note

Le paramètre HomeDirectory est uniquement utilisé si HomeDirectoryType est défini sur la valeur PATH.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : (| / . *)

Obligatoire : non

HomeDirectoryType

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez sur `PATH`, l'utilisateur verra le bucket Amazon S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez sur `LOGICAL`, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

Note

Dans `HomeDirectoryType` l'affirmative `LOGICAL`, vous devez fournir des mappages à l'aide du `HomeDirectoryMappings` paramètre. Si, en revanche, `HomeDirectoryType` c'est le cas `PATH`, vous fournissez un chemin absolu à l'aide du `HomeDirectory` paramètre. Vous ne pouvez pas avoir les deux `HomeDirectory` et `HomeDirectoryMappings` dans votre modèle.

Type : String

Valeurs valides : `PATH` | `LOGICAL`

Obligatoire : non

Role

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedAgreement

Décrit les propriétés d'un accord.

Table des matières

AgreementId

Identifiant unique pour l'accord. Cet identifiant est renvoyé lorsque vous créez un accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : a - ([0-9a-f]{17})

Obligatoire : non

Arn

Le nom de la ressource Amazon (ARN) de l'accord spécifié.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : arn:\S+

Obligatoire : non

Description

Description actuelle de l'accord. Vous pouvez le modifier en appelant l'UpdateAgreementopération et en fournissant une nouvelle description.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : [\p{Graph}] +

Obligatoire : non

LocalProfileId

Identifiant unique pour le profil AS2 local.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : non

PartnerProfileId

Identifiant unique pour le profil du partenaire.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : p-([0-9a-f]{17})

Obligatoire : non

ServerId

L'identifiant unique de l'accord.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : non

Status

L'accord peut être l'un ACTIVE ou l'autre INACTIVE.

Type : String

Valeurs valides : ACTIVE | INACTIVE

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedCertificate

Décrit les propriétés d'un certificat.

Table des matières

ActiveDate

Une date facultative qui indique à quel moment le certificat devient actif.

Type : Timestamp

Obligatoire : non

Arn

Le nom de ressource Amazon (ARN) du certificat spécifié.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : non

CertificateId

Un tableau d'identifiants pour les certificats importés. Vous utilisez cet identifiant pour travailler avec des profils et des profils de partenaires.

Type : String

Contraintes de longueur : longueur fixe de 22.

Modèle : `cert-([0-9a-f]{17})`

Obligatoire : non

Description

Le nom ou la brève description utilisés pour identifier le certificat.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 200.

Modèle : $[\backslash p\{Graph\}]^+$

Obligatoire : non

InactiveDate

Une date facultative qui indique à quel moment le certificat devient inactif.

Type : Timestamp

Obligatoire : non

Status

Le certificat peut être soit ACTIVE, PENDING_ROTATION, ou INACTIVE. PENDING_ROTATION signifie que ce certificat remplacera le certificat actuel à son expiration.

Type : String

Valeurs valides : ACTIVE | PENDING_ROTATION | INACTIVE

Obligatoire : non

Type

Type du certificat. Si une clé privée a été spécifiée pour le certificat, son type est CERTIFICATE_WITH_PRIVATE_KEY. S'il n'y a pas de clé privée, le type est CERTIFICATE.

Type : String

Valeurs valides : CERTIFICATE | CERTIFICATE_WITH_PRIVATE_KEY

Obligatoire : non

Usage

Spécifie si ce certificat est utilisé pour la signature ou le chiffrement.

Type : String

Valeurs valides : SIGNING | ENCRYPTION

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedConnector

Renvoie les détails du connecteur spécifié.

Table des matières

Arn

Le nom de ressource Amazon (ARN) du connecteur spécifié.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : non

ConnectorId

Identifiant unique du connecteur.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `c-([0-9a-f]{17})`

Obligatoire : non

Url

Celui URL du partenaire AS2 ou du SFTP point final.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 255.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedExecution

Renvoie les propriétés de l'exécution spécifiée.

Table des matières

ExecutionId

Identifiant unique pour l'exécution d'un flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 36.

Modèle : `[0-9a-fA-F]{8}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{4}\-[0-9a-fA-F]{12}`

Obligatoire : non

InitialFileLocation

Structure qui décrit l'Amazon S3 ou l'emplacement EFS du fichier. Il s'agit de l'emplacement du fichier lorsque l'exécution commence : si le fichier est copié, il s'agit de l'emplacement du fichier initial (et non de destination).

Type : objet [FileLocation](#)

Obligatoire : non

ServiceMetadata

Objet conteneur pour les détails de session associés à un flux de travail.

Type : objet [ServiceMetadata](#)

Obligatoire : non

Status

Le statut est celui de l'exécution. Peut être en cours, terminé, une exception peut être détectée ou être en cours de traitement.

Type : String

Valeurs valides : IN_PROGRESS | COMPLETED | EXCEPTION | HANDLING_EXCEPTION

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedHostKey

Renvoie les propriétés de la clé d'hôte spécifiée.

Table des matières

Arn

Nom de ressource Amazon unique (ARN) de la clé d'hôte.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

DateImported

Date à laquelle la clé d'hôte a été ajoutée au serveur.

Type : Timestamp

Obligatoire : non

Description

Description actuelle de la clé d'hôte. Vous pouvez le modifier en appelant l'UpdateHostKeyopération et en fournissant une nouvelle description.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 200.

Modèle : `[\p{Print}]*`

Obligatoire : non

Fingerprint

L'empreinte de clé publique, qui est une courte séquence d'octets utilisée pour identifier la clé publique la plus longue.

Type : chaîne

Obligatoire : non

HostKeyId

Identifiant unique pour la clé d'hôte.

Type : String

Contraintes de longueur : longueur fixe de 25.

Modèle : `hostkey-[0-9a-f]{17}`

Obligatoire : non

Type

Algorithme de chiffrement utilisé pour la clé d'hôte. Le Type paramètre est spécifié à l'aide de l'une des valeurs suivantes :

- `ssh-rsa`
- `ssh-ed25519`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ListedProfile

Renvoie les propriétés du profil qui a été spécifié.

Table des matières

Arn

Le nom de ressource Amazon (ARN) du profil spécifié.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : non

As2Id

As2IdIl s'agit du AS2-name, tel que défini dans le [RFC4130](#). Pour les transferts entrants, il s'agit de l'AS2-Fromen-tête des AS2 messages envoyés par le partenaire. Pour les connecteurs sortants, il s'agit de l'AS2-Toen-tête des AS2 messages envoyés au partenaire à l'aide de l'StartFileTransferAPIopération. Cet identifiant ne peut pas inclure d'espaces.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : `[\p{Print}\s]*`

Obligatoire : non

ProfileId

Identifiant unique pour le profil local ou le AS2 profil du partenaire.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `p-([0-9a-f]{17})`

Obligatoire : non

ProfileType

Indique s'il faut répertorier uniquement les profils de type LOCAL ou uniquement les profils de type PARTNER. Si elle n'est pas fournie dans la demande, la commande répertorie tous les types de profils.

Type : String

Valeurs valides : LOCAL | PARTNER

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedServer

Renvoie les propriétés d'un serveur compatible avec le protocole de transfert de fichiers spécifié.

Table des matières

Arn

Spécifie le nom unique de la ressource Amazon (ARN) pour un serveur à répertorier.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

Domain

Spécifie le domaine du système de stockage utilisé pour les transferts de fichiers.

Type : String

Valeurs valides : `S3` | `EFS`

Obligatoire : non

EndpointType

Spécifie le type de VPC point de terminaison auquel votre serveur est connecté. Si votre serveur est connecté à un VPC point de terminaison, il n'est pas accessible via l'Internet public.

Type : String

Valeurs valides : `PUBLIC` | `VPC` | `VPC_ENDPOINT`

Obligatoire : non

IdentityProviderType

Le mode d'authentification pour un serveur. La valeur par défaut est `SERVICE_MANAGED`, ce qui vous permet de stocker et d'accéder aux informations d'identification des utilisateurs au sein du AWS Transfer Family service.

`AWS_DIRECTORY_SERVICE` À utiliser pour fournir un accès aux groupes Active Directory AWS Directory Service for Microsoft Active Directory ou à Microsoft Active Directory dans votre environnement local ou à l' AWS aide d'AD Connector. Cette option exige également que vous indiquiez un ID de répertoire en utilisant le paramètre `IdentityProviderDetails`.

Utilisez la valeur `API_GATEWAY` à intégrer au fournisseur d'identité de votre choix. Le `API_GATEWAY` paramètre vous oblige à fournir un point de terminaison Amazon API Gateway URL à appeler pour l'authentification à l'aide du `IdentityProviderDetails` paramètre.

Utilisez la `AWS_LAMBDA` valeur pour utiliser directement une AWS Lambda fonction comme fournisseur d'identité. Si vous choisissez cette valeur, vous devez spécifier la ARN fonction Lambda dans le `Function` paramètre du type de `IdentityProviderDetails` données.

Type : String

Valeurs valides : `SERVICE_MANAGED` | `API_GATEWAY` | `AWS_DIRECTORY_SERVICE` | `AWS_LAMBDA`

Obligatoire : non

LoggingRole

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un serveur d'activer la CloudWatch journalisation Amazon pour Amazon S3 ou AmazonEFS events. Lorsque cette option est configurée, vous pouvez consulter l'activité des utilisateurs dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

ServerId

Spécifie l'identifiant unique attribué par le système aux serveurs répertoriés.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s-([0-9a-f]{17})

Obligatoire : non

State

État du serveur décrit. La valeur de ONLINE indique que le serveur peut accepter des tâches et transférer des fichiers. StateLa valeur de OFFLINE signifie que le serveur ne peut pas effectuer d'opérations de transfert de fichiers.

Les états de STARTING et STOPPING indiquent que le serveur est dans un état intermédiaire, qu'il n'est pas totalement en mesure de répondre ou qu'il n'est pas complètement hors ligne. Les valeurs de START_FAILED ou STOP_FAILED peuvent indiquer une condition d'erreur.

Type : String

Valeurs valides : OFFLINE | ONLINE | STARTING | STOPPING | START_FAILED | STOP_FAILED

Obligatoire : non

UserCount

Spécifie le nombre d'utilisateurs affectés à un serveur que vous avez spécifié avec leServerId.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedUser

Renvoie les propriétés de l'utilisateur que vous spécifiez.

Table des matières

Arn

Fournit le nom unique de la ressource Amazon (ARN) pour l'utilisateur sur lequel vous souhaitez en savoir plus.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : oui

HomeDirectory

La destination d'un répertoire (dossier) pour un utilisateur lorsqu'il se connecte au serveur à l'aide de son client.

Un exemple de HomeDirectory est `/bucket_name/home/mydirectory`.

Note

Le paramètre HomeDirectory est uniquement utilisé si HomeDirectoryType est défini sur la valeur PATH.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `(|/.*)`

Obligatoire : non

HomeDirectoryType

Le type de répertoire (dossier) de destination du répertoire de base de vos utilisateurs lorsqu'ils se connectent au serveur. Si vous le définissez sur PATH, l'utilisateur verra le bucket Amazon

S3 absolu ou le EFS chemin Amazon tel quel dans ses clients de protocole de transfert de fichiers. Si vous le définissez sur LOGICAL, vous devez fournir des mappages indiquant comment vous souhaitez rendre les EFS chemins Amazon S3 ou Amazon visibles pour vos utilisateurs.

HomeDirectoryMappings

 Note

Dans HomeDirectoryType l'affirmative LOGICAL, vous devez fournir des mappages à l'aide du HomeDirectoryMappings paramètre. Si, en revanche, HomeDirectoryType c'est le cas PATH, vous fournissez un chemin absolu à l'aide du HomeDirectory paramètre. Vous ne pouvez pas avoir les deux HomeDirectory et HomeDirectoryMappings dans votre modèle.

Type : String

Valeurs valides : PATH | LOGICAL

Obligatoire : non

Role

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de EFS fichiers Amazon. Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis votre compartiment Amazon S3 ou votre système de EFS fichiers Amazon. Le IAM rôle doit également contenir une relation de confiance qui permet au serveur d'accéder à vos ressources lorsqu'il répond aux demandes de transfert de vos utilisateurs.

 Note

IAM Rôle qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 pour les serveurs dotés Domain=S3 de ou à votre système de EFS fichiers pour les serveurs dotés de Domain=EFS.

Les politiques associées à ce rôle déterminent le niveau d'accès que vous souhaitez fournir à vos utilisateurs lors du transfert de fichiers vers et depuis vos compartiments ou systèmes de EFS fichiers S3.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

SshPublicKeyCount

Spécifie le nombre de clés SSH publiques stockées pour l'utilisateur que vous avez spécifié.

Type : entier

Obligatoire : non

UserName

Spécifie le nom de l'utilisateur qui ARN a été spécifié. Les noms d'utilisateur sont utilisés à des fins d'authentification.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : `[\w][\w@.-]{2,99}`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ListedWorkflow

Contient l'identifiant, la description textuelle et le nom de ressource Amazon (ARN) du flux de travail.

Table des matières

Arn

Spécifie le nom unique de la ressource Amazon (ARN) pour le flux de travail.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 1600.

Modèle : `arn:\S+`

Obligatoire : non

Description

Spécifie la description textuelle pour le flux de travail.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `[\w- ]*`

Obligatoire : non

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `w-([a-z0-9]{17})`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

LoggingConfiguration

Comprend le rôle de journalisation et le nom du groupe de journaux.

Table des matières

LoggingRole

Le nom de ressource Amazon (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à un serveur d'activer la CloudWatch journalisation Amazon pour Amazon S3 ou AmazonEFS events. Lorsque cette option est configurée, vous pouvez consulter l'activité des utilisateurs dans vos CloudWatch journaux.

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : non

LogGroupName

Nom du groupe de CloudWatch journalisation du AWS Transfer Family serveur auquel appartient ce flux de travail.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 512.

Modèle : `[\.\-_\#A-Za-z0-9]*`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)

- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

PosixProfile

L'POSIX identité complète, y compris l'ID utilisateur (Uid), l'ID de groupe (Gid) et tout groupe secondaire IDs (SecondaryGids), qui contrôle l'accès de vos utilisateurs à vos systèmes de EFS fichiers Amazon. Les POSIX autorisations définies sur les fichiers et les répertoires de votre système de fichiers déterminent le niveau d'accès dont bénéficient vos utilisateurs lors du transfert de fichiers vers et depuis vos systèmes de EFS fichiers Amazon.

Table des matières

Gid

L'ID de POSIX groupe utilisé pour toutes les EFS opérations de cet utilisateur.

Type : long

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : oui

Uid

L'ID POSIX utilisateur utilisé pour toutes les EFS opérations de cet utilisateur.

Type : long

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : oui

SecondaryGids

Le POSIX groupe secondaire IDs utilisé pour toutes les EFS opérations de cet utilisateur.

Type : Tableau de longueurs

Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 16 éléments.

Plage valide : Valeur minimum de 0. Valeur maximale de 4294967295.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

ProtocolDetails

Les paramètres du protocole qui sont configurés pour votre serveur.

Table des matières

As2Transports

Indique le mode de transport des AS2 messages. Actuellement, seul HTTP est pris en charge.

Type : tableau de chaînes

Membres du tableau : nombre fixe de 1 élément.

Valeurs valides : HTTP

Obligatoire : non

PassiveIp

Indique le mode passif, pour FTP et les FTPS protocoles. Entrez une IPv4 adresse unique, telle que l'adresse IP publique d'un pare-feu, d'un routeur ou d'un équilibreur de charge. Par exemple :

```
aws transfer update-server --protocol-details PassiveIp=0.0.0.0
```

Remplacez 0.0.0.0 dans l'exemple ci-dessus par l'adresse IP réelle que vous souhaitez utiliser.

Note

Si vous modifiez la valeur PassiveIp, vous devez arrêter, puis redémarrer votre serveur Transfer Family pour que la modification prenne effet. Pour plus de détails sur l'utilisation du mode passif (PASV) dans un NAT environnement, voir [Configuration de votre FTPS serveur derrière un pare-feu ou NAT avec AWS Transfer Family](#).

Valeurs spéciales

AUTO et 0.0.0.0 sont des valeurs spéciales pour le paramètre PassiveIp. La valeur PassiveIp=AUTO est attribuée par défaut aux serveurs de FTPS type FTP et de type. Dans ce cas, le serveur répond automatiquement avec l'un des points de terminaison IPs contenus dans la PASV réponse. PassiveIp=0.0.0.0 a une application plus unique pour son utilisation. Par exemple, si vous disposez d'un environnement High Availability (HA) Network Load Balancer (NLB) dans lequel vous disposez de 3 sous-réseaux, vous ne pouvez spécifier qu'une seule

adresse IP à l'aide du paramètre. `PassiveIp` Cela réduit l'efficacité de la haute disponibilité. Dans ce cas, il est possible de spécifier `PassiveIp=0.0.0.0`. Cela indique au client d'utiliser la même adresse IP que la connexion de contrôle et de tout utiliser AZs pour ses connexions. Notez toutefois que tous les FTP clients ne soutiennent pas la `PassiveIp=0.0.0.0` réponse. FileZilla et SCP Win le soutient. Si vous utilisez d'autres clients, vérifiez si votre client prend en charge réponse `PassiveIp=0.0.0.0`.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 15.

Obligatoire : non

SetStatOption

Utilisez l'`SetStatOption` pour ignorer l'erreur qui est générée lorsque le client essaye d'utiliser SETSTAT sur un fichier que vous chargez dans un compartiment S3.

Certains clients de transfert de fichiers peuvent tenter de modifier les attributs des fichiers distants, notamment l'horodatage et les autorisations, à l'aide de commandes, par exemple SETSTAT lors du téléchargement du SFTP fichier. Cependant, ces commandes ne sont pas compatibles avec les systèmes de stockage d'objets, tels qu'Amazon S3. En raison de cette incompatibilité, les chargements de fichiers à partir de ces clients peuvent entraîner des erreurs, même si le fichier est correctement chargé.

Définissez la valeur sur `ENABLE_NO_OP` pour que le serveur Transfer Family ignore la SETSTAT commande et télécharge les fichiers sans avoir à apporter de modifications à votre SFTP client. Bien que le `SetStatOption` `ENABLE_NO_OP` paramètre ignore l'erreur, il génère une entrée de journal dans Amazon CloudWatch Logs, afin que vous puissiez déterminer à quel moment le client passe un SETSTAT appel.

Note

Si vous souhaitez conserver l'horodatage d'origine de votre fichier et modifier d'autres attributs de fichier à l'aide de celui-ci SETSTAT, vous pouvez utiliser Amazon EFS comme système de stockage principal avec Transfer Family.

Type : String

Valeurs valides : DEFAULT | ENABLE_NO_OP

Obligatoire : non

TlsSessionResumptionMode

Propriété utilisée avec les serveurs Transfer Family qui utilisent le FTPS protocole. TLSLa reprise de session fournit un mécanisme permettant de reprendre ou de partager une clé secrète négociée entre le contrôle et la connexion de données pour une FTPS session.

TlsSessionResumptionModedétermine si le serveur reprend les sessions récemment négociées par le biais d'un identifiant de session unique. Cette propriété est disponible lors des appels `CreateServer` et `UpdateServer`. Si une valeur `TlsSessionResumptionMode` n'est pas spécifiée pendant `CreateServer`, elle est définie sur `ENFORCED` par défaut.

- **DISABLED**: le serveur ne traite pas les demandes des clients de reprise de TLS session et crée une nouvelle TLS session pour chaque demande.
- **ENABLED**: le serveur traite et accepte les clients qui reprennent TLS leur session. Le serveur ne rejette pas les connexions de données client qui n'effectuent pas le traitement du client de reprise de TLS session.
- **ENFORCED**: le serveur traite et accepte les clients qui reprennent TLS leur session. Le serveur rejette les connexions de données client qui n'effectuent pas le traitement du client de reprise de TLS session. Avant de définir la valeur sur `ENFORCED`, testez vos clients.

Note

Tous les FTPS clients ne reprennent pas leur TLS session. Ainsi, si vous choisissez d'imposer la reprise de TLS session, vous empêchez toute connexion provenant de FTPS clients qui n'effectuent pas la négociation du protocole. Pour déterminer si vous pouvez utiliser ou non la valeur `ENFORCED`, vous devez tester vos clients.

Type : String

Valeurs valides : `DISABLED` | `ENABLED` | `ENFORCED`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

S3FileLocation

Spécifie les détails de l'emplacement du fichier utilisé dans le flux de travail. Applicable uniquement si vous utilisez le stockage S3.

Table des matières

Bucket

Spécifie le compartiment S3 qui contient le fichier utilisé.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 63.

Modèle : `[a-z0-9][\.\-a-z0-9]{1,61}[a-z0-9]`

Obligatoire : non

Etag

La balise d'entité est un hachage de l'objet. Le ETag reflète uniquement les modifications apportées au contenu d'un objet, et non à ses métadonnées.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 65536.

Modèle : `.+`

Obligatoire : non

Key

Le nom attribué au fichier lors de sa création dans Amazon S3. Vous utilisez la clé de l'objet pour récupérer l'objet.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `[\P{M}\p{M}]*`

Obligatoire : non

VersionId

Spécifie la version du fichier.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 1024.

Modèle : .+

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

S3InputFileLocation

Spécifie l'emplacement du fichier Amazon S3 saisi par le client. S'il est utilisé à l'intérieur `copyStepDetails.DestinationFileLocation`, il doit être la destination de copie S3.

Vous devez fournir le seau et la clé. La clé peut représenter un chemin ou un fichier. Cela dépend du fait que vous terminiez ou non la valeur clé par la barre oblique (/). Si le dernier caractère est «/», votre fichier est copié dans le dossier et son nom ne change pas. Si, au contraire, le dernier caractère est alphanumérique, le fichier téléchargé est renommé avec la valeur du chemin. Dans ce cas, si un fichier portant ce nom existe déjà, il est remplacé.

Par exemple, si votre chemin est `shared-files/bob/`, les fichiers que vous avez téléchargés sont copiés dans `shared-files/bob/` le dossier. Si votre chemin est le cas `shared-files/today`, chaque fichier téléchargé est copié `shared-files` dans le dossier et nommé `today` : chaque téléchargement remplace la version précédente du fichier `bob`.

Table des matières

Bucket

Spécifie le compartiment S3 pour le fichier d'entrée du client.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 63.

Modèle : `[a-z0-9][\.-a-z0-9]{1,61}[a-z0-9]`

Obligatoire : non

Key

Le nom attribué au fichier lors de sa création dans Amazon S3. Vous utilisez la clé de l'objet pour récupérer l'objet.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `[\P{M}\p{M}]*`

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

S3StorageOptions

Les options de stockage Amazon S3 configurées pour votre serveur.

Table des matières

DirectoryListingOptimization

Spécifie si les performances de vos annuaires Amazon S3 sont optimisées ou non. Par défaut, l'option est désactivée.

Par défaut, les mappages du répertoire de base ont la valeur TYPE de DIRECTORY. Si vous activez cette option, vous devrez alors définir explicitement le HomeDirectoryMapEntry Type à FILE si vous souhaitez qu'un mappage ait une cible de fichier.

Type : String

Valeurs valides : ENABLED | DISABLED

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

S3Tag

Spécifie la paire clé-valeur attribuée à un fichier lors de l'exécution d'une étape de balisage.

Table des matières

Key

Le nom attribué à la balise que vous créez.

Type : String

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : ([\p{L}\p{Z}\p{N}_.: /+=\ -@] *)

Obligatoire : oui

Value

La valeur correspondant à la clé.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : ([\p{L}\p{Z}\p{N}_.: /+=\ -@] *)

Obligatoire : oui

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

ServiceMetadata

Objet conteneur pour les détails de session associés à un flux de travail.

Table des matières

UserDetails

L'ID du serveur (ServerId), l'ID de session (SessionId) et l'utilisateur (UserName) constituent le UserDetails.

Type : objet [UserDetails](#)

Obligatoire : oui

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

SftpConnectorConfig

Contient les détails d'un objet SFTP connecteur. L'objet connecteur est utilisé pour transférer des fichiers depuis et vers le SFTP serveur d'un partenaire.

Note

Comme le type de `SftpConnectorConfig` données est utilisé à la fois pour créer et mettre à jour des SFTP connecteurs, `TrustedHostKeys` ses paramètres `UserSecretId` sont marqués comme non obligatoires. Cela est un peu trompeur, car ils ne sont pas obligatoires lorsque vous mettez à jour un SFTP connecteur existant, mais le sont lorsque vous créez un nouveau SFTP connecteur.

Table des matières

TrustedHostKeys

Partie publique de la ou des clés d'hôte utilisées pour identifier le serveur externe auquel vous vous connectez. Vous pouvez utiliser la `ssh-keyscan` commande sur le SFTP serveur pour récupérer la clé nécessaire.

Les trois éléments de format de clé SSH publique standard sont `<key type><body base64>`, et un facultatif `<comment>`, avec des espaces entre chaque élément. Spécifiez uniquement le `<key type>` et `<body base64>` : ne saisissez pas la `<comment>` partie de la clé.

Pour la clé d'hôte fiable, AWS Transfer Family accepte RSA et ECDSA clés.

- Pour RSA les clés, la `<key type>` chaîne est `ssh-rsa`.
- Pour ECDSA les clés, la `<key type>` chaîne est soit `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, soit `ecdsa-sha2-nistp521`, selon la taille de la clé que vous avez générée.

Exécutez cette commande pour récupérer la clé d'hôte SFTP du serveur, où se trouve le nom de votre SFTP serveur `ftp.host.com`.

```
ssh-keyscan ftp.host.com
```

Cela imprime la clé de l'hôte public sur la sortie standard.

```
ftp.host.com ssh-rsa AAAAB3Nza...<long-string-for-public-key>
```

Copiez et collez cette chaîne dans le `TrustedHostKeys` champ de la `create-connector` commande ou dans le champ `Trusted host keys` de la console.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048.

Obligatoire : non

UserSecretId

Identifiant du secret (dans AWS Secrets Manager) qui contient la clé privée, le mot de passe ou les deux de l'SFTPutilisateur. L'identifiant doit être le Amazon Resource Name (ARN) du secret.

Type : String

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

SshPublicKey

Fournit des informations sur la clé publique Secure Shell (SSH) associée à un utilisateur Transfer Family pour le serveur compatible avec le protocole de transfert de fichiers spécifique (tel qu'identifié par). `ServerId` Les informations retournées incluent la date à laquelle la clé a été importée, le contenu de la clé publique et l'ID de la clé publique. Un utilisateur peut stocker plusieurs clés SSH publiques associées à son nom d'utilisateur sur un serveur spécifique.

Table des matières

`DateImported`

Spécifie la date à laquelle la clé publique a été ajoutée à l'utilisateur Transfer Family.

Type : Timestamp

Obligatoire : oui

`SshPublicKeyBody`

Spécifie le contenu de la clé SSH publique tel que spécifié par `lePublicKeyId`.

AWS Transfer Family accepte RSAECDSA, et ED25519 clés.

Type : String

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Obligatoire : oui

`SshPublicKeyId`

Spécifie que le `SshPublicKeyId` paramètre contient l'identifiant de la clé publique.

Type : String

Contraintes de longueur : longueur fixe de 21.

Modèle : `key-[0-9a-f]{17}`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

Tag

Créez une paire clé-valeur pour une ressource spécifique. Les balises sont des métadonnées que vous pouvez utiliser pour rechercher et regrouper une ressource à différentes fins. Vous pouvez appliquer des balises aux serveurs, aux utilisateurs et aux rôles. Une clé de balise peut prendre plusieurs valeurs. Par exemple, pour regrouper des serveurs à des fins de comptabilité, vous pouvez créer une balise appelée Group et attribuer les valeurs Research et Accounting à ce groupe.

Table des matières

Key

Le nom attribué à la balise que vous créez.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 128.

Obligatoire : oui

Value

Contient une ou plusieurs valeurs que vous avez attribuées au nom de clé que vous créez.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximale de 256.

Obligatoire : oui

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)
- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

TagStepDetails

Chaque type d'étape possède sa propre `StepDetails` structure.

Les paires clé/valeur utilisées pour baliser un fichier lors de l'exécution d'une étape du flux de travail.

Table des matières

Name

Le nom de l'étape, utilisé comme identifiant.

Type : String

Contraintes de longueur : longueur minimum de 0. Longueur maximale de 30.

Modèle : `[\w-]*`

Obligatoire : non

SourceFileLocation

Spécifie le fichier à utiliser comme entrée pour l'étape du flux de travail : soit le résultat de l'étape précédente, soit le fichier initialement chargé pour le flux de travail.

- Pour utiliser le fichier précédent comme entrée, entrez `${previous.file}`. Dans ce cas, cette étape du flux de travail utilise le fichier de sortie de l'étape précédente du flux de travail comme entrée. C'est la valeur par défaut.
- Pour utiliser l'emplacement du fichier initialement chargé comme entrée pour cette étape, entrez `${original.file}`.

Type : String

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `\$\{(\w+.\w+)\}`

Obligatoire : non

Tags

Tableau contenant de 1 à 10 paires clé/valeur.

Type : tableau d'objets [S3Tag](#)

Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 10 éléments.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

UserDetails

Spécifie le nom d'utilisateur, l'ID du serveur et l'ID de session d'un flux de travail.

Table des matières

ServerId

Identifiant unique attribué par le système pour une instance de serveur de transfert.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : s - ([0-9a-f]{17})

Obligatoire : oui

UserName

Chaîne unique qui identifie un utilisateur de Transfer Family associé à un serveur.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximum de 100.

Modèle : [\w][\w@.-]{2,99}

Obligatoire : oui

SessionId

Identifiant unique attribué par le système pour une session correspondant au flux de travail.

Type : String

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 32.

Modèle : [\w-]*

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

WorkflowDetail

Spécifie l'ID du flux de travail à attribuer et le rôle d'exécution utilisé pour exécuter le flux de travail.

En plus d'un flux de travail à exécuter lorsqu'un fichier est complètement chargé, `WorkflowDetails` peut également contenir un ID de flux de travail (et un rôle d'exécution) pour un flux de travail à exécuter lors d'un chargement partiel. Un téléchargement partiel se produit lorsque la session du serveur se déconnecte alors que le fichier est toujours en cours de téléchargement.

Table des matières

ExecutionRole

Inclut les autorisations nécessaires pour les opérations S3 et Lambda que Transfer peut assumer, afin que toutes les étapes du flux de travail puissent fonctionner sur les ressources requises EFS

Type : String

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `arn:.*role/\S+`

Obligatoire : oui

WorkflowId

Un identifiant unique pour le flux de travail.

Type : String

Contraintes de longueur : longueur fixe de 19.

Modèle : `w-([a-z0-9]{17})`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

WorkflowDetails

Conteneur pour le type de données `WorkflowDetail`. Il est utilisé par les actions qui déclenchent le début de l'exécution d'un flux de travail.

Table des matières

OnPartialUpload

Déclencheur qui démarre un flux de travail si un fichier n'est que partiellement chargé. Vous pouvez associer un flux de travail à un serveur qui s'exécute en cas de téléchargement partiel.

Un téléchargement partiel se produit si un fichier est ouvert lorsque la session se déconnecte.

Type : tableau d'objets [WorkflowDetail](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

OnUpload

Un déclencheur qui démarre un flux de travail : le flux de travail commence à s'exécuter après le chargement d'un fichier.

Pour supprimer un flux de travail associé d'un serveur, vous pouvez fournir un objet `OnUpload` vide, comme dans l'exemple suivant.

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-  
details '{"OnUpload":[]}'
```

Type : tableau d'objets [WorkflowDetail](#)

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 1 élément.

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDKpour C++](#)
- [AWS SDKpour Go](#)
- [AWS SDKpour Java V2](#)
- [AWS SDKpour Ruby V3](#)

WorkflowStep

La composante de base d'un flux de travail.

Table des matières

CopyStepDetails

Détails relatifs à une étape qui effectue une copie de fichier.

Comprend les valeurs suivantes :

- Une description
- Un emplacement Amazon S3 pour la destination de la copie du fichier.
- Un indicateur qui indique s'il faut écraser un fichier existant portant le même nom. L'argument par défaut est FALSE.

Type : objet [CopyStepDetails](#)

Obligatoire : non

CustomStepDetails

Détails d'une étape qui appelle une AWS Lambda fonction.

Se compose du nom de la fonction Lambda, de la cible et du délai d'expiration (en secondes).

Type : objet [CustomStepDetails](#)

Obligatoire : non

DecryptStepDetails

Détails d'une étape de déchiffrement d'un fichier chiffré.

Comprend les valeurs suivantes :

- Un nom descriptif
- Emplacement Amazon S3 ou Amazon Elastic File System (AmazonEFS) pour le fichier source à déchiffrer.
- Un EFS emplacement S3 ou Amazon pour la destination du déchiffrement du fichier.
- Un indicateur qui indique s'il faut écraser un fichier existant portant le même nom. L'argument par défaut est FALSE.
- Le type de cryptage utilisé. Actuellement, seul PGP le chiffrement est pris en charge.

Type : objet [DecryptStepDetails](#)

Obligatoire : non

DeleteStepDetails

Détails d'une étape qui supprime le fichier.

Type : objet [DeleteStepDetails](#)

Obligatoire : non

TagStepDetails

Détails d'une étape qui crée une ou plusieurs balises.

Vous spécifiez une ou plusieurs balises. Chaque balise contient une paire clé-valeur.

Type : objet [TagStepDetails](#)

Obligatoire : non

Type

Les types d'étape suivants ne sont actuellement pas pris en charge.

- **COPY** : copier le fichier à un autre emplacement.
- **CUSTOM**- Effectuez une étape personnalisée avec une AWS Lambda fonction cible.
- **DECRYPT** : déchiffrer un fichier chiffré avant d'être chargé.
- **DELETE** : supprimer le fichier.
- **TAG** : ajouter une balise au fichier.

Type : String

Valeurs valides : COPY | CUSTOM | TAG | DELETE | DECRYPT

Obligatoire : non

consultez aussi

Pour plus d'informations sur son utilisation API dans l'une des langues spécifiques AWS SDKs, consultez ce qui suit :

- [AWS SDK pour C++](#)

- [AWS SDK pour Go](#)
- [AWS SDK pour Java V2](#)
- [AWS SDK pour Ruby V3](#)

Faire des demandes d'API

Outre l'utilisation de la console, vous pouvez utiliser l'AWS Transfer Family API pour configurer et gérer vos serveurs par programmation. Cette section décrit les opérations AWS Transfer Family, la signature des requêtes pour l'authentification et la gestion des erreurs. Pour plus d'informations sur les régions et les points de terminaison disponibles pour Transfer Family, consultez la section [AWS Transfer Family Points de terminaison et quotas](#) dans le Références générales AWS

Note

Vous pouvez également utiliser les AWS SDK lorsque vous développez des applications avec Transfer Family ;. Les AWS SDK pour Java, .NET et PHP intègrent l'API Transfer Family sous-jacente, simplifiant ainsi vos tâches de programmation. Pour plus d'informations sur le téléchargement des bibliothèques du SDK, consultez la section [Exemples de bibliothèques de code](#).

Rubriques

- [Transfer Family a requis les en-têtes de demande](#)
- [Transfer Family : saisie et signature des demandes](#)
- [Réponses d'erreur](#)
- [Bibliothèques disponibles](#)

Transfer Family a requis les en-têtes de demande

Cette section décrit les en-têtes obligatoires que vous devez envoyer avec chaque requête POST à AWS Transfer Family. Vous incluez les en-têtes HTTP pour identifier les informations clés relatives à la requête, y compris l'opération que vous souhaitez appeler, la date de la requête et les informations correspondant à votre autorisation en tant qu'expéditeur de la requête. Les en-têtes ne sont pas sensibles à la casse et leur ordre n'est pas important.

L'exemple suivant montre les en-têtes utilisés dans l'[ListServers](#) opération.


```

POST / HTTP/1.1
Host: transfer.us-east-1.amazonaws.com
x-amz-target: TransferService.ListServers
x-amz-date: 20220507T012034Z
Authorization: AWS4-HMAC-SHA256 Credential=AKIDEXAMPLE/20220507/us-east-1/transfer/
aws4_request,
    SignedHeaders=content-type;host;x-amz-date;x-amz-target,
    Signature=13550350a8681c84c861aac2e5b440161c2b33a3e4f302ac680ca5b686de48de
Content-Type: application/x-amz-json-1.1
Content-Length: 17

{"MaxResults":10}

```

Les en-têtes suivants doivent être inclus dans vos requêtes POST adressées à Transfer Family. Les en-têtes ci-dessous qui commencent par « x-amz » sont spécifiques à AWS. Tous les autres en-têtes répertoriés sont des en-têtes courants utilisés dans les transactions HTTP.

En-tête	Description
Authorization	L'en-tête d'autorisation est obligatoire. Le format est la signature de demande Sigv4 standard, qui est documentée dans la section Signing AWS API requests .
Content-Type	application/x-amz-json-1.1 À utiliser comme type de contenu pour toutes les demandes adressées à Transfer Family. <pre>Content-Type: application/x-amz-json-1.1</pre>
Host	Utilisez l'en-tête de l'hôte pour spécifier le point de terminaison Transfer Family auquel vous envoyez votre demande. Par exemple, <code>transfer.us-east-1.amazonaws.com</code> est le point de terminaison pour la région USA Est (Ohio). Pour plus d'informations sur les points de terminaison disponibles pour Transfer Family, consultez la section AWS Transfer Family Points de terminaison et quotas dans le. Références générales AWS <pre>Host: transfer. <i>region</i>.amazonaws.com</pre>

En-tête	Description
x-amz-date	Vous devez fournir l'horodatage dans l'en-tête HTTP ou dans l'AWSx-amz-date en-tête. (Certaines bibliothèques client HTTP ne vous permettent pas de définir l'en-tête Date.) Lorsqu'un x-amz-date en-tête est présent, Transfer Family ignore tout Date en-tête lors de l'authentification de la demande. Le x-amz-date format doit être ISO8601, au format YYYYMMDD'T'HHMMSS'Z'. <pre>x-amz-date: YYYYMMDD'T'HHMMSS'Z'</pre>
x-amz-target	Cet en-tête spécifie la version de l'API et l'opération que vous demandez. Les valeurs d'en-tête cibles sont formées en concaténant la version de l'API avec le nom de l'API et ont le format suivant. <pre>x-amz-target: TransferService. operationName</pre> La valeur OperationName (ListServers par exemple) se trouve dans la liste des API, ListServers
x-amz-security-token	Cet en-tête est obligatoire lorsque les informations d'identification utilisées pour signer la demande sont des informations d'identification temporaires ou des informations d'identification de session (pour plus de détails, voir Utilisation d'informations d'identification temporaires avec les AWS ressources dans le guide de l'utilisateur IAM). Voir Ajouter la signature à la requête HTTP dans le Référence générale d'Amazon Web Services pour plus d'informations.

Transfer Family : saisie et signature des demandes

Toutes les entrées de demande doivent être envoyées dans le cadre de la charge utile JSON dans le corps de la demande. Pour les actions dans lesquelles tous les champs de requête sont facultatifs, par exemple `ListServers`, vous devez toujours fournir un objet JSON vide dans le corps de la

demande, tel que`{}`. La structure de la demande/réponse de charge utile de Transfer Family est documentée dans la référence d'API existante, par exemple. [DescribeServer](#)

Transfer Family prend en charge l'authentification à l'aide de AWS Signature Version 4. Pour plus de détails, consultez [la section Signature des demandes d'AWSAPI](#).

Réponses d'erreur

Lorsqu'il y a une erreur, les informations de l'en-tête de réponse contiennent :

- Type de contenu : `application/x-amz-json-1.1`
- Un code d'état HTTP approprié 4xx ou 5xx

Le corps d'une réponse d'erreur contient des informations sur l'erreur qui s'est produite. L'exemple de réponse d'erreur suivant illustre la syntaxe de sortie des éléments de réponse commune à toutes les réponses d'erreur.

```
{
  "__type": "String",
  "Message": "String", <!-- Message is lowercase in some instances -->
  "Resource": String,
  "ResourceType": String
  "RetryAfterSeconds": String
}
```

Le tableau suivant explique les champs de réponse d'erreur JSON affichés dans la syntaxe précédente.

`__type`

L'une des exceptions à un appel d'API Transfer Family.

Type : chaîne

Message ou message

Un des messages de code d'erreur d'opération .

 Note

Certaines exceptions utilisent `message`, d'autres utilisent `Message`. Vous pouvez vérifier le code de votre interface afin de déterminer le cas approprié. Vous pouvez également tester chaque option pour voir laquelle fonctionne.

Type : chaîne

Resource

La ressource pour laquelle l'erreur est invoquée. Par exemple, si vous essayez de créer un utilisateur qui existe déjà, il `Resource` s'agit du nom d'utilisateur de l'utilisateur existant.

Type : chaîne

ResourceType

Type de ressource pour lequel l'erreur est invoquée. Par exemple, si vous essayez de créer un utilisateur qui existe déjà, `ResourceType` c'est le `casUser`.

Type : chaîne

RetryAfterSeconds

Le nombre de secondes à attendre avant de réessayer la commande.

Type : chaîne

Exemples de réponses aux erreurs

Le corps JSON suivant est renvoyé si vous appelez `DescribeServerAPI` et spécifiez un serveur qui n'existe pas.

```
{
  "__type": "ResourceNotFoundException",
  "Message": "Unknown server",
  "Resource": "s-11112222333344444",
  "ResourceType": "Server"
}
```

Le corps JSON suivant est renvoyé si l'exécution d'une API entraîne un ralentissement.

```
{
  "__type": "ThrottlingException",
  "RetryAfterSeconds": "1"
}
```

Le corps JSON suivant est renvoyé si vous utilisez l'`CreateServerAPI` et que vous ne disposez pas des autorisations suffisantes pour créer un serveur Transfer Family.

```
{
  "__type": "AccessDeniedException",
  "Message": "You do not have sufficient access to perform this action."
}
```

Le corps JSON suivant est renvoyé si vous utilisez l'`CreateUserAPI` et spécifiez un utilisateur qui existe déjà.

```
{
  "__type": "ResourceExistsException",
  "Message": "User already exists",
  "Resource": "Alejandro-Rosalez",
  "ResourceType": "User"
}
```

Bibliothèques disponibles

AWS fournit des bibliothèques, des exemples de code, des didacticiels et d'autres ressources aux développeurs de logiciels qui préfèrent créer des applications à l'aide d'API spécifiques au langage plutôt que des outils de ligne de commande et de l'API de requête. Ces bibliothèques fournissent des fonctions de base (non incluses dans les API), telles que l'authentification des demandes, les nouvelles tentatives et la gestion des erreurs, afin de faciliter le démarrage. Voir [Outils sur lesquels s'appuyer AWS](#)

Pour les bibliothèques et les exemples de code dans toutes les langues, voir [Exemples de code et bibliothèques](#).

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 Signature Version 4, consultez [Signature des demandes d'API AWS](#) dans le Guide de l'utilisateur IAM.

Action

Action à effectuer.

Type : chaîne

Obligatoire : oui

Version

Version de l'API pour laquelle la demande est écrite, au format AAAA-MM-JJ.

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 [Création d'une demande d'API AWS 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/heure suivante est une valeur X-Amz-Date valide : 20120325T120000Z.

Condition : X-Amz-Date est un en-tête facultatif pour toutes les demandes. Il peut être utilisé pour remplacer la date dans la signature des demandes. Si l'en-tête Date est spécifié au format de base ISO 8601, X-Amz-Date n'est pas obligatoire. Lorsque X-Amz-Date est utilisé, il remplace toujours la valeur de l'en-tête Date. Pour plus d'informations, consultez [Éléments d'une signature de demande d'API AWS](#) dans le Guide de l'utilisateur IAM.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Security-Token

Le jeton de sécurité temporaire obtenu lors d'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 issues d'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 [Création d'une demande d'API AWS 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

Erreurs courantes

Cette section répertorie les erreurs communes aux actions d'API de tous les services AWS. 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 requête n'est pas conforme aux normes AWS.

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 l'ID de clé d'accès AWS fourni(e) 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'accès AWS a besoin d'un abonnement pour le service.

Code d'état HTTP : 403

RequestExpired

La demande a atteint le service plus de 15 minutes après la date affichée sur la demande ou plus de 15 minutes après la date d'expiration de la demande (comme pour les URL pré-signées) ou la date affichée sur la demande est postérieure de 15 minutes.

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 service AWS.

Code d'état HTTP : 400

Historique du document pour AWS Transfer Family

Le tableau suivant décrit la documentation de cette version de AWS Transfer Family.

- APIversion : transfer-2018-11-05
- Dernière mise à jour de la documentation : 16 janvier 2024

Modification	Description	Date
Intégrer à Amazon EventBridge	AWS Transfer Family publie désormais automatiquement des événements sur Amazon EventBridge pour toutes les opérations de transfert de fichiers. Pour plus de détails, consultez Gestion des Transfer Family événements à l'aide de Amazon EventBridge .	8 février 2024
Ajout de nouvelles politiques de sécurité	AWS Transfer Family a ajouté de nouvelles FIPS politiques non liées à FIPS la sécurité. En outre, la politique de sécurité par défaut attribuée aux serveurs est toujours la plus récente. Pour plus de détails, consultez Politiques de sécurité pour AWS Transfer Family .	5 février 2024
Support des adresses IP statiques pour les SFTP connecteurs et AS2	Transfer Family fournit désormais des adresses IP statiques pour les SFTP connecteurs et AS2. Cela permet de se connecter à des SFTP serveurs distants	16 janvier 2024

Modification	Description	Date
	sécurisés par des contrôles de liste d'adresses IP autorisées. En effet AS2, nous introduisons des adresses IP statiques pour les MDN réponses asynchrones des AS2 serveurs.	
Le guide de l'utilisateur a été réorganisé afin de mieux correspondre à la dernière version de AWS Transfer Family.	Transfer Family a ajouté de nombreuses fonctionnalités depuis la création du guide, ce qui a nécessité une restructuration du guide.	3 janvier 2024

Modification	Description	Date
Améliorations apportées aux mappages de répertoires logiques Optimisation des performances des listes Amazon S3	Transfer Family prend désormais en charge les mappages de répertoires logiques jusqu'à 2,1 Mo. Vous pouvez également désormais déclarer si le mappage d'un utilisateur est dirigé vers un fichier. Pour de plus amples informations, veuillez consulter Règles d'utilisation des répertoires logiques. Lorsque vous créez ou mettez à jour un serveur qui utilise Amazon S3 pour le stockage, vous pouvez désormais optimiser les performances de la liste de vos répertoires (ou dossiers) S3. Pour de plus amples informations, veuillez consulter Configuration d'un point SFTP de FTPS terminais on ou d'FTPun serveur.	17 novembre 2023
Port alternatif pour les SFTP serveurs dotés de points de terminaison de cloud privé virtuel (VPC)	Vous pouvez désormais activer un autre port non standard pour vos serveurs SFTP Transfer Family dotés de points de VPC terminais on. Pour de plus amples informations, veuillez consulter Création d'un serveur dans un cloud privé virtuel.	17 novembre 2023

Modification	Description	Date
Support pour SFTP connecteurs	SFTPLes connecteurs étendent les capacités de AWS Transfer Family communication avec des serveurs distants à la fois dans le cloud et sur site. Pour de plus amples informations, veuillez consulter Envoyer et récupérer des fichiers à l'aide d'un SFTP connecteur .	25 juillet 2023
Support pour l'authentification AS2 de base	Transfer Family prend désormais en charge l'utilisation de l'authentification de base pour les serveurs utilisant le protocole Applicability Statement 2 (AS2). Pour de plus amples informations, veuillez consulter Authentification de base pour les AS2 connecteurs .	30 juin 2023

Modification	Description	Date
Support pour la JSON journalisation structurée	Transfer Family prend désormais en charge la fourniture de JSON journaux structurés à Amazon CloudWatch, le regroupement des flux de journaux dans des groupes de journaux personnalisés et l'exécution de requêtes de journal communes à travers les protocoles. Pour de plus amples informations, veuillez consulter Amazon CloudWatch Logging pour AWS Transfer Family .	24 juin 2023
Support de plusieurs méthodes d'authentification	Transfer Family prend en charge l'authentification à l'aide d'un mot de passe, d'une paire de clés publique/privée, ou des deux. Ceci est disponible pour les serveurs qui utilisent le SFTP protocole et un fournisseur d'identité personnalisé. Pour de plus amples informations, veuillez consulter Création d'un SFTP serveur activé .	17 mai 2023

Modification	Description	Date
Support pour le déchiffrement de Pretty Good Privacy (PGP) avec des fichiers traités par Transfer Family à l'aide de workflows	Transfer Family dispose d'un support intégré pour le déchiffrement de Pretty Good Privacy (PGP). Vous pouvez utiliser le PGP déchiffrement sur les fichiers chargés sur SFTP Amazon Simple Storage Service (Amazon S3) ou FTP Amazon Elastic File System (Amazon) ou sur Amazon Elastic File System (Amazon). FTPS EFS Pour plus d'informations, consultez Génération et gestion PGP des clés et Utilisez PGP le déchiffrement dans votre flux de travail .	21 décembre 2022
Support entièrement géré du protocole de transfert de fichiers Applicability Statement 2 (AS2) avec les serveurs Transfer Family Family	Vous pouvez créer des serveurs qui utilisent le AS2 protocole pour envoyer et recevoir des informations à destination et en provenance de partenaires commerciaux situés à l'intérieur ou à l'extérieur de l' AWS environnement. Pour de plus amples informations, veuillez consulter Configuration AS2 .	25 juillet 2022

Modification	Description	Date
Support pour l'affichage de bannières lors de la création d'un serveur	Vous pouvez ajouter des messages personnalisés lorsque vous créez des serveurs. Vous pouvez afficher un message de pré-authentification (tous les protocoles) et un message de post-authentification (pour FTP et les FTPS serveurs) . Pour plus d'informations, veuillez consulter Création d'un SFTP serveur activé, Création d'un FTPS serveur activé ou Création d'un FTP serveur activé.	17 février 2022
Support en AWS Lambda tant que fournisseur d'identité	Vous pouvez désormais vous connecter à un fournisseur d'identité personnalisé à l'AWS Lambda aide de ses serveurs Transfer Family. Auparavant, vous deviez fournir un Amazon API Gateway URL pour intégrer un fournisseur d'identité personnalisé. Pour de plus amples informations, veuillez consulter Utilisation AWS Lambda pour intégrer votre fournisseur d'identité.	16 novembre 2021

Modification	Description	Date
Support pour les flux de travail de transfert de fichiers gérés	Les flux de travail de transfert de fichiers gérés vous fournissent des abstractions de traitement après le téléchargement pour les tâches courantes que vous effectuez actuellement manuellement. Pour de plus amples informations, veuillez consulter AWS Transfer Family flux de travail gérés .	2 septembre 2021
Support pour AWS Directory Service for Microsoft Active Directory	Outre les fournisseurs d'identité personnalisés et gérés par des services, vous pouvez désormais les utiliser pour gérer l'accès des utilisateurs AWS Directory Service for Microsoft Active Directory à des fins d'authentification et d'autorisation. Pour de plus amples informations, veuillez consulter Utilisation du fournisseur d'identité du AWS Directory Service .	24 mai 2021

Modification	Description	Date
Nouveau Régions AWS	AWS Transfer Family est désormais disponible dans la région Afrique (Cape Town). Pour plus d'informations sur les points de terminaison Transfer Family, consultez la section AWS Transfer Family Points de terminaison et quotas dans le. Références générales AWS	24 février 2021
Nouveau Régions AWS	AWS Transfer Family est désormais disponible dans les régions Asie-Pacifique (Hong Kong) et Moyen-Orient (Bahreïn). Pour plus d'informations sur les points de terminaison Transfer Family, consultez la section AWS Transfer Family Points de terminaison et quotas dans le. Références générales AWS	17 février 2021
Support pour Amazon EFS en tant que magasin de données	Transfer Family prend désormais en charge les transferts de fichiers vers et depuis Amazon Elastic File System (AmazonEFS). Amazon EFS est un système de NFS fichiers élastique simple, évolutif et entièrement géré. Pour de plus amples informations, veuillez consulter Configuration d'un système de EFS fichiers Amazon .	6 janvier 2021

Modification	Description	Date
Support pour AWS WAF	Transfer Family prend désormais en charge AWS WAF un pare-feu pour applications Web qui aide à protéger les applications Web et les API opérations contre les attaques. Pour de plus amples informations, veuillez consulter Ajouter un pare-feu pour applications Web .	24 novembre 2020
Support de plusieurs groupes de sécurité dans un cloud privé virtuel (VPC)	Vous pouvez désormais associer plusieurs groupes de sécurité à un serveur dans un VPC. Pour de plus amples informations, veuillez consulter Création d'un serveur dans un cloud privé virtuel .	15 octobre 2020

Modification	Description	Date
Nouveau Régions AWS	Transfer Family est désormais disponible dans les AWS GovCloud (US) régions. Pour plus d'informations sur les points de terminais on Transfer Family pour les AWS GovCloud (US) régions, consultez la section AWS Transfer Family Points de terminaison et quotas dans le. Références générales AWS Pour plus d'informations sur l'utilisation de Transfer Family dans les AWS GovCloud (US) régions, consultez AWS Transfer Family le guide de AWS GovCloud (US) l'utilisa teur.	30 septembre 2020
Une politique de sécurité avec des algorithmes cryptogra phiques pris en charge peut désormais être attachée à votre serveur	Vous pouvez désormais associer à votre serveur une politique de sécurité contenant un ensemble d'algorithmes cryptographiques pris en charge. Pour de plus amples informations, veuillez consulter Politiques de sécurité pour AWS Transfer Family .	12 août 2020

Modification	Description	Date
Support pour les points de terminaison du Federal Information Processing Standard (FIPS)	FIPS Les points de terminaison compatibles sont désormais disponibles en Amérique du Nord. Régions AWS Pour les régions disponibles, consultez les AWS Transfer Family points de terminaison et les quotas dans le Références générales AWS. FIPS Pour activer un point de terminaison de serveur SFTP activé, consultez Création d'un SFTP serveur activé. FIPS Pour activer un point de terminaison de serveur FTPS activé, consultez Création d'un FTPS serveur activé. FIPS Pour activer un point de terminaison de serveur FTP activé, consultez Création d'un FTP serveur activé.	12 août 2020
Augmentation de la longueur des caractères du nom d'utilisateur et ajout de caractères autorisés	Les noms d'utilisateur peuvent désormais contenir des signes (@) et des points (.), et leur longueur maximale est de 100 caractères. Pour ajouter un utilisateur, consultez Gestion des utilisateurs pour les points de terminaison du serveur.	12 août 2020

Modification	Description	Date
Support pour la création automatique de rôles Amazon CloudWatch logging AWS Identity and Access Management (IAM)	Transfer Family prend désormais en charge la création automatique d'un IAM rôle de CloudWatch journalisation pour visualiser l'activité de l'utilisateur final. Pour plus d'informations, veuillez consulter Création d'un SFTP serveur activé , Création d'un FTPS serveur activé ou Création d'un FTP serveur activé .	30 juillet 2020
AWS Transfer Family prend désormais en charge l'adresse IP source comme facteur d'autorisation.	Transfer Family prend en charge l'utilisation des adresses IP sources des utilisateurs finaux comme facteur d'autorisation, ce qui vous permet d'appliquer un niveau de sécurité supplémentaire lorsque vous autorisez l'accès via Secure File Transfer Protocol (SFTP), File Transfer Protocol over SSL (FTPS) ou File Transfer Protocol (FTP). Pour de plus amples informations, veuillez consulter Travailler avec des fournisseurs d'identité personnalisés .	9 juin 2020

Modification	Description	Date
AWS Transfer for SFTP existe maintenant AWS Transfer Family et ajoute le support pour FTP etFTPS.	Vous pouvez désormais utiliser deux protocoles supplémentaires pour les transferts de fichiers de vos utilisateurs : File Transfer Protocol Secure (FTPS) et File Transfer Protocol (FTP). Les utilisateurs peuvent déplacer, exécuter, sécuriser et intégrer des flux de travail FTP basés FTP sur over SSL (FTPS) et en texte brut AWS, en plus de la prise en charge existante du protocole de transfert de fichiers sécurisé (SFTP).	23 avril 2020

Modification	Description	Date
Support pour les groupes de sécurité du cloud privé virtuel (VPC) et les adresses IP élastiques	Vous pouvez désormais créer une liste d'autorisations pour les adresses IP entrantes à l'aide de groupes de sécurité, fournissant ainsi un niveau de sécurité supplémentaire aux serveurs. Vous pouvez également associer des adresses IP élastiques au point de terminaison de votre serveur. Ce faisant, vous pouvez permettre aux utilisateurs protégés par des pare-feux d'autoriser l'accès à ce point de terminaison. Pour de plus amples informations, veuillez consulter Création d'un serveur dans un cloud privé virtuel .	10 janvier 2020
Support pour travailler dans un VPC	Vous pouvez désormais créer un serveur dans un VPC. Vous pouvez utiliser votre serveur pour transférer des données via votre client vers et depuis un compartiment Amazon S3 sans passer par Internet public. Pour de plus amples informations, veuillez consulter Création d'un serveur dans un cloud privé virtuel .	27 mars 2019

Modification	Description	Date
La première version de AWS Transfer Family a été publiée.	Cette version initiale comprend des directives pour la configuration, explique comment se lancer et fournit des informations sur la configuration du client, la configuration des utilisateurs et la surveillance de l'activité.	25 novembre 2018

Glossaire AWS

Pour connaître la terminologie la plus récente d'AWS, consultez le [Glossaire AWS](#) dans la Référence Glossaire AWS.

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.