



Guide de l'utilisateur

AWS Transfer Family



AWS Transfer Family: Guide de l'utilisateur

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

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

Table of Contents

Qu'est-ce que c'est AWS Transfer Family ?	1
Comment AWS Transfer Family fonctionne	4
Articles de blog pertinents pour Transfer Family	5
Conditions préalables	9
Régions, points de terminaison et quotas	9
Inscrivez-vous pour AWS	10
Configurer le stockage	10
Configuration d'un compartiment Amazon S3	11
Configuration d'un système de fichiers Amazon EFS	16
Création d'un rôle et d'une politique IAM	20
Créer un rôle d'utilisateur	21
Comment fonctionnent les politiques de session	24
Exemple de politique read/write d'accès	28
Tutoriels Transfer Family	32
Commencez avec les points de terminaison de serveur	33
Conditions préalables	33
Étape 1 : connectez-vous à la AWS Transfer Family console	34
Étape 2 : Création d'un SFTP-enabled serveur	35
Étape 3 : Ajouter un utilisateur géré par le service	36
Étape 4 : Transférer un fichier à l'aide d'un client	37
Création d'un flux de travail de déchiffrement	39
Étape 1 : Configuration d'un rôle d'exécution	40
Étape 2 : créer un flux de travail géré	41
Étape 3 : ajouter le flux de travail à un serveur et créer un utilisateur	42
Étape 4 : Création d'une paire de clés PGP	44
Étape 5 : Stocker la clé privée PGP dans AWS Secrets Manager	45
Étape 6 : Chiffrer un fichier	46
Étape 7 : Exécuter le flux de travail et afficher les résultats	47
Création et utilisation de connecteurs SFTP	48
Types de sorties de connecteurs	49
Étape 1 : créer les ressources de soutien nécessaires	50
Étape 2 : Création et test d'un connecteur SFTP	56
Étape 3 : Envoyer et récupérer des fichiers à l'aide du connecteur SFTP	62
Procédures pour créer un serveur Transfer Family à utiliser comme serveur SFTP distant	67

Utiliser un fournisseur d'identité personnalisé	70
Conditions préalables	70
Étape 1 : créer une CloudFormation pile	71
Étape 2 : Vérifiez la configuration de la méthode API Gateway pour votre serveur	72
Étape 3 : Afficher les détails du serveur Transfer Family	73
Étape 4 : vérifiez que votre utilisateur peut se connecter au serveur	75
Étape 5 : tester la connexion SFTP et le transfert de fichiers	75
Étape 6 : Limiter l'accès au bucket	76
Mettre à jour Lambda si vous utilisez Amazon EFS	78
Configuration d'une configuration AS2	79
Étape 1 : créer des certificats pour AS2	81
Étape 2 : Importer des certificats en tant que ressources de certificats Transfer Family	85
Étape 3 : Créez des profils pour vous et votre partenaire commercial	86
Étape 4 : Création d'un serveur Transfer Family utilisant le protocole AS2	87
Étape 5 : Créez un accord entre vous et votre partenaire	91
Étape 6 : Créez un lien entre vous et votre partenaire	93
Étape 7 : Testez l'échange de fichiers via AS2 à l'aide de Transfer Family	94
Configuration d'une application Web de base	96
Conditions préalables	96
Étape 1 : créer les ressources de soutien nécessaires	97
Étape 2 : Création d'une application Web Transfer Family	97
Étape 3 : configurer le partage Cross-origin des ressources (CORS) pour votre bucket	99
Étape 4 : Ajouter un utilisateur à votre application Web Transfer Family	100
Étape 5 : enregistrer un emplacement dans Amazon S3 et créer une autorisation d'accès ...	101
Étape 6 : Accédez à votre application Web Transfer Family en tant qu'utilisateur	104
Étapes suivantes	105
Intégrez Okta en tant que fournisseur d'identité pour les applications Web	106
Configurer une application Web avec un accès sélectif à plusieurs compartiments	108
Conditions préalables	108
Étape 1 : créer une application Web Transfer Family	109
Étape 2 : Configuration des rôles IAM pour l'accès S3	110
Étape 3 : configurer les autorisations d'accès S3	112
Étape 4 : enregistrer les emplacements des compartiments S3	113
Étape 5 : créer des autorisations d'accès	113
Étape 6 : Configuration de la politique CORS pour les compartiments S3	114
Étape 7 : tester la configuration	115

Conclusion	115
Transfer Family pour SFTP, FTPS, FTP	116
Options du fournisseur d'identité	116
AWS Transfer Family matrice des types de terminaux	118
Configuration d'un point de terminaison du serveur Transfer Family	123
Création d'un SFTP-enabled serveur	125
Création d'un FTPS-enabled serveur	133
Création d'un FTP-enabled serveur	142
Création d'un serveur dans un VPC	151
Utilisation de noms d'hôtes personnalisés	176
FTP/FTPS Considérations relatives à la NLB	180
Transférer des fichiers via le terminal du serveur	181
SFTP/FTPS/FTP Commandes disponibles	184
Trouvez votre point de terminaison Amazon VPC	186
Évitez les setstat erreurs	187
Utiliser OpenSSH	38
Utiliser WinSCP	190
Utilisez Cyberduck	37
Utiliser FileZilla	193
Utiliser un client Perl	194
Utiliser le LFTP	195
Traitement après le téléchargement	195
Messages SFTP	196
Gérer les utilisateurs	199
Comparaison entre Amazon EFS et Amazon S3	199
Répertoires logiques	200
Quotas de groupe Active Directory	201
Service-managed utilisateurs	202
Fournisseur d'identité personnalisé	212
Service d'annuaire pour MS AD	252
Service d'annuaire pour Entra ID	264
Utiliser des répertoires logiques	271
Comprendre le chroot et la structure des répertoires	272
Règles d'utilisation des répertoires logiques	272
Implémentation de répertoires logiques	274
Exemples de configuration de répertoires logiques	278

Configuration de répertoires logiques pour Amazon EFS	280
AWS Lambda Réponse personnalisée	280
Access FSx pour les systèmes de fichiers NetApp ONTAP	281
Présentation de	282
Conditions préalables	283
Comment fonctionne le stockage FSx avec Transfer Family	284
Création d'un point d'accès S3 pour FSx	285
Utilisation d'alias de point d'accès S3 avec FSx	287
Configuration de Transfer Family pour le stockage FSx	289
Gestion des utilisateurs pour le stockage FSx	291
Configuration des clients de transfert de fichiers	292
Résolution des problèmes de stockage FSx	294
Applications Web Transfer Family	295
Régions AWS pour les applications Web Transfer Family	296
Compatibilité du navigateur pour AWS Transfer Family applications Web	296
Comment créer une application Web Transfer Family	296
Configuration de votre fournisseur d'identité	299
Configuration des rôles IAM	301
Configuration d'une application Web Transfer Family	304
Création d'une application Web Transfer Family	304
Adressage IP	306
Création d'une application Web Transfer Family dans un VPC	307
Création d'une application Web Transfer Family	308
Post-creation étapes	310
Cross-origin politique de partage des ressources (CORS)	310
Restriction de l'accès à un point de terminaison d'un VPC spécifique	312
Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family	313
Configurer le partage Cross-origin des ressources (CORS) pour votre bucket	316
Configurer les autorisations d'accès Amazon S3	318
Utiliser une URL personnalisée	324
Enregistrement pour les applications Web Transfer Family	327
Activation des événements de données Amazon S3	328
Exemples de journaux d'authentification	330
Afficher les entrées du journal	338
Résolution des problèmes liés à vos applications Web	339
Résoudre les erreurs réseau	339

Résoudre les problèmes liés à l'absence d'affichage du bucket configuré	340
Résoudre les erreurs d'URL personnalisées	340
Résoudre les erreurs diverses	341
Des compartiments S3 dupliqués apparaissent dans l'application Web	342
Instructions pour l'utilisateur final	342
Quotas d'applications Web	342
Utilisateurs d'IAM Identity Center	343
Third-party utilisateurs finaux	344
Interface utilisateur final de Transfer Family	345
Actions disponibles	346
Connecteurs SFTP	349
Création de connecteurs SFTP	349
Choix du type de sortie du connecteur SFTP	350
Choix du mode d'adressage IP	351
Stockez les informations d'identification dans Secrets Manager	352
Création d'un connecteur SFTP avec sortie gérée par service	354
Création d'un connecteur SFTP avec sortie VPC-based	365
Tester un connecteur SFTP	377
Connectivité VPC	378
Utilisation de connecteurs SFTP	379
Transférer des fichiers	380
Lister le contenu des répertoires distants	382
Déplacer et supprimer des fichiers sur le serveur distant	384
Surveillance des connecteurs SFTP	386
Utilisez l'API du connecteur pour connaître l'état des demandes de transfert de fichiers	386
Afficher les événements relatifs au connecteur SFTP sur Amazon EventBridge	387
Afficher les journaux du connecteur SFTP sur Amazon CloudWatch	387
Surveillance des connecteurs de type sortie VPC	387
Gestion des connecteurs SFTP	389
Mettre à jour les connecteurs SFTP	390
Afficher les détails du connecteur SFTP	391
Quotas pour les connecteurs SFTP	392
Quotas pour les connecteurs SFTP	392
Dimensionnement de vos connecteurs SFTP	394
Architectures de référence	395
Billets de blogs	395

Ateliers	395
Des solutions	395
Architectures de référence VPC	396
Transfer Family pour AS2	398
Cas d'utilisation de l'AS2	399
Modèles AS2 CloudFormation	404
Personnalisation des modèles AS2	404
Test de votre déploiement AS2	405
Bonnes pratiques pour le déploiement de modèles AS2	405
Configurer AS2	406
Configurations AS2	407
Quotas AS2	409
Caractéristiques et capacités de l'AS2	412
Gérer les certificats AS2	414
Importer des certificats AS2	415
Rotation des certificats AS2	417
Création de profils AS2	419
Création d'un serveur AS2	420
Création d'un serveur AS2 à l'aide de la console Transfer Family	420
Création d'un serveur AS2 à l'aide d'un modèle	424
Création d'un accord AS2	427
Configuration des connecteurs AS2	429
Création d'un connecteur AS2	430
Algorithmes du connecteur AS2	433
Authentification de base pour les connecteurs AS2	434
Activer l'authentification de base pour les connecteurs AS2	436
Afficher les détails du connecteur	439
Transférer des messages AS2	442
Recevoir des messages AS2	443
Configuration du protocole HTTPS pour AS2	444
Transférez des fichiers avec des connecteurs AS2	450
Noms et emplacements des fichiers	453
Codes d'état	455
Exemples de fichiers JSON	456
En-têtes HTTP personnalisés pour AS2	458
Présentation du modèle	459

Comment ça marche	459
Fonctionnalités principales	460
Détails de l'implémentation	460
Déploiement et utilisation	461
Moniteur AS2	462
Codes d'état AS2	464
Codes d'erreur AS2	465
Surveillance de l'expiration des certificats	478
DaysUntilExpiry métrique	478
Bonnes pratiques en matière de surveillance des certificats	479
Exemples de configurations d'alarme	480
Gestion des flux de travail de traitement de fichiers	481
Création d'un flux de travail	483
Configuration et exécution d'un flux de travail	485
Afficher les détails du flux de travail	487
Utiliser des étapes prédéfinies	490
Copier le fichier	490
Déchiffrer le fichier	495
Fichier de balises	501
Supprimer le fichier	502
Variables nommées pour les flux de travail	503
Exemple de balise et de flux de travail de suppression	503
Utiliser des étapes de traitement de fichiers personnalisées	508
Utilisation consécutive de plusieurs fonctions Lambda	510
Accès à un fichier après un traitement personnalisé	510
Exemples d'événements envoyés à une adresse AWS Lambda lors du chargement d'un fichier	511
Exemple de fonction Lambda pour une étape de flux de travail personnalisée	513
Autorisations IAM pour une étape personnalisée	513
Politiques IAM pour les flux de travail	514
Relations de confiance en matière de flux	516
Exemple de rôle d'exécution : déchiffrer, copier et étiqueter	516
Exemple de rôle d'exécution : exécuter la fonction et supprimer	518
Gestion des exceptions pour un flux de travail	519
Surveiller l'exécution du flux de	520
CloudWatch journalisation pour un flux de travail	520

CloudWatch métriques pour les flux de travail	523
Créer un flux de travail à partir du modèle	523
Supprimer un flux de travail d'un serveur Transfer Family	527
Restrictions et limites	528
Gestion des serveurs	531
Afficher la liste des serveurs	531
Supprimer un serveur	532
Afficher les détails du serveur SFTP	533
Afficher les détails du serveur AS2	534
Prise en charge d'IPv6	536
Limitations du protocole IPv6	537
Configuration d'IPv6 pour les serveurs	537
Utiliser ALB pour un serveur public AS2 à double pile	538
Modifier les détails du serveur	540
Modifier les protocoles de transfert de fichiers	543
Modifier le point de terminaison du serveur	545
Modifier la journalisation	546
Modifier la politique de sécurité	547
Modifier le flux de travail géré	549
Modifier les bannières d'affichage de votre serveur	550
Mettez votre serveur en ligne ou hors ligne	550
Modifier la configuration du fournisseur d'identité	551
Passage à un fournisseur d'identité géré par des services	552
Passage au AWS Directory Service	552
Passage à un fournisseur d'identité personnalisé	552
Préservation des utilisateurs lors des transitions entre fournisseurs d'identité	558
Considérations importantes lors du changement de fournisseur d'identité	558
Gérer les clés d'hôte du serveur	558
Quand importer les clés d'hôte	560
Ajouter une clé d'hôte de serveur supplémentaire	560
Supprimer la clé d'hôte d'un serveur	562
Faites pivoter les clés de l'hôte du serveur	563
Informations supplémentaires sur la clé de l'hôte du serveur	565
Surveiller l'utilisation dans la console	565
Gestion des contrôles d'accès	572
Création d'une politique d'accès au compartiment S3	573

Création d'une politique de session	574
Exemple de politique de session	575
Substitutions imbriquées pour les politiques de session	578
Gestion dynamique des autorisations	578
Comprendre l'architecture des autorisations Transfer Family	578
Deux approches de gestion des autorisations	579
Mise en œuvre des politiques de session	580
Implémentation par type d'utilisateur	581
Exemple : simplification de la gestion des rôles avec des politiques de session	582
CloudTrail journalisation	585
Activer la CloudTrail journalisation	587
Activation des événements de données Amazon S3	587
Exemple d'entrée de journal pour la création d'un serveur	588
Journaux d'accès aux données	589
Exemple d'entrée de journal pour un accès aux données réussi	589
Opérations communes d'accès aux données	592
CloudWatch journalisation	593
Types de CloudWatch journalisation pour Transfer Family	593
Création d'une journalisation pour les serveurs	596
Création d'une journalisation pour les serveurs	599
Mettre à jour la journalisation d'un serveur	599
Affichage de la configuration du serveur	602
Gestion de la journalisation des flux de travail	604
Configuration d'un rôle pour CloudWatch	607
Afficher les flux de log de Transfer Family	609
Création d' CloudWatch alarmes Amazon	613
Enregistrement des appels d'API S3 dans les journaux d'accès S3	614
Exemples pour limiter le problème de confusion des adjoints	614
CloudWatch structure du journal pour Transfer Family	616
Journaux structurés JSON pour Transfer Family	616
Les anciens journaux de Transfer Family	619
Exemples d'entrées de CloudWatch journal	622
Exemples d'entrées du journal des sessions de transfert	623
Exemples d'entrées de journal pour les connecteurs SFTP	624
Exemples d'entrées de journal pour les connecteurs VPC Lattice	626
Exemples d'entrées de journal pour les défaillances de l'algorithme d'échange de clés	627

Utilisation de CloudWatch métriques	628
Dimensions de Transfer Family	633
Notifications utilisateur	633
CloudWatch requêtes	634
Gestion des événements à l'aide de EventBridge	637
Transfer Family events	638
Événements relatifs aux serveurs SFTP, FTPS et FTP	638
Événements relatifs au connecteur SFTP	641
Événements AS2	643
Envoi d' Transfer Family événements	644
Création de modèles d'événements	645
Tester les modèles d'événements pour les Transfer Family événements	646
Permissions	647
Ressources supplémentaires	647
Référence détaillée des événements	647
Événements liés au serveur	648
Événements relatifs au connecteur	656
Événements AS2	663
Sécurité	670
Avantages de la connectivité VPC en termes de sécurité	671
Modèle de sécurité VPC Lattice	671
Bonnes pratiques de sécurité pour la connectivité VPC	672
Politiques de sécurité pour les serveurs	672
Algorithmes cryptographiques	674
Détails de la politique de sécurité	685
Politiques de sécurité pour les connecteurs SFTP	703
Algorithmes cryptographiques	704
Détails de la politique de sécurité du connecteur SFTP	704
Post-Quantum politiques de sécurité	706
À propos de l'échange de clés hybrides post-quantiques en SSH	707
Comment l'utiliser	708
Comment le tester	709
Protection des données	713
Chiffrement des données dans Transfer Family	714
Chiffrement au repos	715
Gestion des clés	716

Présentation de l'algorithme	717
Authentification SSH	717
Algorithmes PGP	718
Génération de clés SSH	720
Faire pivoter les clés SSH	725
Génération de clés PGP	728
Gérer les clés PGP	729
Clients PGP pris en charge	734
Gestion des identités et des accès	736
Public ciblé	736
Authentification par des identités	737
Gestion de l'accès à l'aide de politiques	738
Comment ? AWS Transfer Family fonctionne avec IAM	740
Identity-based exemples de politiques	745
Tag-based exemples de politiques	748
Résolution des problèmes d'identité et d'accès avec	751
Clés de condition IAM	754
Validation de conformité	756
Résilience	757
Points de terminaison VPC pour les API	758
Contrôle de l'accès à l'aide des politiques de point de terminaison VPC	758
Créer un point de terminaison d'un VPC	759
Sécurité de l'infrastructure	760
Considérations relatives à la NLB et au NAT	760
Sécurité de l'infrastructure de connectivité VPC	762
Pare-feu pour applications Web	763
Cross-service prévention confuse des adjoints	764
Rôles des utilisateurs de Transfer Family	766
Rôles du flux de travail Transfer Family	768
Rôles du connecteur Transfer Family	769
logging/invoctionRôles de Transfer Family	770
AWS politiques gérées	772
AWSTransferConsoleFullAccess	773
AWSTransferFullAccess	773
AWSTransferLoggingAccess	773
AWSTransferReadOnlyAccess	773

Mises à jour des politiques	773
Modules Transfer Family Terraform	775
Serveurs SFTP	775
Connecteurs SFTP	775
AS2	776
Échange de données B2B	776
Résolution des problèmes liés à Transfer Family	777
Problèmes d'authentification	777
Défaillances d'authentification : SSH/SFTP	778
Problème de domaines incompatibles avec Managed AD	778
Limites de groupe Active Directory dépassées	779
Problèmes d'authentification divers	779
Résoudre les problèmes liés à Amazon API Gateway	780
Résoudre les problèmes liés au test de votre fournisseur d'identité	782
Dupliquer des compartiments Amazon S3 dans une application Web	342
Problèmes liés au connecteur SFTP	783
Résoudre les problèmes liés à l'ajout de clés d'hôte fiables pour votre connecteur SFTP	783
Échec d'une négociation clé	784
Régulation du connecteur SFTP	784
Optimisation des performances du connecteur SFTP	785
Résoudre les problèmes de connectivité VPC	786
Problèmes divers liés au connecteur SFTP	789
Problèmes de connectivité SFTP	790
Résoudre les problèmes de connectivité SFTP	790
Résoudre les problèmes liés au client SFTP	791
Résoudre les problèmes de téléchargement de fichiers	791
Résoudre les problèmes de connecteur SFTP de type VPC de sortie	792
Problèmes liés aux fournisseurs d'identité personnalisés	794
Résoudre les erreurs d'intégration d'API Gateway	795
Résoudre les problèmes de temporisation des fonctions Lambda	796
Résoudre les problèmes de temporisation Lambda constants	797
Résoudre les problèmes liés aux exceptions <code>KeyError</code>	797
Problèmes de flux de travail	798
Résoudre les problèmes liés aux flux de travail gérés	798
Résoudre les problèmes de déchiffrement du flux de travail	801
Problèmes liés à l'EFS	805

Résoudre les problèmes liés à Amazon EFS	805
Problèmes de stockage et de chiffrement	808
Résoudre les problèmes liés aux compartiments Amazon S3 chiffrés	808
Résolution des problèmes d'exception ResourceNotFound	809
Problèmes de surveillance et d'alerte	809
Résoudre les problèmes liés aux métriques manquantes ou incomplètes CloudWatch	810
Résoudre les problèmes liés aux événements manquants EventBridge	811
Cross-region problèmes de transfert	812
Résoudre les problèmes d'autorisation de transfert entre régions	812
Résoudre les problèmes de performances de transfert entre régions	814
Problèmes de déploiement de Terraform	815
Résoudre les problèmes de création de ressources Terraform	815
Résoudre les problèmes de gestion de l'état de Terraform	816
Problèmes d'intégration du WAF	817
Résoudre les problèmes liés au blocage du trafic légitime par le WAF	817
Résoudre les problèmes d'intégration du WAF avec les fournisseurs d'identité personnalisés	818
Service-managed problèmes liés aux utilisateurs	819
Résoudre les problèmes des utilisateurs gérés par des services	819
Problèmes liés à l'AS2	820
Résoudre les problèmes liés à l'AS2	821
Problèmes liés aux certificats AS2	821
Problèmes de réception AS2 MDN	821
Problèmes de surveillance de l'expiration des certificats	822
Référence API	824
Effectuer des demandes d'API	825
Transfer Family a requis les en-têtes de demande	826
Transfer Family : saisie et signature des demandes	826
Réponses d'erreur	827
Bibliothèques disponibles	829
Fournisseurs d'identité	830
Conventions	831
Formats d'identification	831
Formats ARN	832
DNS et points de terminaison	833
Points de terminaison d'API	833

Points de terminaison du serveur 833

Historique de la documentation 835

..... dcccliv

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 via SFTP, AS2, FTPS, FTP et les transferts basés sur un navigateur Web directement vers et depuis les services de stockage. AWS 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 NFS (Network File System) Amazon Elastic File System (Amazon EFS). Pour plus d'informations sur Amazon EFS, 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 sécurisé (SFTP) : version 3

Le document officiel de l'IETF est ici : [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

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

Note

Pour les connexions de données FTP et FTPS, 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.
- Subscription-based distribution de données avec vos clients.
- Transferts interne au sein de votre organisation.

Voici quelques exemples d'utilisation courants de l'utilisation 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 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)

Voici quelques exemples d'utilisation courants des applications Web Transfer Family :

- Accès simplifié aux données d'Amazon S3 pour un éventail plus large et diversifié d'utilisateurs professionnels
- Gestion centralisée de l'accès aux données pour votre personnel
- Visualisation des autorisations d'accès Amazon S3 via une interface gérée

Avec Transfer Family, vous avez accès à un serveur compatible avec le protocole de transfert de fichiers AWS (ou à une interface Web de transfert de fichiers géré), 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. Pour les serveurs, vous devez d'abord associer votre nom d'hôte au point de terminaison du serveur, puis ajouter vos utilisateurs et leur fournir 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.

Pour les applications Web Transfer Family, déterminez vos paramètres de configuration et appliquez des personnalisations facultatives. Ensuite, vos utilisateurs peuvent se connecter et transférer directement des données vers et depuis Amazon S3.

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 se mettre à l'échelle à la demande et peut atteindre plusieurs pétaoctets sans perturber les applications. Il augmente ou diminue automatiquement la capacité au fil de vos ajouts et suppressions de fichiers. 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 la référence de l'API du service.

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

- [Comment AWS Transfer Family fonctionne](#)
- [Conditions préalables](#)
- [Commencer à utiliser les points de terminaison AWS Transfer Family de serveur](#)
- [Applications Web Transfer Family](#)

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 (Amazon EFS) via les protocoles ou navigateurs Web suivants :

- Protocole de transfert de fichiers sécurisé (SFTP) : version 3

Le document officiel de l'IETF est ici : [SSH File Transfer](#) Protocol draft-ietf-secsh-filexfer-02.txt.

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

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 Latency-based routage, consultez le billet de blog [Minimisez la latence du réseau lors de vos AWS transferts pour les serveurs SFTP](#).

Transfer Family Managed File Transfer Workflows (MFTW) est 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 de. AWS Transfer Family Les clients peuvent utiliser MFTW pour automatiser diverses étapes de traitement telles que la copie, le balisage, la numérisation, le filtrage et encrypting/decrypting les données transférées à l'aide de Transfer Family.

compressing/decompressing 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 :

- [OpenSSH](#) — Un utilitaire de ligne de commande pour Macintosh et Linux.
- [WinSCP](#) — Windows-only Un client graphique.
- [Cyberduck](#) — Un client graphique pour Linux, Macintosh et Microsoft Windows.
- [FileZilla](#) — Un client graphique pour Linux, Macintosh et Windows.

AWS propose les ateliers Transfer Family suivants.

- Créez une solution de transfert de fichiers qui tire parti des SFTP/FTPS points de terminaison gérés et d'Amazon Cognito et DynamoDB AWS Transfer Family pour la gestion des utilisateurs. Vous pouvez consulter les détails de cet atelier [ici](#).
- [Créez un point de terminaison Transfer Family avec AS2 activé et un connecteur Transfer Family AS2. Vous pouvez consulter les détails de cet atelier ici.](#)
- Développez une solution qui fournit des conseils prescriptifs et un laboratoire pratique sur la manière de créer une architecture de transfert de fichiers évolutive et sécurisée AWS sans avoir à modifier les applications existantes ou à gérer l'infrastructure de serveurs. Vous pouvez consulter les détails de cet atelier [ici](#).

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 présenté 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
Déployez Okta en tant que fournisseur d'identité personnalisé pour AWS Transfer Family	11 août 2025

Titre et lien de l'article de blog	Date
Automatiser le traitement des demandes de soins de santé du papier au format électronique avec AWS	29 mai 2025
Comment utiliser AWS Transfer Family et GuardDuty pour se protéger contre les malwares	30 avril 2025
Comment FICO modernise les transferts de fichiers grâce à l'automatisation ETL en utilisant AWS Transfer Family	24 avril 2025
Annonce d'applications AWS Transfer Family Web pour des transferts de fichiers Amazon S3 entièrement gérés	1er décembre 2024
Six conseils pour améliorer la sécurité de votre AWS Transfer Family serveur	24 septembre 2024
Simplifiez l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family	12 août 2024
Conception de transferts de fichiers gérés sécurisés et conformes à l'aide de connecteurs AWS Transfer Family SFTP et de chiffrement PGP	16 mai 2024
Utilisation d'Amazon Cognito comme fournisseur d'identité avec Amazon AWS Transfer Family S3	14 mai 2024
Comment Transfer Family peut vous aider à créer une solution de transfert de fichiers géré sécurisée et conforme	3 janvier 2024

Titre et lien de l'article de blog	Date
Détectez les menaces de logiciels malveillants en utilisant AWS Transfer Family	20 juillet 2023
Élargir les charges de travail SAP avec AWS Transfer Family	13 juillet 2023
Chiffrer et déchiffrer des fichiers avec PGP et 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
Sécurisation AWS Transfer Family avec AWS le Web Application Firewall et Amazon API Gateway	5 mai 2021

Titre et lien de l'article de blog	Date
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 des serveurs SFTP	19 février 2020
Migration Lift and Shift des serveurs SFTP vers AWS	12 février 2020
Simplifiez votre structure AWS SFTP 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

Conditions préalables

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 Gestion des identités et des accès AWS un rôle (IAM). Votre rôle doit également établir une relation d'approbation. Cette relation de confiance permet à Transfer Family d'assumer le rôle IAM pour accéder à votre bucket afin de répondre aux demandes de transfert de fichiers de vos utilisateurs.

Pour plus d'informations sur la prise en charge d'IPv6 pour les AWS Transfer Family serveurs, reportez-vous [Support IPv6 pour les serveurs Transfer Family](#) au chapitre Gestion des serveurs.

Rubriques

- [AWS Régions, points de terminaison et quotas pris en charge pour les serveurs Transfer Family](#)
- [Inscrivez-vous pour AWS](#)
- [Configuration du stockage à utiliser avec AWS Transfer Family les serveurs](#)
- [Création d'un rôle et d'une politique IAM](#)

AWS Régions, points de terminaison et quotas pris en charge pour les serveurs Transfer Family

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, représentent le nombre maximal de ressources ou d'opérations de service pour votre Compte AWS. Dans ce guide, vous trouverez les quotas dans [Quotas AS2](#) et [Quotas pour les connecteurs SFTP](#).

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

Pour les applications Web Transfer Family, les régions prises en charge sont répertoriées dans [Régions AWS pour les applications Web Transfer Family](#). Pour les quotas relatifs aux applications Web Transfer Family, voir [Quotas d'applications Web](#).

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. Ouvrir <https://portal.aws.amazon.com/billing/signup>.
2. Suivez les instructions en ligne.

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

Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte 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, 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.

Configuration du stockage à utiliser avec AWS Transfer Family les serveurs

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 fichiers Amazon EFS](#)
 - [Propriété des fichiers Amazon EFS](#)
 - [Configurer les utilisateurs Amazon EFS pour Transfer Family](#)
 - [Configuration des utilisateurs de Transfer Family sur Amazon EFS](#)
 - [Création d'un utilisateur root Amazon EFS](#)
 - [Commandes Amazon EFS 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 à chacun un rôle IAM. 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 Multi-Region d'accès 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 sont 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. Zero-byte des objets 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 Gestion des identités et des accès AWS (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, *amzn-s3-demo-bucket* remplacez-la par le nom de votre compartiment.

Note

Pour corriger le comportement de téléchargement de WinSCP, assurez-vous d'ajouter la "arn:aws:s3:::amzn-s3-demo-bucket/*.*filepart" ligne comme indiqué dans l'exemple de politique suivant. Cette ligne garantit une gestion correcte des objets .filepart afin d'éviter les défaillances.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListing",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
      "Sid": "AllowReadWrite",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ]
    },
    {
      "Sid": "DenyIfNotFolder",
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],

```

```
    "NotResource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*/",
      "arn:aws:s3:::amzn-s3-demo-bucket/*.filepart"
    ]
  }
}
```

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. La solution recommandée pour résoudre ce problème consiste à activer les annuaires optimisés afin de réduire la latence.

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 Amazon 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. Vous définissez cette option dans l'écran Configurer les détails supplémentaires lors de la procédure de création ou de mise à jour du serveur. Ces procédures sont détaillées dans la [Configuration d'un point de terminaison de serveur SFTP, FTPS ou FTP](#) rubrique.

Note

Les clients de l'interface graphique peuvent émettre une `ls` commande indépendante de votre volonté. Il est donc important d'activer ce paramètre si possible.

Si vous n'optimisez pas ou ne pouvez pas optimiser vos répertoires, une autre solution 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.

Enfin, 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 fichiers Amazon EFS

AWS Transfer Family accède à Amazon Elastic File System (Amazon EFS) pour traiter les demandes de transfert de vos utilisateurs. Vous devez donc fournir un système de fichiers Amazon EFS 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 fichiers Amazon EFS, 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 à chacun un rôle IAM. Ce rôle détermine le niveau d'accès dont ils disposent à votre système de fichiers Amazon EFS.
- Pour en savoir plus sur le montage d'un système de fichiers Amazon EFS, consultez [Montage de systèmes de fichiers Amazon EFS](#).

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

Propriété des fichiers Amazon EFS

Amazon EFS utilise le modèle d'autorisation de fichier POSIX (Portable Operating System Interface) 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 fichiers Amazon EFS en utilisant AWS Transfer Family, vous devez lui attribuer un « profil POSIX ». Ce profil est utilisé pour déterminer leur accès aux fichiers et aux répertoires du système de fichiers Amazon EFS.

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

En outre, sur les Unix-style systèmes, les utilisateurs et les groupes sont mappés à des identifiants numériques, qu'Amazon EFS 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 les identifiants numériques mappés pour vérifier les autorisations lorsqu'un utilisateur tente d'accéder à un objet du système de fichiers.

Configurer les utilisateurs Amazon EFS pour Transfer Family

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

- Vous pouvez créer des utilisateurs et configurer leurs dossiers personnels dans Amazon EFS. Consultez [Configuration des 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 root Amazon EFS](#).

 Note

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

Configuration des utilisateurs de Transfer Family sur Amazon EFS

Transfer Family mappe les utilisateurs vers les répertoires UID/GID et que vous spécifiez. S'ils n' UID/GID/directories existent pas déjà dans EFS, vous devez les créer avant de les attribuer dans Transfer to a user. Les détails relatifs à la création d'utilisateurs Amazon EFS sont décrits dans la section [Utilisation des utilisateurs, des groupes et des autorisations au niveau du système de fichiers réseau \(NFS\)](#) du guide de l'utilisateur Amazon Elastic File System.

Étapes pour configurer les utilisateurs Amazon EFS dans Transfer Family

1. Mappez l'UID et le GID EFS de votre utilisateur dans Transfer Family à l'[PosixProfile](#) aide des champs.
2. Si vous souhaitez que l'utilisateur commence dans un dossier spécifique lors de la connexion, vous pouvez spécifier le répertoire EFS 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 la section Utilisation d'[Amazon EFS pour vos applications AWS Lambda sans](#) 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 root Amazon EFS

Si votre organisation vous permet d'activer l'accès des utilisateurs root SFTP/FTPS pour la configuration de vos utilisateurs, vous pouvez créer un utilisateur dont l'UID et le GID sont 0 (utilisateur root), puis utiliser cet utilisateur root pour créer des dossiers et attribuer des propriétaires

d'ID POSIX 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 service Amazon EFS](#), et entrez 0 (zéro) pour l'ID utilisateur et l'ID de groupe.

 Tip

Ne laissez pas ce compte de superutilisateur exister plus longtemps que nécessaire. Ou, si vous conservez le compte utilisateur root, assurez-vous qu'il est bien protégé.

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 rôle et d'une politique IAM

Cette rubrique décrit les types de politiques et de rôles qui peuvent être utilisés avec AWS Transfer Family, et décrit le processus de création d'un rôle utilisateur. Il 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 ARN utilisateur de Transfer Family.
- **Rôle d'accès** — Permet d'accéder uniquement aux fichiers Amazon S3 en cours de transfert. Pour les transferts AS2 entrants, le rôle d'accès utilise l'Amazon Resource Name (ARN) pour l'accord. Pour les transferts AS2 sortants, le rôle d'accès utilise l'ARN du 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 ARN de serveur Transfer Family.
- **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 ARN de serveur Transfer Family. Pour les transferts AS2 sortants, le rôle de journalisation utilise l'ARN du connecteur.
- **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 (ARN) Transfer Family.

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 une Auto-generate politique basée sur le 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 l'utilisateur IAM.

Rubriques

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

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 fichiers Amazon EFS 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 devez créer une politique et un rôle basés sur l'identité Gestion des identités et des accès AWS (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 fichiers Amazon EFS 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 politique IAM pour AWS Transfer Family. Ceci est décrit sous [Pour créer une politique IAM pour AWS Transfer Family](#).
2. Créez un rôle IAM et associez la nouvelle politique IAM. Pour obtenir un exemple, consultez [Exemple de politique read/write d'accès](#).
3. Établissez une relation de confiance entre AWS Transfer Family et le rôle IAM. Ceci est décrit sous [Étape 1 : Établir une relation d'approbation](#).

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

Pour créer une politique IAM pour AWS Transfer Family

1. Ouvrez la console IAM 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 stratégie, choisissez l'onglet JSON.
4. Dans l'éditeur qui apparaît, remplacez le contenu de l'éditeur par la politique IAM que vous souhaitez associer au rôle IAM.

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

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

Créez ensuite un rôle IAM et attachez-lui une nouvelle stratégie IAM.

Pour créer un rôle IAM 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 élaborerez 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 console IAM, 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 l'ARN source est l'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 chacun *user input placeholder* par vos propres informations.

Pour plus de détails sur le problème des députés confus et d'autres exemples, voir [Cross-service prévention confuse des adjoints](#).

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

Vous avez maintenant créé un rôle IAM qui permet d' AWS Transfer Family appeler AWS des services en votre nom. Vous avez associé au rôle la politique IAM 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

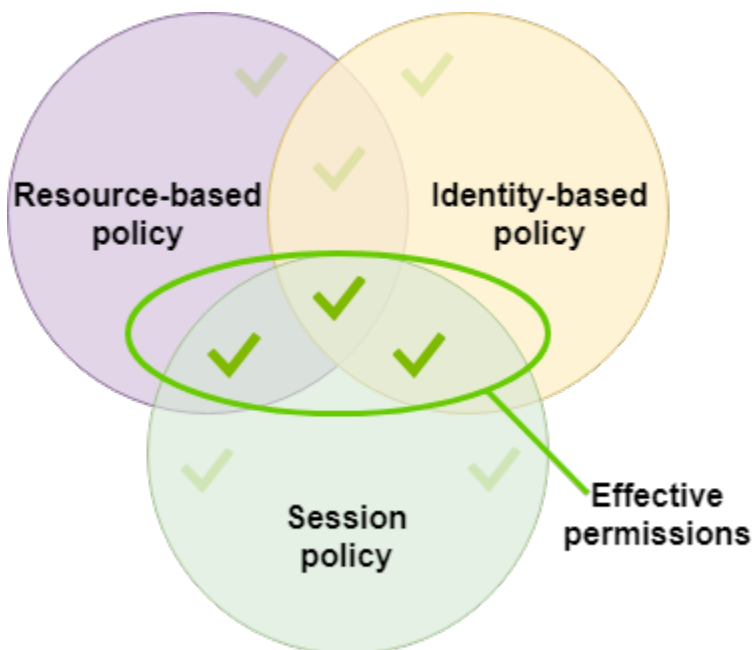
- Pour des informations plus générales sur les rôles IAM, consultez la section [Création d'un rôle pour déléguer des autorisations à un AWS service](#) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur les politiques basées sur l'identité pour les ressources Amazon S3, consultez la section [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 pour les ressources Amazon EFS, consultez la section [Utilisation d'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 [URL](#)

[de console](#), 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 [read/write accès](#), vous pouvez configurer une URL qui limite l'accès des utilisateurs à leur répertoire personnel uniquement.

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 la section [Politiques de session](#) dans le guide de l'utilisateur IAM.

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 Policy](#) pour l'CreateUseraction dans la référence de l'API.

- 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 en savoir plus, consultez [Protection et chiffrement des données](#).
- Pour utiliser les politiques de session afin de créer des autorisations d'accès basées sur les attributs des utilisateurs sans créer de rôles IAM distincts pour chaque utilisateur, voir [Approches dynamiques de gestion des autorisations](#).

```
{
  "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 (ARN) S3 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 `Transfer Family` soit `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` est défini sur `/home`.
- `transfer:HomeFolder` est défini sur `/bob/amazon/stuff/`.
- `transfer:HomeDirectorydevienthome/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 read/write d'accès

Accorder l' read/write accès au compartiment Amazon S3

L'exemple de politique suivant AWS Transfer Family permet d' read/write autoriser l'accès aux objets de votre compartiment Amazon S3.

Notez ce qui suit :

- Remplacez `amzn-s3-demo-bucket` par le nom de votre compartiment Simple Storage Service (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:::amzn-s3-demo-bucket"
    ]
  },
  {
    "Sid": "HomeDirObjectAccess",
    "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:::amzn-s3-demo-bucket/*"
  }
]
}

```

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

Note

Outre la politique, vous devez également vous assurer que les autorisations de vos fichiers POSIX accordent l'accès approprié. Pour plus d'informations, consultez [Working with users, groups, and permissions at the Network File System \(NFS\) Level](#) (Utilisation d'utilisateurs,

de groupes et d'autorisations au niveau NFS (Network File System)) dans le Guide de l'utilisateur Amazon Elastic File System.

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

 Note

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RootFileSystemAccess",
      "Effect": "Allow",
      "Action": [
        "elasticfilesystem:ClientRootAccess",
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
      ],
      "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-
system/file-system-id"
    }
  ]
}
```

L'exemple de politique suivant autorise le système de fichiers utilisateur à accéder aux fichiers de votre système de fichiers Amazon EFS.

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

```
    "Sid": "UserFileSystemAccess",
    "Effect": "Allow",
    "Action": [
        "elasticfilesystem:ClientMount",
        "elasticfilesystem:ClientWrite"
    ],
    "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012: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](#)- Créez un serveur SFTP Transfer Family avec un utilisateur géré par le service et transférez des fichiers à l'aide d'un client.
- [Configuration et utilisation des connecteurs SFTP](#)- Configurez un connecteur SFTP pour transférer des fichiers entre le stockage Amazon S3 et un serveur SFTP.
- [Configuration d'une méthode Amazon API Gateway en tant que fournisseur d'identité personnalisé](#)- Configurez une méthode Amazon API Gateway en tant que fournisseur d'identité personnalisé pour le téléchargement de fichiers sur un AWS Transfer Family serveur.
- [Configuration d'un flux de travail géré pour le déchiffrement d'un fichier](#)- Créez un flux de travail géré pour déchiffrer des fichiers, charger des fichiers chiffrés sur Amazon S3 et afficher le contenu déchiffré.
- [Configuration d'une configuration AS2](#)- Configurez un serveur AS2 Transfer Family, y compris l'importation de certificats, la création de profils et d'accords, la configuration du connecteur AS2 en option et les tests.
- Les didacticiels suivants vous guident dans la création et la configuration des applications Web Transfer Family. Choisissez le didacticiel qui correspond le mieux à vos besoins :

[Tutoriel : Configuration d'une application Web Transfer Family de base](#)- Découvrez comment créer et configurer une application Web Transfer Family.

[Tutoriel : Configuration d'une application AWS Transfer Family Web avec un accès sélectif à plusieurs compartiments](#)- Configurez une application Web Transfer Family avec des autorisations granulaires sur le bucket Amazon S3 pour un seul utilisateur.

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 connecteurs SFTP](#)
- [Configuration d'une méthode Amazon API Gateway en tant que fournisseur d'identité personnalisé](#)

- [Configuration d'une configuration AS2](#)
- [Tutoriel : Configuration d'une application Web Transfer Family de base](#)
- [Tutoriel : Configuration d'une application AWS Transfer Family Web avec un accès sélectif à plusieurs compartiments](#)

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

Utilisez ce tutoriel pour commencer à utiliser AWS Transfer Family (Transfer Family). Vous apprendrez à créer un SFTP-enabled serveur 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

- [Conditions préalables](#)
- [Étape 1 : connectez-vous à la AWS Transfer Family console](#)
- [Étape 2 : Création d'un SFTP-enabled serveur](#)
- [Étape 3 : Ajouter un utilisateur géré par le service](#)
- [Étape 4 : Transférer un fichier à l'aide d'un client](#)

Conditions préalables

Avant de commencer, assurez-vous de remplir les conditions requises dans [Conditions préalables](#). Dans le cadre de cette configuration, vous créez un bucket Amazon Simple Storage Service (Amazon S3) et Gestion des identités et des accès AWS un rôle d'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, AmazonS3FullAccess accorde AWS l'autorisation de configurer et d'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` accorde à votre utilisateur SFTP l'autorisation de créer des ressources Transfer Family.
- `IAMFullAccess` (ou plus précisément une politique autorisant la création de rôles IAM) 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 serveurs VPC, vous devez ajouter les actions `ec2:CreateVpcEndpoint` et `ec2:DeleteVpcEndpoints` à votre politique. Pour plus d'informations sur la limitation de l'accès aux points de terminaison VPC pour des raisons de sécurité, consultez [Limiter l'accès aux points de terminaison VPC pour les serveurs Transfer Family](#)

Note

Les `IAMFullAccess` politiques `AmazonS3FullAccess` ne sont en elles-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 : connectez-vous à la AWS Transfer Family console

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 d'utilisateur IAM, entrez le nom du rôle utilisateur que vous avez créé pour Transfer Family.
4. Dans le champ Mot de passe, saisissez le mot de passe de votre AWS compte.
5. Choisissez Sign in (Connexion).

Étape 2 : Création d'un SFTP-enabled serveur

Le protocole de transfert de fichiers (SFTP) Secure Shell (SSH) 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-enabled serveur

1. Sélectionnez Serveurs dans le volet de navigation, puis choisissez Créer un serveur.
2. Dans Choisir les protocoles, sélectionnez SFTP, puis Next.
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, pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur. Notre dernière politique de sécurité est celle par défaut : pour plus de détails, voir [Politiques de sécurité pour AWS Transfer Family serveurs](#).

Note

Choisissez Créer un nouveau rôle pour la CloudWatchjournalisation uniquement si vous ajoutez un flux de travail géré pour votre serveur. Pour consigner les événements du serveur, il n'est pas nécessaire de créer un rôle IAM.

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. Pour plus de détails sur la création d'utilisateurs, consultez [Gestion des utilisateurs pour les points de terminaison du serveur](#).

Étape 3 : Ajouter un utilisateur géré par le service

Pour ajouter un utilisateur au SFTP-enabled serveur

1. Sur la page Serveurs, sélectionnez le 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, 0—9 A-Z, trait de soulignement « _ », tiret « - », point « . » et le signe « @ ». Le nom d'utilisateur ne peut pas commencer par un tiret « - », un point « . » ou par le signe « @ ».
4. Pour Access, choisissez le rôle IAM que vous avez créé dans [Création d'un rôle et d'une politique IAM](#). Ce rôle IAM inclut une politique IAM qui contient les autorisations d'accès à votre compartiment Amazon S3, ainsi qu'une relation de confiance avec le AWS Transfer Family service. La procédure décrite dans le présent document [Étape 1 : Établir une relation d'approbation](#) montre comment établir une relation de confiance appropriée.
5. Pour Politique, choisissez Aucune.
6. Pour le répertoire personnel, choisissez le compartiment Amazon S3 dans lequel vous souhaitez stocker les données que vous transférez à l'aide desquelles vous souhaitez stocker AWS Transfer Family. Entrez le chemin d'accès au home répertoire. Il s'agit du répertoire que voient vos utilisateurs lorsqu'ils se connectent à l'aide de leur client.

Nous vous recommandons d'utiliser un chemin de répertoire contenant le nom d'utilisateur afin d'avoir la possibilité d'utiliser une politique de session. Une politique de session limite l'accès d'un utilisateur au home répertoire de cet utilisateur dans le compartiment Amazon S3. Pour plus d'informations sur l'utilisation des politiques de session, consultez [Comment fonctionnent les politiques de session](#).

Si vous préférez, vous pouvez laisser ce paramètre vide pour utiliser le root répertoire de votre compartiment Amazon S3. Si vous choisissez cette option, assurez-vous que votre rôle IAM donne accès à l'root annuaire.

7. Cochez la case Restreint pour empêcher vos utilisateurs d'accéder à tout ce qui se trouve en dehors de leur home répertoire. Cela empêche également les utilisateurs de voir le nom du compartiment ou du dossier Amazon S3.

8. Pour la clé publique SSH, entrez la partie clé SSH publique de la paire de clés SSH au format.
`ssh-rsa <string>`

Votre clé doit être validée par le service avant que vous puissiez ajouter votre nouvel utilisateur. Pour plus d'informations sur la façon de générer une paire de clés SSH, consultez [Génération de clés SSH 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 d'OpenSSH.

Rubriques

- [Utilisez Cyberduck](#)
- [Utiliser OpenSSH](#)

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 (SSH File 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 les détails des serveurs SFTP, FTPS et FTP](#).
5. Dans le champ Numéro de port, entrez **22** 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 la clé privée SSH, choisissez ou entrez la clé privée SSH.
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 OpenSSH

Suivez les instructions ci-dessous pour transférer des fichiers depuis la ligne de commande en utilisant OpenSSH.

Note

Ce client fonctionne uniquement avec un SFTP-enabled serveur.

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

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 privée SSH. `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 /amzn-s3-demo-bucket/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 /amzn-s3-demo-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 montre 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 simplement déchiffrer des fichiers sans écrire de code à l'aide des flux de travail Transfer Family Managed, [crypter et déchiffrer des fichiers avec](#) PGP et 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 clés PGP](#)
- [Étape 5 : Stocker la clé privée PGP 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 Gestion des identités et des accès AWS (IAM) que Transfer Family peut utiliser pour lancer un flux de travail. Le processus de création d'un rôle d'exécution est décrit dans [Politiques IAM pour les 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 démarrer le flux de travail que vous créez dans ce didacticiel. Pour utiliser cet exemple de politique, remplacez *user input placeholders* par vos propres informations. amzn-s3-demo-bucket Remplacez-le par le nom du compartiment Amazon S3 dans lequel vous chargez vos fichiers chiffrés.

Note

Tous les flux de travail ne nécessitent pas toutes les autorisations répertoriées dans cet exemple. Vous pouvez restreindre 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 [Autorisations IAM 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:::amzn-s3-demo-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
},
{
    "Sid": "DecryptSecret",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-east-1:123456789012: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 détails suivants :
 - 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 `amzn-s3-demo-bucket` dans la politique IAM 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 l'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 capable d'accéder au serveur par SFTP et de 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 protocole SFTP.
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 le flux de travail 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 rôle IAM 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 clés PGP 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 vers le bas 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 **amzn-s3-demo-bucket**.

- Pour les clés publiques SSH, collez une clé publique correspondant à une clé privée que vous possédez. Pour en savoir plus, consultez [Génération de clés SSH 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 clés PGP

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

Pour générer une paire de clés PGP

1. Pour ce didacticiel, vous pouvez utiliser le client gpg (GnuPG) version 2.0.22 pour générer une paire de clés PGP qui utilise 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. Si vous choisissez ECC, vous pouvez choisir entre NIST BrainPool et Curve25519 pour la courbe elliptique.

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 : Stocker la clé privée PGP 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 la section [AWS Secrets Manager Tarification](#).

Pour stocker une clé privée PGP 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 panneau 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 des Key/value paires, choisissez l'Key/valueonglet.
 - 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 des Key/value paires, sélectionnez l'Key/valueonglet.
 - Clé — Entrée**PGPPassphrase**.
 - valeur — Entrez le mot de passe que vous avez utilisé lorsque vous avez généré votre paire de clés PGP. [Étape 4 : Création d'une paire de clés PGP](#)
7. Choisissez Suivant.

8. Sur la page Configurer le secret, entrez le nom et la description de votre secret. Vous pouvez créer un secret pour un utilisateur spécifique ou un secret utilisable par tous les utilisateurs. Si l'ID de votre serveur est le même **s-1111222233344445**, nommez le secret comme suit.
 - Pour créer un secret par défaut pour tous les utilisateurs, nommez-le **aws/transfer/s-1111222233344445/@pgp-default**.
 - Pour créer un secret uniquement pour l'utilisateur que vous avez créé précédemment, nommez-le **aws/transfer/s-1111222233344445/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 privée PGP à Secrets Manager, voir [Utiliser AWS Secrets Manager pour stocker votre clé PGP](#).

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'-r argument, remplacez-le **marymajor@example.com** par l'adresse e-mail que vous avez utilisée lors de la création de la paire de clés PGP.
- Le --openpgp drapeau est facultatif. Ce drapeau rend le fichier crypté conforme à la norme [OpenPGP RFC4880](#).
- Cette commande crée un fichier nommé **testfile.txt.gpg** au même emplacement que **testfile.txt**.

Important

Lorsque vous chiffrez des fichiers destinés à être utilisés avec AWS Transfer Family des flux de travail, assurez-vous toujours de spécifier un destinataire non anonyme à l'aide du -r paramètre. Le chiffrement anonyme (sans indication de destinataire) peut entraîner

des échecs de déchiffrement dans le flux de travail, car le système ne sera pas en mesure d'identifier la clé à utiliser pour le déchiffrement. Les informations de débogage relatives à ce problème sont disponibles à l'adresse [Résoudre les problèmes de chiffrement des destinataires anonymes](#).

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 privée SSH 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: /amzn-s3-demo-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
```

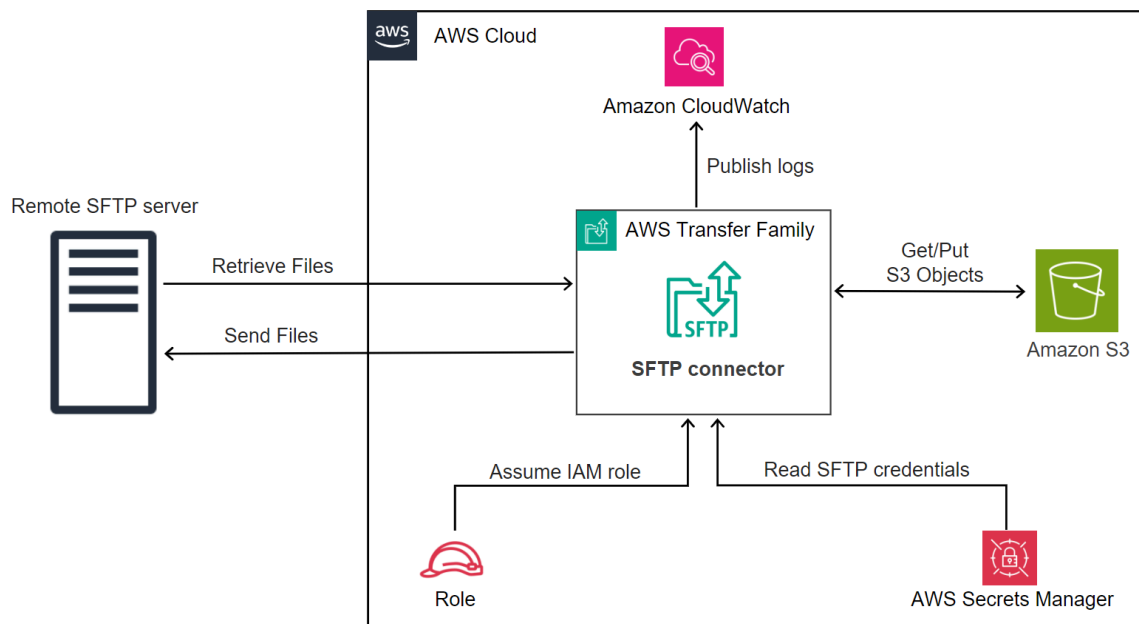
En cas de succès, la `ls` commande répertorie le `testfile.txt` fichier. Vous pouvez télécharger ce fichier et vérifier qu'il est identique au fichier d'origine que vous avez chiffré précédemment.

Configuration et utilisation des connecteurs SFTP

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

Ce didacticiel explique comment configurer un connecteur SFTP avec des types de sortie gérés par le service et VPC_LATTICE, puis transférer des fichiers entre le stockage Amazon S3 et un serveur SFTP.

Un connecteur SFTP récupère les informations d'identification SFTP AWS Secrets Manager pour s'authentifier sur un serveur SFTP distant et établir une connexion. Le connecteur envoie des fichiers au serveur distant ou en extrait des fichiers, puis les stocke dans Amazon S3. Vous pouvez choisir entre une sortie gérée par service (à l'aide d'une infrastructure AWS gérée) ou une sortie VPC (routage via votre Cross-VPC VPC à l'aide de l'accès aux ressources). Un rôle IAM 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.



Le billet de blog suivant fournit une architecture de référence pour créer un flux de travail MFT à l'aide de connecteurs SFTP, y compris le chiffrement de fichiers à l'aide de PGP avant de les envoyer à un serveur SFTP distant à l'aide de connecteurs SFTP : [Architecture de transferts de fichiers gérés sécurisés et conformes avec AWS Transfer Family les connecteurs SFTP et le chiffrement PGP](#).

Types de sorties de connecteurs

Les connecteurs SFTP prennent en charge deux types de sortie qui déterminent la manière dont votre connecteur achemine le trafic vers les serveurs SFTP distants :

- **SERVICE_MANAGED** (par défaut) : utilise l'infrastructure gérée par AWS Transfer Family avec des adresses IP statiques pour les connexions sortantes.
- **VPC** : achemine le trafic via votre VPC à l'aide de l'accès aux Cross-VPC ressources, permettant ainsi la connectivité des points de terminaison privés et l'utilisation de vos propres passerelles NAT.

Ce didacticiel couvre les deux types de sortie. Choisissez le type de sortie VPC lorsque vous devez :

- Connectez-vous à des serveurs SFTP privés dans votre VPC (adresses IP privées)
- Connectez-vous à des serveurs SFTP sur site via Direct Connect ou VPN
- Acheminez le trafic des points de terminaison publics via votre VPC pour les contrôles de sécurité
- Utilisez vos propres adresses IP élastiques pour les connexions sortantes

Rubriques

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

Étape 1 : créer les ressources de soutien nécessaires

Vous pouvez utiliser des connecteurs SFTP pour copier des fichiers entre Amazon S3 et n'importe quel serveur SFTP distant. Pour ce didacticiel, nous utilisons un AWS Transfer Family serveur comme serveur SFTP 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 serveur SFTP distant :. [Création de compartiments Amazon S3](#)
- Créez un Gestion des identités et des accès AWS rôle pour accéder au stockage Amazon S3 et à notre secret dans Secrets Manager :[Créez un rôle IAM avec les autorisations nécessaires](#).
- Créez un serveur Transfer Family qui utilise le protocole SFTP et un utilisateur géré par le service qui utilise le connecteur SFTP pour transférer des fichiers vers ou depuis le serveur SFTP :. [Création d'un serveur SFTP Transfer Family et d'un utilisateur](#)
- Créez un AWS Secrets Manager secret qui stocke les informations d'identification utilisées par le connecteur SFTP pour se connecter au serveur SFTP distant :. [Créez et stockez un secret dans AWS Secrets Manager](#)

Pour les connecteurs de type sortie VPC, vous avez également besoin de :

- Un VPC doté de sous-réseaux et de groupes de sécurité appropriés
- Une passerelle de ressources (minimum 2 zones de disponibilité requises) :[Création d'une passerelle de ressources \(type de sortie VPC uniquement\)](#).
- Une configuration de ressources pointant vers votre serveur SFTP :[Création d'une configuration de ressource \(type de sortie VPC uniquement\)](#). Pour plus d'informations, consultez [Configurations de ressources](#) dans le Guide de l'utilisateur Amazon VPC Lattice.

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 rôle IAM avec les autorisations nécessaires

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
```

```

        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
}
]
}

```

Remplacez les éléments comme suit :

- Caramzn-s3-demo-bucket, le didacticiel utilise **sftp-server-storage-east**.
- Car *region*, le didacticiel utilise **us-east-1**.
- Pour *account-id*, utilisez votre Compte AWS identifiant.
- Car *SecretName-6RandomCharacters* nous sommes là **using sftp-connector1** 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 pour stocker les informations d'identification utilisateur de votre connecteur SFTP. Vous pouvez utiliser un mot de passe, une clé privée SSH 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 la section [AWS Secrets Manager Tarification](#).

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 serveur SFTP distant. Pour notre tutoriel, la clé privée doit correspondre à la clé publique qui est stockée pour notre utilisateur de test sur le serveur SFTP 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 de l'utilisateur dans Secrets Manager pour un connecteur SFTP

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 panneau 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 des Key/value paires, choisissez l'onglet Key/value.

- 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.

Création d'une passerelle de ressources (type de sortie VPC uniquement)

Pour les connecteurs de type sortie VPC, vous devez créer une passerelle de ressources dans votre VPC. La passerelle de ressources sert de point d'entrée pour l'accès aux Cross-VPC ressources.

Pour créer une passerelle de ressources

1. Exécutez la commande suivante pour créer une passerelle de ressources (remplacez l'ID VPC et les ID de sous-réseau par vos valeurs) :

```
aws vpc-lattice create-resource-gateway \  
  --name my-sftp-resource-gateway \  
  --vpc-identifier vpc-12345678 \  
  --subnet-ids subnet-12345678 subnet-87654321
```

Note

Les passerelles de ressources nécessitent des sous-réseaux dans au moins 2 zones de disponibilité.

2. Notez l'ID de passerelle de ressources indiqué dans la réponse à utiliser à l'étape suivante.

Création d'une configuration de ressource (type de sortie VPC uniquement)

Créez une configuration de ressources qui pointe vers votre serveur SFTP. Il peut s'agir d'une adresse IP privée pour les serveurs de votre VPC ou d'un nom DNS public pour les serveurs externes. Pour plus d'informations sur les configurations des ressources, consultez la section [Configurations des ressources](#) dans le guide de l'utilisateur Amazon VPC Lattice.

Pour créer une configuration de ressources

1. Pour un serveur SFTP privé, exécutez :

```
aws vpc-lattice create-resource-configuration \  
  --name my-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"}
```

2. Pour un serveur SFTP public (nom DNS uniquement), exécutez :

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-sftp-resource-config \  
  --port-ranges 22 \  
  --type SINGLE \  
  --resource-gateway-identifier rgw-12345678 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"}
```

 Note

Les points de terminaison publics doivent utiliser des noms DNS et non des adresses IP.

3. Notez l'ARN de configuration des ressources indiqué dans la réponse à utiliser lors de la création du connecteur.

Étape 2 : Création et test d'un connecteur SFTP

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

Pour créer un connecteur SFTP

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 SFTP Connectors, puis Create SFTP connector.
3. Pour le type de sortie, choisissez l'une des options suivantes :
 - Service géré (par défaut) : utilise l'infrastructure gérée par AWS Transfer Family avec des adresses IP statiques pour les connexions sortantes.
 - Réseau VPC : achemine le trafic via votre VPC à l'aide de l'accès aux ressources. Cross-VPC Choisissez cette option pour la connectivité des terminaux privés ou pour utiliser vos propres passerelles NAT.

 Important

Vous ne pouvez pas modifier le type de sortie après avoir créé le connecteur. Choisissez avec soin en fonction de vos besoins en matière de connectivité.

4. Dans la section Configuration du connecteur, fournissez les informations suivantes :

- Pour l'URL, entrez l'URL du serveur SFTP distant. Pour le didacticiel, nous saisissons l'URL du serveur Transfer Family que nous utilisons comme serveur SFTP distant.

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

1111aaaa2222bbbb3 Remplacez-le par votre identifiant de serveur Transfer Family.

- Pour le rôle Access, entrez le rôle que nous avons créé précédemment, **sftp-connector-role**.
- Pour l'ARN de configuration des ressources (type de sortie VPC Lattice uniquement), entrez l'ARN de la configuration des ressources que vous avez créée précédemment :

```
arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678
```

- Pour le rôle Logging, choisissez un rôle qui inclut une politique de confiance `transfer.amazonaws.com` dans l'élément Principal.

Conseil : Outre l'ajout de Transfer Family en tant qu'entité de confiance, vous pouvez ajouter la politique `AWSTransferLoggingAccess` AWS gérée au rôle. Cette politique est décrite en détail dans [AWSTransferLoggingAccess](#).

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

▼

↻

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

▼

↻

5. Dans la section Configuration SFTP, fournissez les informations suivantes :

- Pour les informations d'identification du connecteur, choisissez le nom de votre ressource Secrets Manager qui contient les informations d'identification SFTP. 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 lançant `ssh-keyscan` votre commande sur votre serveur SFTP. Pour plus de détails sur le formatage et le stockage de la clé d'hôte fiable, consultez la documentation sur les types de [SftpConnectorConfig](#) données.
- Pour le nombre maximal de connexions simultanées, sélectionnez une valeur entière comprise entre 1 et 5 : la valeur par défaut est 5.

SFTP configuration [Info](#)**Connector credentials** [Info](#)

Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

aws/transfer/sftp-connector1 ▼



[Store a new secret](#)

Trusted host keys - optional [Info](#)

Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

ssh-rsa AAAAE

[Remove](#)

[Add trusted host key](#)

Maximum concurrent connections [Info](#)

Select the maximum number of concurrent connections that your connector can create to the remote server

5 ▼

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

Vous pouvez également créer des connecteurs à l'aide du AWS Command Line Interface.

- Pour créer un connecteur SFTP avec une sortie gérée par service, exécutez la commande suivante :

```
aws transfer create-connector \
  --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-
rsa AAAAB3NzaC..."
```

- Pour créer un connecteur SFTP avec VPC-based sortie, exécutez la commande suivante :

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
  --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa
AAAAB3NzaC..." \
```

```
--egress-config VpcLattice={ResourceConfigurationArn="arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678",PortNumber=22}
```

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

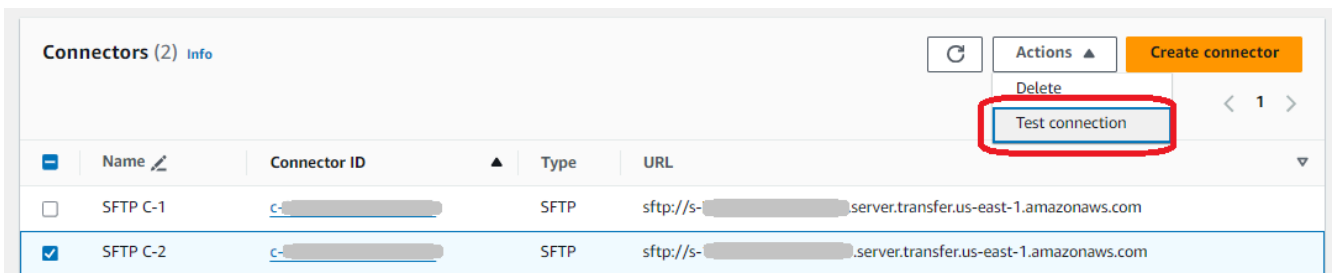
Note

Pour les connecteurs de type sortie VPC, la résolution DNS peut prendre plusieurs minutes après la création. Pendant ce temps, l'état du connecteur sera PENDING et TestConnection retournera « Connecteur non disponible ». Attendez que le statut change ACTIVE avant de tenter de transférer des fichiers.

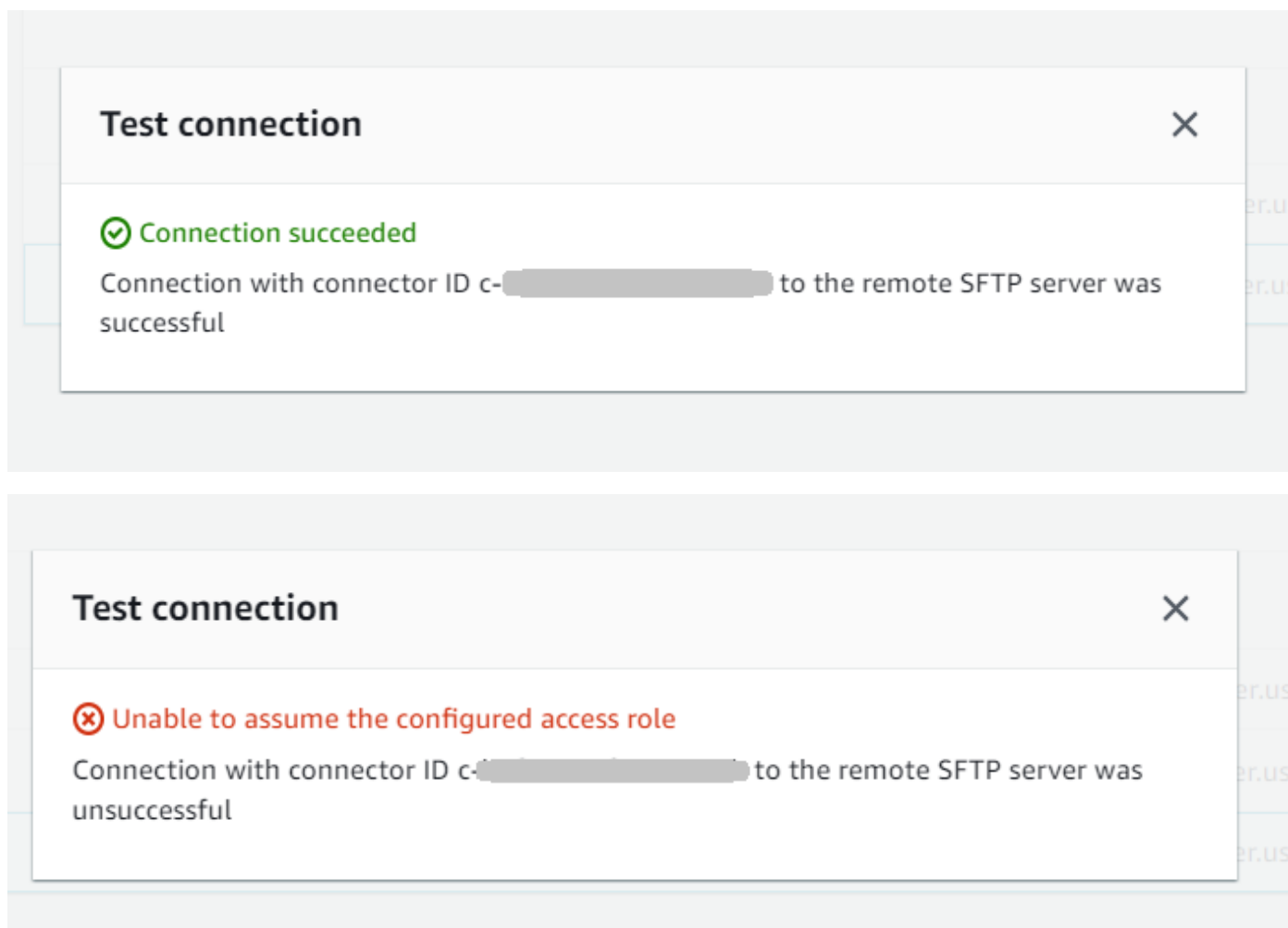
Test a connector using the console

Pour tester un connecteur SFTP

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 SFTP 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 de AWS Command Line Interface, exécutez la commande suivante à l'invite de commande (*connector-id* remplacez-la par votre identifiant de connecteur réel) :

```
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"
}
```

Lorsque vous décrivez un connecteur de type sortie VPC, la réponse inclut les nouveaux champs :

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::219573224423:role/sftp-connector-role",
    "Arn": "arn:aws:transfer:us-east-1:219573224423:connector/c-5dfa309ccabf40759",
    "ConnectorId": "c-5dfa309ccabf40759",
    "Status": "ACTIVE",
    "EgressConfig": {
      "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-east-1:025066256552:resourceconfiguration/rcfg-079259b27a357a190"
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/sftp-connector1"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}
```

Notez que cela `ServiceManagedEgressIpAddresses` est nul pour les connecteurs de type sortie VPC, car le trafic passe par votre VPC plutôt que par l'infrastructure gérée. AWS

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

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 serveur SFTP n'utilise pas le stockage Amazon S3, vous pouvez remplacer le chemin par `sftp-server-storage-east` un chemin d'accès aux

emplacements de fichiers accessibles depuis votre serveur SFTP, quel que soit l'endroit indiqué dans les commandes suivantes.

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

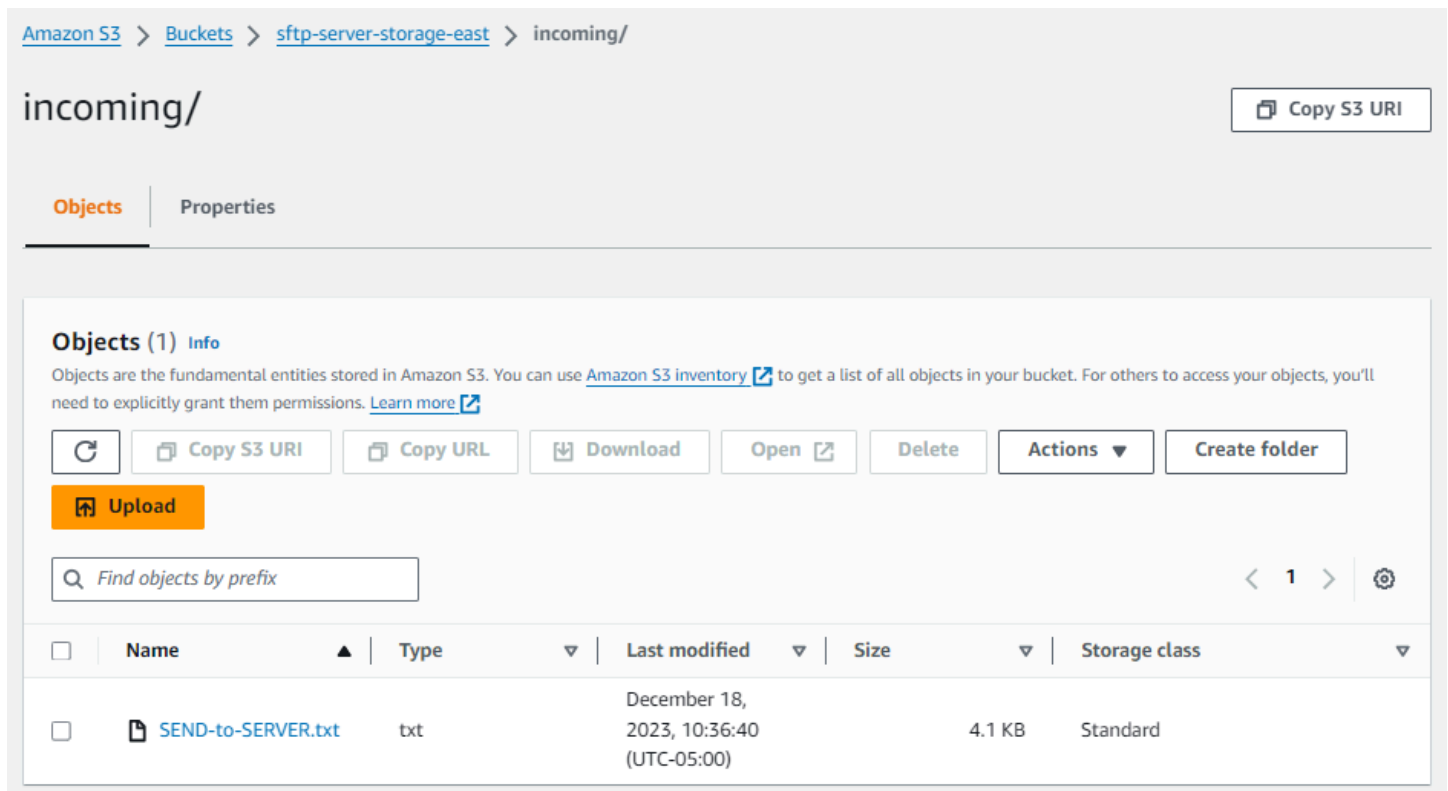
 Note

Dans les commandes suivantes, remplacez par *connector-id* l'ID de votre connecteur.

Tout d'abord, nous envoyons un fichier depuis notre compartiment Amazon S3 vers le serveur SFTP 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 "/  
sftp-server-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.



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": "/sftp-server-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": "account-id",
"connector-arn": "arn:aws:transfer:us-east-1:account-id: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 indiquant le problème. Les causes courantes d'erreurs sont les problèmes liés aux autorisations IAM et les chemins de fichiers incorrects.

Ensuite, nous récupérons un fichier du serveur SFTP 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 "/sftp-server-
storage-east/incoming"

```

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

The screenshot shows the Amazon S3 console interface. The breadcrumb navigation at the top indicates the path: [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' tab shows a list of objects with the following details:

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

At the top of the object list, there are several action buttons: Refresh, Copy S3 URI, Copy URL, Download, Open, Delete, Actions (dropdown), and Create folder. There is also an 'Upload' button and a search bar labeled 'Find objects by prefix'.

En cas de réussite, l'entrée du journal se présente comme 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": "account-id",
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/c-connector-id",
  "local-directory-path": "/sftp-server-storage-east/incoming"
}
```

Résolution des problèmes liés aux connecteurs de sortie VPC

Si vous rencontrez des problèmes avec les connecteurs de sortie VPC, vérifiez les points suivants :

- L'état du connecteur est EN ATTENTE : la résolution DNS des connecteurs VPC peut prendre plusieurs minutes. Attendez que le statut devienne ACTIF avant de tenter de vous connecter.
- Délais de connexion : vérifiez que les groupes de sécurité autorisent le trafic sur le port 22 entre vos sous-réseaux Resource Gateway et le serveur SFTP cible.
- Erreurs de configuration des ressources : assurez-vous que votre configuration des ressources pointe vers la bonne adresse IP ou le bon nom DNS, et que la passerelle de ressources se trouve dans le même VPC que votre serveur SFTP (pour les points de terminaison privés). Pour plus d'informations, consultez [Configurations de ressources](#) dans le Guide de l'utilisateur Amazon VPC Lattice.
- Problèmes liés aux points de terminaison publics : pour les points de terminaison publics, assurez-vous d'utiliser un nom DNS, et non une adresse IP, dans la configuration de vos ressources. Vérifiez que votre VPC dispose d'une passerelle NAT pour l'accès Internet sortant.
- Disponibilité AZ : les passerelles de ressources nécessitent des sous-réseaux dans au moins 2 zones de disponibilité. Les AZ ne sont pas toutes compatibles avec le VPC Lattice. Vérifiez les AZ compatibles dans votre région.

Considérations financières relatives au type de sortie VPC :

- VPC Lattice facture 0\$. 006/GB pour le traitement des données en tant que fournisseur de ressources (facturé directement par VPC Lattice)
- AWS Transfer Family absorbe les 0\$. 01/GB coûts de consommation des ressources (1 premier PB)
- Pour les points de terminaison publics via VPC, des frais supplémentaires de passerelle NAT et de transfert de données peuvent s'appliquer
- Aucun frais Transfer Family supplémentaire au-delà du montant standard de 0\$. 40/GB frais de traitement des données

Procédures pour créer un serveur Transfer Family à utiliser comme serveur SFTP distant

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

- Nous utilisons un serveur Transfer Family pour représenter un serveur SFTP distant. Les utilisateurs classiques d'un connecteur SFTP disposent de leur propre serveur SFTP distant. Consultez [Création d'un serveur SFTP Transfer Family et d'un utilisateur](#).
- Comme nous utilisons un serveur Transfer Family, nous utilisons également un utilisateur SFTP géré par service. 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 connecteur SFTP ont un utilisateur SFTP distinct qui n'est pas associé à un serveur Transfer Family. Consultez [Création d'un serveur SFTP Transfer Family et d'un utilisateur](#).
- Dans le cadre du didacticiel, étant donné que nous utilisons le stockage Amazon S3 pour notre serveur SFTP distant, nous devons créer un deuxième compartiment afin de pouvoir transférer des fichiers d'un compartiment à un autre. **sftp-server-storage-east**

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

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

Suivez la procédure décrite dans [Création d'un SFTP-enabled serveur](#) 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 rôle IAM pour notre utilisateur SFTP et pour accéder au connecteur SFTP. 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 connecteur SFTP](#) 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 utilisateur SFTP 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:::sftp-server-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:::sftp-server-storage-east/*"
        ]
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-east-1:111122223333: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

- [Conditions préalables](#)
- [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 connexion SFTP et le transfert de fichiers](#)
- [Étape 6 : Limiter l'accès au bucket](#)
- [Mettre à jour Lambda si vous utilisez Amazon EFS](#)

Conditions préalables

Avant de créer les ressources Transfer Family dans 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 fichiers Amazon EFS, consultez [Configuration d'un système de fichiers Amazon EFS](#).
2. Pour créer un rôle d'utilisateur, voir [Création d'un rôle et d'une politique IAM](#)

Vous entrez les détails de votre espace de stockage et de votre rôle d'utilisateur lorsque vous créez votre 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 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, choisissez Choisir un modèle existant.
4. Copiez ce lien, [modèle de pile de base](#), et collez-le dans le champ URL d'Amazon S3.
5. Cliquez sur 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 fichiers Amazon EFS) que vous avez créé précédemment.
 - Remplacez le rôle UserRoleArnp par défaut par le rôle utilisateur que vous avez créé précédemment. Le rôle Gestion des identités et des accès AWS (IAM) doit disposer des autorisations appropriées. Pour un exemple de rôle IAM et de politique de compartiment, 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 UserPublicKey1 champ. La première fois que vous vous connectez au serveur via 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 Fonctionnalités, vous devez reconnaître que des ressources IAM CloudFormation peuvent être créées.

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 requêtes HTTP et HTTPS qui sont transmises à Amazon API Gateway. Pour en savoir plus, consultez [Ajouter un pare-feu pour applications Web](#).

Ne pas activer la mise en cache d'API Gateway

N'activez pas la mise en cache pour votre méthode API Gateway lorsque vous l'utilisez comme fournisseur d'identité personnalisé pour Transfer Family. La mise en cache est inappropriée et non valide pour les demandes d'authentification pour les raisons suivantes :

- Chaque demande d'authentification est unique et nécessite une réponse en direct, et non une réponse en cache
- La mise en cache n'apporte aucun avantage puisque Transfer Family n'envoie jamais de demandes dupliquées ou répétées à l'API Gateway.
- L'activation de la mise en cache entraînera la réponse de l'API Gateway avec des données incompatibles, ce qui se traduira par des réponses non valides aux demandes d'authentification

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 l'API du modèle de base Transfer Custom Identity Provider générée par le CloudFormation modèle.
3. Dans le volet Ressources, choisissez GET, puis Method Request.
4. Pour Actions, choisissez Deploy 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'adresse URL 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 CloudFormation pile, un serveur Transfer Family est automatiquement créé.

Pour consulter les détails de votre serveur Transfer Family

1. Ouvrez la 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	

L'ARN du serveur est affiché dans la colonne Physical ID de la TransferServer ligne. L'ID du serveur est contenu dans l'ARN, 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 TransferServer ressource dans 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 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 réponse `StatusCode: 200` HTML et un objet JSON 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 connexion SFTP et le transfert de fichiers

Pour tester la connexion SFTP

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 CloudFormation pile :

- `CreateServer`: `true`
- `UserHomeDirectory`: `/amzn-s3-demo-bucket1`
- `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

UserPublicKey1Il s'agit d'une clé publique que vous avez générée dans le cadre d'une paire de public/private clés.

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:::amzn-s3-demo-bucket1"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectAcl",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}
```

Pour vous connecter au serveur via 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 la 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: /amzn-s3-demo-bucket1
```

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

```
sftp> pwd  
Remote working directory: /amzn-s3-demo-bucket1  
sftp> cd ..  
sftp> ls  
Couldn't read directory: Permission denied
```

Mettre 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 ***stack-name***- GetUserConfigLambda - ***lambda-identifiant***, où ***stack-name*** est le nom de la CloudFormation pile et ***lambda-identifiant*** 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 ***uid-value*** et ***gid-value*** sont des nombres entiers, égaux ou supérieurs 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 configuration AS2

Ce didacticiel explique comment configurer une configuration d'Applicability Statement 2 (AS2) avec AWS Transfer Family. Après avoir effectué les étapes décrites ici, vous disposerez d'un AS2-enabled serveur prêt à accepter les messages AS2 provenant d'un exemple de partenaire commercial. Vous disposerez également d'un connecteur qui pourra être utilisé pour envoyer des messages AS2 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. Importez les certificats que vous avez créés à l'étape 1.

Ce processus est décrit dans [Étape 2 : Importer des certificats en tant que ressources de certificats Transfer Family](#).

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

Ce processus est décrit dans [Étape 3 : Créez des profils pour vous et votre partenaire commercial](#).

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

Ce processus est décrit dans [Étape 4 : Création d'un serveur Transfer Family utilisant le protocole AS2](#).

 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.

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 fichiers AS2.

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

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

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

Étape 1 : créer des certificats pour AS2

Les deux parties d'un échange AS2 ont besoin de X.509 certificats. Vous pouvez créer ces certificats comme bon vous semble. Cette rubrique décrit comment utiliser [OpenSSL](#) 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 clé pour les certificats AS2 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 une interface graphique, [Porteclec](#) 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 (CA).

1. Exécutez la commande suivante pour générer une clé privée RSA 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.

	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, tels que LLC, 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 AS2-enabled serveurs, 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
```

4. Exécutez les commandes suivantes pour créer des demandes de signature de certificat (CSR) que la clé racine doit signer.

```
/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
```

5. 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
```

6. 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 : 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 “Importer des certificats AS2”](#).

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).

Note

Si vous avez un fichier contenant à la fois un certificat et sa chaîne, vous pouvez fournir ce fichier à la `import-certificate` commande en utilisant uniquement le `certificate` paramètre. Par exemple :

```
aws transfer import-certificate --usage ENCRYPTION --certificate
file://combined-cert-and-chain-file.pem
```

Si vous utilisez le `certificate` paramètre pour télécharger à la fois le certificat et sa chaîne, ne l'`certificate-chain` utilisez pas.

Si vous combinez le certificat et sa chaîne, votre clé est formatée selon les normes PEM classiques, qui incluent une nouvelle ligne «\n» tous les 64 caractères. Le certificat stocké est fonctionnellement équivalent à celui que vous avez chargé, à la seule différence que la `DescribeCertificate` réponse via le AWS CLI contiendra ces caractères de nouvelle ligne.

```
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 3 : Créez des profils pour vous et votre partenaire commercial

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

Créez votre profil AS2 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 nom AS2 et les identifiants de certificat de votre partenaire.

```
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* par le nom de votre organisation et *PARTNER-COMPANY* par le nom de l'organisation de votre partenaire commercial.

Étape 4 : Création d'un serveur Transfer Family utilisant le protocole AS2

Cette procédure explique comment créer un AS2-enabled serveur 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 serveur AS2 à l'aide de la console Transfer Family](#).

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

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

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

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

- L'ID de votre VPC (par exemple, `vpc-abcdef01`).
- Les ID de vos sous-réseaux VPC (par exemple, `subnet-abcdef01`, `subnet-subnet-abcdef01`, `subnet-021345ab`).
- Un ou plusieurs identifiants des groupes de sécurité qui autorisent le trafic entrant sur le port TCP 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 point de terminaison VPC.
- Si votre partenaire commercial n'est pas connecté à votre VPC via un VPN, vous avez besoin d'une passerelle Internet. Pour plus d'informations, consultez [Connexion à l'Internet à l'aide d'une passerelle Internet](#) dans le Guide de l'utilisateur Amazon VPC.

Pour créer un AS2-enabled serveur

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 point de terminaison VPC 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-abcd012345ccccccc
```

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

Cette `start-server` commande crée automatiquement un enregistrement DNS 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

L'URL complète que vous fournissez à votre partenaire commercial est la suivante :

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

3. Pour vérifier si votre AS2-enabled serveur est accessible, utilisez les commandes suivantes. Assurez-vous que votre serveur est accessible via l'adresse DNS privée de votre point de terminaison VPC 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 le code d'état HTTP 400 (mauvaise demande) car vous n'envoyez pas de message AS2 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.server.transfer.your-region.amazonaws.com:5080
```

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

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

Cette `describe-server` commande renvoie l'ID de votre point de terminaison VPC 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 nom DNS 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-11111aaaaa2222bbbb.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 format JSON 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 Gestion des identités et des accès AWS (IAM) qui fait confiance `transfer.amazonaws.com` à la politique `AWSTransferLoggingAccess` gérée et attachez-la. Pour en savoir plus, consultez [Création d'un rôle et d'une politique IAM](#). Notez le nom de ressource Amazon (ARN) du rôle IAM 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 5 : Créez un accord entre vous et votre partenaire

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

Les accords réunissent les deux profils (local et partenaire), leurs certificats et une configuration de serveur qui autorise les transferts AS2 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 Amazon S3 et un rôle IAM avec read/write accès au compartiment et depuis celui-ci. Les instructions pour créer ce rôle sont les mêmes que pour les protocoles SFTP, FTP et FTPS de Transfer Family et sont disponibles dans. [Création d'un rôle et d'une politique IAM](#)

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

- Le nom du compartiment Amazon S3 (et le préfixe d'objet, s'il est spécifié) pour stocker vos fichiers AS2. Nous vous recommandons de spécifier des répertoires distincts pour les différents types de fichiers.
- L'ARN du rôle IAM avec accès au bucket
- L'identifiant de votre serveur Transfer Family
- Votre identifiant de profil et l'identifiant de profil de votre partenaire

Enregistrez le code suivant dans un fichier, par exemple `agreementDetails.json`. Remplacez chaque *user input placeholder* par vos propres informations.

```
{
  "Description": "ExampleAgreementName",
  "ServerId": "your-server-id",
  "LocalProfileId": "your-profile-id",
  "PartnerProfileId": "your-partner-profile-id",
  "AccessRole": "arn:aws:iam::111111111111:role/TransferAS2AccessRole",
  "Status": "ACTIVE",
  "PreserveFilename": "ENABLED",
  "EnforceMessageSigning": "ENABLED",
  "CustomDirectories": {
    "FailedFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-failed",
    "MdnFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-mdn",
    "PayloadFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-payload",
    "StatusFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-status",
    "TemporaryFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-temp"
  }
}
```

Note

Pour utiliser un répertoire de base unique au lieu de répertoires séparés, supprimez la CustomDirectories ligne et ses lignes de répertoire individuelles du code précédent et utilisez plutôt le paramètre suivant :

"BaseDirectory": "/amzn-s3-demo-destination-bucket/AS2-inbox"

N'utilisez pas à la fois un répertoire de base et des paramètres de répertoire distincts, sinon la commande échouera.

Exécutez ensuite la commande ci-après.

```
aws transfer create-agreement --cli-input-json file://agreementDetails.json
```

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

Vous pouvez utiliser l'opération `StartFileTransfer` API pour envoyer des fichiers stockés dans Amazon S3 au point de terminaison AS2 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 l'URL du serveur AS2 de votre partenaire. 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",
  "PreserveContentType": "FALSE",
  "SigningAlgorithm": "SHA256"
}
```

Note

En effet `EncryptionAlgorithm`, ne spécifiez pas `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 via AS2 à l'aide de Transfer Family

Recevez un fichier de votre partenaire commercial

Si vous avez associé une adresse IP Elastic publique à votre point de terminaison VPC, Transfer Family a automatiquement créé un nom DNS contenant votre adresse IP publique. Le sous-domaine est l'ID de votre AWS Transfer Family serveur (au format `-1234567890abcdef0`). Fournissez l'URL de votre serveur à votre partenaire commercial au 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 point de terminaison VPC, recherchez le nom d'hôte du point de terminaison VPC qui peut accepter les messages AS2 via HTTP POST provenant de vos partenaires commerciaux sur le port 5080. Pour récupérer les détails du point de terminaison VPC, utilisez la commande suivante.

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

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

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

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

Le nom DNS est répertorié dans le `DnsEntries` tableau. Votre partenaire commercial doit se trouver au sein de votre VPC pour accéder à votre point de terminaison VPC (par exemple via AWS PrivateLink un VPN). Fournissez l'URL de votre point de terminaison VPC 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, l'URL suivante présente 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 `/amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.messageId.txt` et `/amzn-s3-demo-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 messages AS2.

Envoyez un fichier à votre partenaire commercial

Vous pouvez utiliser Transfer Family pour envoyer des messages AS2 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 "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-bucket/myfile2.txt"
```

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

```
aws transfer list-connectors
```

La `list-connectors` commande renvoie les ID de connecteur, les URL et les noms de ressources Amazon (ARN) de vos connecteurs.

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 son URL, ses rôles, ses profils, 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 fichiers JSON et MDN. 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 messages AS2 dans vos CloudWatch journaux.

Tutoriel : Configuration d'une application Web Transfer Family de base

Ce didacticiel explique comment configurer une application Web Transfer Family. Les applications Web Transfer Family offrent une interface simple pour transférer des données vers et depuis Amazon S3 via un navigateur Web. Pour obtenir une documentation détaillée sur cette fonctionnalité, consultez [Applications Web Transfer Family](#).

Tutoriel sur les applications Web : prérequis

- Créez une instance de compte ou une instance d'organisation de AWS IAM Identity Center. Pour en savoir plus, consultez [Configurer votre fournisseur d'identité pour les applications Web Transfer Family](#).

Si vous n'utilisez pas IAM Identity Center comme fournisseur d'identité, [Intégrez Okta en tant que fournisseur d'identité pour les applications Web](#) illustre comment utiliser un autre fournisseur d'identité (dans ce cas Okta).

- Vous avez besoin d'un compartiment Amazon S3 pour interagir avec votre application Web Transfer Family. Pour plus d'informations, consultez [Configuration d'un compartiment Amazon S3](#).

Note

Ce didacticiel part du principe que vous utilisez le répertoire IAM Identity Center pour votre fournisseur d'identité. Si ce n'est pas le cas, reportez-vous à ce didacticiel [Configurer votre fournisseur d'identité pour les applications Web Transfer Family](#) avant de poursuivre ce didacticiel.

Une fois le didacticiel terminé, votre utilisateur peut se connecter et interagir avec l'application Web que vous créez.

Étape 1 : créer les ressources de soutien nécessaires

Vous devez ajouter un utilisateur à votre répertoire IAM Identity Center. Vous avez également besoin de deux rôles : un à utiliser comme rôle de porteur d'identité pour votre application Web, et un second à utiliser pour configurer une autorisation d'accès Amazon S3. Pour le didacticiel, nous autorisons les AWS services à créer ces rôles pour nous.

Pour ajouter un utilisateur

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Dans le volet de navigation de gauche, sélectionnez Utilisateurs.
3. Choisissez Ajouter un utilisateur et spécifiez les détails de l'utilisateur.

Spécifiez un nom d'utilisateur, une adresse e-mail et les autres informations requises. Vous pouvez choisir d'envoyer un e-mail à l'utilisateur avec des instructions pour configurer son mot de passe ou de générer un mot de passe à usage unique à partager avec lui.

4. Choisissez Next et assignez éventuellement le nouvel utilisateur à un ou plusieurs groupes.
5. Choisissez Next et passez en revue vos choix.

Si tout semble correct, choisissez Ajouter un utilisateur pour créer le nouvel utilisateur avec les informations que vous avez spécifiées.

Pour le didacticiel, l'exemple d'utilisateur est Bob Stiles, le nom d'utilisateur bobstiles et l'adresse e-mail bobstiles@example.com.

Étape 2 : Création d'une application Web Transfer Family

Pour créer une application Web 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 volet de navigation de gauche, sélectionnez Web apps.
3. Choisissez Créer une application Web.

Pour l'accès par authentification, notez que le service trouve automatiquement l' AWS IAM Identity Center instance que vous avez configurée comme condition préalable.

4. Dans le volet Type d'autorisation, sélectionnez Créer et utiliser un nouveau rôle de service. Le service crée pour vous le rôle de porteur d'identité. Un rôle de porteur d'identité inclut l'identité d'un utilisateur authentifié dans ses sessions.
5. Dans le volet des unités de l'application Web, acceptez la valeur par défaut de 1 ou ajustez-la à une valeur supérieure si nécessaire.
6. Ajoutez une balise pour vous aider à organiser vos applications Web. Pour le didacticiel, entrez le nom de la clé et l'application Web du didacticiel pour la valeur.

 Tip

Vous pouvez modifier le nom de l'application Web directement depuis la page de liste des applications Web après l'avoir créée.

7. Choisissez Suivant pour ouvrir la page de l'application Web Design. Sur cet écran, fournissez les informations suivantes.

Vous pouvez éventuellement fournir un titre pour votre application Web. Vous pouvez également télécharger des fichiers image pour votre logo et votre favicon.

- Pour le titre de page, personnalisez le titre de l'onglet du navigateur que vos utilisateurs voient lorsqu'ils se connectent à l'application Web. Si vous ne saisissez rien pour le titre de la page, la valeur par défaut est Transfer Web App.
- Pour le logo, téléchargez un fichier image. La taille de fichier maximale pour l'image de votre logo est de 50 Ko.
- Pour le favicon, téléchargez un fichier image. La taille de fichier maximale de votre favicon est de 20 Ko.

8. Choisissez Suivant, puis sélectionnez Créer une application Web.

Pour offrir une expérience personnalisée, vous pouvez fournir une URL personnalisée permettant à vos utilisateurs d'accéder à votre application Web Transfer Family. Pour en savoir plus, consultez [Mettez à jour votre point de terminaison d'accès avec une URL personnalisée](#).

Étape 3 : configurer le partage Cross-origin des ressources (CORS) pour votre bucket

Vous devez configurer le partage de ressources entre origines (CORS) pour tous les compartiments utilisés par votre application Web. Une configuration CORS est un document qui définit des règles identifiant les origines auxquelles vous autoriserez l'accès à votre bucket. Pour plus d'informations sur CORS, voir [Configuration du partage de ressources entre origines \(CORS\)](#).

Pour configurer le partage Cross-origin des ressources (CORS) pour votre compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez Buckets dans le panneau de navigation de gauche et recherchez votre compartiment dans la boîte de dialogue de recherche, puis choisissez l'onglet Autorisations.
3. Dans le partage de Cross-origin ressources (CORS), choisissez Modifier et collez le code suivant. *AccessEndpoint* Remplacez-le par le point de terminaison d'accès réel de votre application Web. Veillez à ne pas saisir de barres obliques à la fin, car cela entraîne des erreurs lorsque les utilisateurs tentent de se connecter à votre application Web.
 - Exemple incorrect : `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Exemple correct : `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`

Si vous réutilisez un bucket pour plusieurs applications Web, ajoutez leurs points de terminaison d'accès aux applications Web à la liste. `AllowedOrigins`

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
  },
]
```

```
"AllowedOrigins": [  
  "https://AccessEndpoint"  
],  
"ExposeHeaders": [  
  "last-modified",  
  "content-length",  
  "etag",  
  "x-amz-version-id",  
  "content-type",  
  "x-amz-request-id",  
  "x-amz-id-2",  
  "date",  
  "x-amz-cf-id",  
  "x-amz-storage-class",  
  "access-control-expose-headers"  
],  
"MaxAgeSeconds": 3000  
}  
]
```

4. Choisissez Enregistrer les modifications pour mettre à jour le CORS.

Étape 4 : Ajouter un utilisateur à votre application Web Transfer Family

Ajoutez l'utilisateur que vous avez créé précédemment dans IAM Identity Center.

Pour attribuer des utilisateurs à une application Web Transfer Family

1. Accédez à l'application Web que vous avez créée précédemment.
2. Choisissez Assign users and groups (Attribuer des utilisateurs et des groupes).

webapp-

[Assign users and groups](#) [Clear customization](#) [Delete](#)

Web app details [Edit](#)

Access endpoint [Info](#)
Share this with your users and add to your CORS policy.
<https://webapp-.transfer-webapp.us-east-2.on.aws>

Web app endpoint
[https://webapp--webapp.us-east-2.on.aws](#)

Web app units [Info](#)
1

Identity provider
[AWS IAM Identity Center](#)

IAM role
-

Instance ARN
arn:aws:sso::instance/ssoins-

Users **Groups**

Users (2) [Delete](#)

After you assign users to your web app, set up user permissions to access your S3 data in [S3 Access Grants](#)

< 1 >

☐	Display name	User ID	Username
☐	-	-	-
☐	-	-	-

3. Pour attribuer l'utilisateur que vous avez créé précédemment dans IAM Identity Center, sélectionnez Attribuer des utilisateurs et des groupes existants, puis sélectionnez Suivant.
 - a. Recherchez l'utilisateur par son nom d'affichage. Notez qu'aucun utilisateur n'apparaît tant que vous n'avez pas commencé à saisir vos critères de recherche. Pour ajouter **Bob Stiles**, saisissez bob dans le champ de recherche. Si vous ne trouvez pas votre utilisateur, accédez à la console de gestion IAM Identity Center, trouvez-le, puis copiez-collez son nom d'affichage ici.
 - b. Choisissez l'**Bob Stiles** utilisateur, puis choisissez Attribuer.

Étape 5 : enregistrer un emplacement dans Amazon S3 et créer une autorisation d'accès

Après avoir attribué un utilisateur à votre application Web, vous devez enregistrer un bucket et créer une autorisation d'accès pour cet utilisateur.

 Note

Vous devez disposer d'une instance S3 Access Grants avant de pouvoir continuer. Pour plus de détails, consultez la section [Créer une instance S3 Access Grants](#) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour enregistrer un emplacement et créer une autorisation d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez Access Grants dans le volet de navigation de gauche.
3. Choisissez Afficher les détails pour voir les détails de votre instance S3 Access Grants.
4. Sélectionnez l'onglet Emplacements, puis sélectionnez Enregistrer l'emplacement.
5. Saisissez les informations suivantes.
 - Pour le champ d'application, recherchez un compartiment ou entrez le nom de votre compartiment, et éventuellement un préfixe. Notez que le champ d'application commence par la chaîne **s3://**.
 - Pour le rôle IAM, choisissez Create new role pour qu'Amazon S3 crée un rôle. Ce rôle permet à S3 Access Grants d'accéder à l'étendue de localisation que vous avez spécifiée.

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location [Info](#)

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location [Info](#)

Location scope [Info](#)

You can't edit the location scope after registering the location.

Scope

s3://

View [View](#) [Browse S3](#)

Format for all buckets: s3://
 Format for bucket: s3://<bucket>
 Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

[To ensure the role has proper permissions to access the location scope, consult the list of permissions \[link\]](#)

IAM role [Info](#)

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role
☐ Choose from existing IAM roles
☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

Choisissez Enregistrer la localisation pour continuer.

6. Sélectionnez l'onglet Subventions, puis choisissez Créer une subvention et fournissez les informations suivantes.

- Dans Emplacement, sélectionnez Parcourir les emplacements et choisissez le lieu que vous avez enregistré à l'étape précédente.
- Dans le champ Sous-préfixe, entrez * pour indiquer que l'autorisation d'accès s'applique à l'ensemble du compartiment.
- Pour les autorisations, sélectionnez Lire et écrire.
- Pour le type de bénéficiaire, choisissez Directory identity dans IAM Identity Center.
- Pour le type d'identité du répertoire, sélectionnez Utilisateur.
- Dans le champ Utilisateur/ID d'IAM Identity Center, copiez et collez le nom d'utilisateur pour. **Bob Stiles** Cet identifiant est disponible dans le volet Utilisateurs de votre application Web Transfer Family.

7. Choisissez Create Grant.

L'autorisation d'accès est créée.

Étape 6 : Accédez à votre application Web Transfer Family en tant qu'utilisateur

À présent, nous accédons à l'URL de l'application Web et nous nous connectons en tant qu'utilisateur que nous avons attribué précédemment.

Pour vous connecter à l'application Web Transfer Family

1. Accédez à votre application Web
2. Choisissez le point de terminaison Access dans le volet de détails de l'application Web.

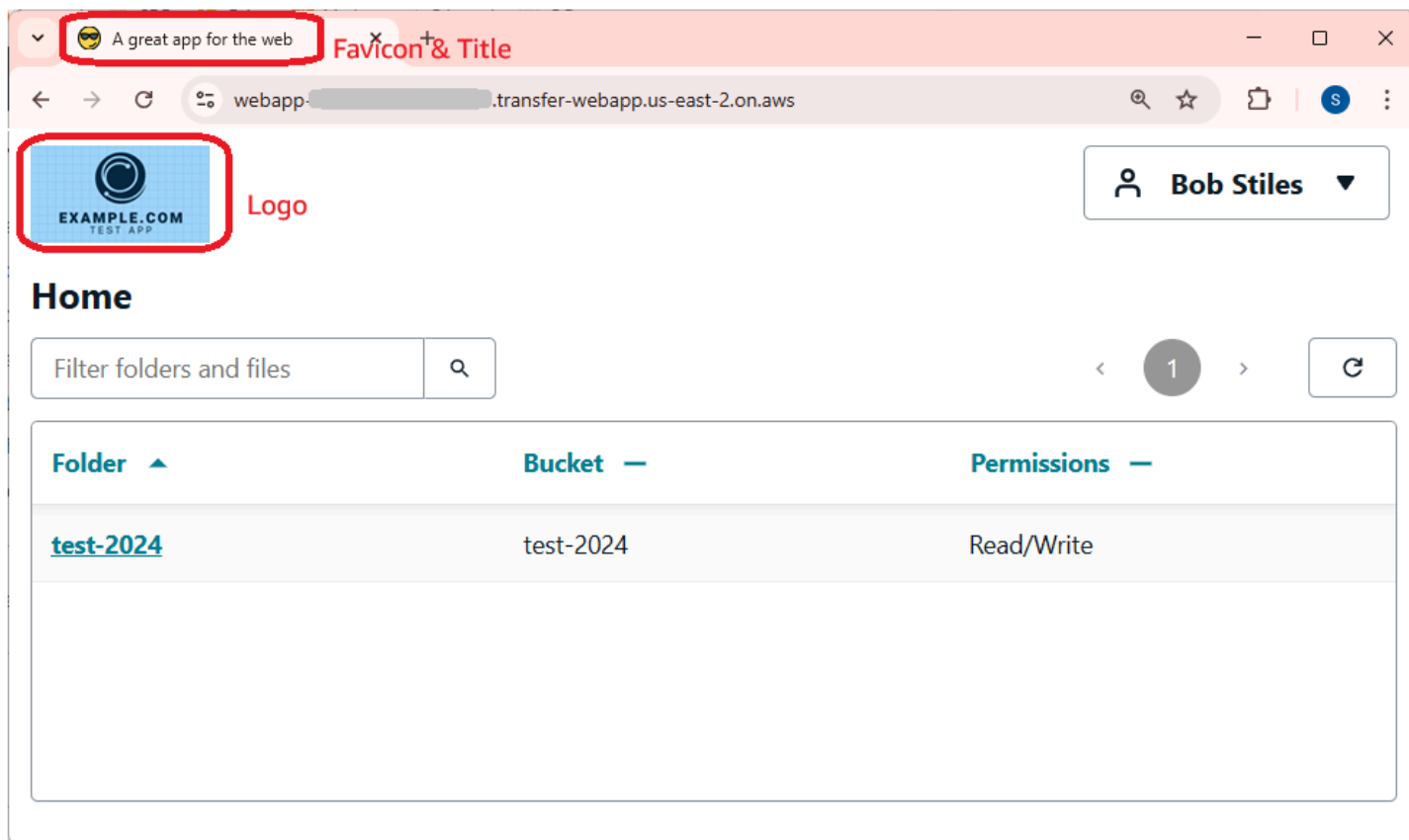
The screenshot shows the AWS IAM console interface for a web application. At the top, there's a header with the application name 'webapp-' followed by a redacted ID. To the right are buttons: 'Assign users and groups' (orange), 'Clear customization' (blue), and 'Delete' (blue). Below this is a 'Web app details' section with an 'Edit' button. It contains two columns of information. The left column has 'Access endpoint' (highlighted with a red box) with a link to 'https://webapp-...transfer-webapp.us-east-2.on.aws', 'Web app endpoint' with a similar link, and 'Web app units' (1). The right column lists 'Identity provider' (AWS IAM Identity Center), 'IAM role' (AWSTransferWebAppIdentityBearer-us-east-2), and 'Instance ARN' (arn:aws:sso::instance/ssoins-...). Below the details is a 'Users' tab (selected) and a 'Groups' tab. The 'Users' section shows 'Users (1)' with a 'Delete' button. A search bar 'Find resources' is present. Below is a table with columns 'Display name', 'User ID', and 'Username'. One user is listed: 'Bob Stiles' (highlighted with a red box), with a redacted User ID and username 'bobstiles'.

Display name	User ID	Username
Bob Stiles	[Redacted]	bobstiles

3. Sur l'écran de connexion, entrez l'utilisateur que vous avez créé **bobstiles**, puis sélectionnez Suivant.
4. Entrez le mot de passe attribué par le système à cet utilisateur lors de sa création et sélectionnez Suivant.
5. Si votre organisation a besoin d'une authentification multifactorielle (MFA), vous devez la configurer dès maintenant. Si ce n'est pas le cas, passez à l'étape 6.

- a. Un écran s'affiche pour enregistrer votre appareil MFA. Choisissez l'une des options disponibles, puis sélectionnez Suivant.
- b. Effectuez les étapes nécessaires pour configurer l'authentification multifacteur pour cet utilisateur : les étapes dépendent de l'option MFA que vous avez choisie.
- c. Vous devrez peut-être définir un nouveau mot de passe pour votre utilisateur : si nécessaire, faites-le maintenant. Le système peut également vous demander de vous reconnecter en utilisant les nouvelles informations d'identification MFA que vous avez configurées.

Votre utilisateur devrait voir un écran similaire au suivant. Notez que cette capture d'écran inclut la personnalisation du favicon et du logo.



Étapes suivantes

Vous avez correctement configuré une application Web Transfer Family de base avec un accès standard au bucket S3. Si vous avez besoin d'un contrôle plus précis des autorisations de compartiment, par exemple en permettant aux utilisateurs de télécharger depuis un compartiment

et de le télécharger vers un autre, consultez [Tutoriel : Configuration d'une application AWS Transfer Family Web avec un accès sélectif à plusieurs compartiments](#).

Intégrez Okta en tant que fournisseur d'identité pour les applications Web

Vous pouvez intégrer un fournisseur d'identité externe aux applications Web Transfer Family. Cette section explique comment configurer Okta en tant que fournisseur d'identité.

1. Dans Okta, créez un utilisateur, un groupe et une application. Pour plus de détails sur la procédure à suivre, consultez [Configurer SAML et SCIM avec Okta et IAM Identity Center](#).

The screenshot shows the AWS IAM Identity Center console. The left sidebar contains navigation links: Applications, Self Service, API Service Integrations, Your OIN Integrations, Security, Workflow, Reports, and Settings. The main content area is titled 'AWS IAM Identity Center' and shows the 'Push Groups' configuration page. The page has tabs for General, Sign On, Provisioning, Import, Assignments, and Push Groups. The 'Push Groups' tab is active, showing a table of pushed groups. The table has columns: Pushed Groups, Group in Okta, Group in AWS IAM Identity Center, Last Push, and Push Status. One group, 'Examplegroup', is listed with a status of 'Active'.

2. Connectez Okta et importez des utilisateurs et des groupes depuis Okta vers AWS IAM Identity Center. Suivez les étapes 1 à 4 de la section [Configurer SAML et SCIM avec Okta et IAM Identity Center](#).

The screenshot shows the AWS IAM Identity Center console. The left sidebar contains navigation links: Dashboard, Users, Groups, Settings, Multi-account permissions, AWS accounts, and Permission sets. The main content area is titled 'IAM Identity Center' and shows the 'Users' configuration page. The page has a message: 'Your identity source is currently configured as 'External identity provider'. To add new users or edit their attributes, you must do this using your external identity provider (IdP)'. Below the message, there is a 'Users (2)' section with a 'Delete users' button. A table of users is displayed with columns: Username, Display name, Status, and Created by. Two users are listed: 'Exampleuser' and 'johnstiles'. The 'Exampleuser' row is highlighted with a red box.

IAM Identity Center

Managing instance
ssoins-6684735b83d16df8

Dashboard

Users

Groups

Settings

Multi-account permissions

AWS accounts

Permission sets

Your identity source is currently configured as 'External identity provider'. To add new groups or edit their memberships, you must do this using your external identity provider.

Groups (2)

With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. [Learn more](#)

Find groups by group name

< 1 >

	Group name	Users	Description	Created by
☐	Examplegroup	1 user	-	SCIM
☐	dev	1 user	-	Manual

3. Vérifiez que la source d'identité dans IAM Identity Center est SAML 2.0.

Settings

Details

Configure your identity source and multi-factor authentication settings for use when managing access to your AWS accounts, resources, and cloud applications.

Instance name - [Edit](#)

Region
US East (Ohio) | us-east-2

Instance ID
ssoins-

Date created
Thursday, November 14, 2024 at 4:11:19 PM EST

Organization ID
AWS Organizations not enabled

Instance ARN
[arn:aws:sso:::instance/ssoins-](#)

Identity source

Authentication

Management

Tags

Identity source

Choose the directory where you want to manage your users and groups. [Learn More](#)

Identity source
External identity provider

Authentication method
SAML 2.0

Provisioning method
SCIM

AWS access portal URL
[https://.awsapps.com/start](#)

Identity store ID
d-

Issuer URL
[https://identitycenter.amazonaws.com/ssoins-](#)

Actions

Intégrez Okta en tant que fournisseur d'identité pour les applications Web

107

4. Attribuez votre utilisateur et votre groupe, comme décrit dans [Étape 4 : Ajouter un utilisateur à votre application Web Transfer Family](#).
5. Pour éviter que vos utilisateurs n'aient besoin d'utiliser le MFA lorsqu'ils se connectent à votre application Web, effectuez les étapes suivantes dans Okta.
 - a. Depuis la console d'administration Okta, accédez à [Applications] - [Applications], puis sélectionnez l' AWS IAM Identity Center application.
 - b. Dans l'onglet Connexion, sélectionnez [Authentification utilisateur] - Modifier.
 - c. Sélectionnez Mot de passe uniquement.

Après avoir effectué toutes les autres étapes du didacticiel, votre utilisateur devrait pouvoir accéder à votre application Web Transfer Family en accédant au point d'accès de l'application Web dans un navigateur Web.

Tutoriel : Configuration d'une application AWS Transfer Family Web avec un accès sélectif à plusieurs compartiments

Ce didacticiel vous explique comment configurer une application Web Transfer Family avec des autorisations de bucket Amazon S3 spécifiques pour un seul utilisateur. Vous allez apprendre à configurer une solution qui permet aux utilisateurs de télécharger depuis un compartiment et de le télécharger vers un autre tout en préservant la sécurité. Il s'agit d'un didacticiel avancé qui s'appuie sur les concepts abordés dans le didacticiel de base. Si vous débutez dans le domaine des applications AWS Transfer Family Web, pensez à commencer par [Tutoriel : Configuration d'une application Web Transfer Family de base](#).

Conditions préalables

Avant de démarrer ce tutoriel, assurez-vous de disposer des éléments suivants :

- IAM Identity Center est configuré dans la même région que votre application AWS Transfer Family Web. Notez qu'une AWS seule instance d'IAM Identity Center par AWS compte est autorisée pour toutes les régions.
- Au moins un utilisateur est configuré dans IAM Identity Center.
- Deux compartiments S3 : un pour les téléchargements et un pour les téléchargements.

 Note

Ce didacticiel partage de nombreux prérequis avec le didacticiel de base de l'application Web. Pour plus d'informations sur la configuration d'IAM Identity Center et la création d'utilisateurs, consultez [Tutoriel : Configuration d'une application Web Transfer Family de base](#).

Étape 1 : créer une application Web Transfer Family

Pour créer une application Web 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 volet de navigation de gauche, sélectionnez Web apps.
3. Choisissez Créer une application Web.

Pour l'accès par authentification, notez que le service trouve automatiquement l' AWS IAM Identity Center instance que vous avez configurée comme condition préalable.

4. Dans le volet Type d'autorisation, sélectionnez Créer et utiliser un nouveau rôle de service. Le service crée pour vous le rôle de porteur d'identité. Un rôle de porteur d'identité inclut l'identité d'un utilisateur authentifié dans ses sessions.
5. Dans le volet des unités de l'application Web, acceptez la valeur par défaut de 1 ou ajustez-la à une valeur supérieure si nécessaire.
6. Ajoutez une balise pour vous aider à organiser vos applications Web. Pour le didacticiel, entrez le nom de la clé et l'application Web du didacticiel pour la valeur.

 Tip

Vous pouvez modifier le nom de l'application Web directement depuis la page de liste des applications Web après l'avoir créée.

7. Choisissez Suivant pour ouvrir la page de l'application Web Design. Sur cet écran, fournissez les informations suivantes.

Vous pouvez éventuellement fournir un titre pour votre application Web. Vous pouvez également télécharger des fichiers image pour votre logo et votre favicon.

- Pour le titre de page, personnalisez le titre de l'onglet du navigateur que vos utilisateurs voient lorsqu'ils se connectent à l'application Web. Si vous ne saisissez rien pour le titre de la page, la valeur par défaut est Transfer Web App.
- Pour le logo, téléchargez un fichier image. La taille de fichier maximale pour l'image de votre logo est de 50 Ko.
- Pour le favicon, téléchargez un fichier image. La taille de fichier maximale de votre favicon est de 20 Ko.

8. Choisissez Suivant, puis sélectionnez Créer une application Web.

Étape 2 : Configuration des rôles IAM pour l'accès S3

Vous devez créer deux rôles IAM : un avec un accès en téléchargement uniquement au premier compartiment et un autre avec un accès en téléchargement uniquement au second compartiment.

Politique de confiance pour les deux rôles

Utilisez la politique de confiance suivante pour les deux rôles IAM :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AccessGrantsTrustPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity",
        "sts:SetContext"
      ]
    }
  ]
}
```

Politique IAM pour le bucket de téléchargement

Créez un rôle IAM avec la politique suivante pour un accès en lecture seule à votre compartiment de téléchargement :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        "arn:aws:s3:::amzn-s3-demo-bucket1"
      ]
    }
  ]
}
```

Important

Remplacez `amzn-s3-demo-bucket1` par le nom réel de votre bucket de téléchargement.

Politique IAM pour le bucket de téléchargement

Créez un autre rôle IAM avec la politique suivante pour l'accès en écriture à votre compartiment de téléchargement :

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

```
"Statement": [
  {
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutObjectVersionAcl",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:AbortMultipartUpload",
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket2/*",
      "arn:aws:s3:::amzn-s3-demo-bucket2"
    ]
  }
]
```

Important

Remplacez amzn-s3-demo-bucket2 par le nom réel de votre bucket de téléchargement.

Étape 3 : configurer les autorisations d'accès S3

1. Ouvrez la console S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation, sélectionnez Access Grants.
3. Cliquez sur Créer une instance S3 Access Grants.
4. Sélectionnez l'option Ajouter une instance de centre d'identité IAM et entrez l'ARN de l'instance de centre d'identité.
5. Cliquez sur Suivant, puis sur Annuler pour terminer la création de l'instance S3 Access Grants sans passer par d'autres étapes.

Cette étape crée l'instance S3 Access Grants. Vous allez maintenant enregistrer les sites et créer des autorisations d'accès.

Étape 4 : enregistrer les emplacements des compartiments S3

Enregistrez les deux compartiments S3 en tant qu'emplacements avec des autorisations d'accès S3 :

1. Dans la console S3 Access Grants, accédez à Emplacements et cliquez sur Enregistrer l'emplacement.
2. Sous Zone d'emplacement, choisissez le compartiment S3 spécifique pour les téléchargements (amzn-s3-demo-bucket1).
3. Lorsque vous êtes invité à choisir un rôle IAM, sélectionnez le rôle IAM de téléchargement que vous avez créé précédemment.
4. Terminez le processus d'inscription.
5. Répétez le processus pour enregistrer le bucket de téléchargement (amzn-s3-demo-bucket2), en sélectionnant le rôle IAM de téléchargement lorsque vous y êtes invité.

Étape 5 : créer des autorisations d'accès

Créez deux subventions, une pour chaque établissement enregistré :

1. Dans la console S3 Access Grants, accédez à Grants et cliquez sur Create grant grant.
2. Dans Emplacement, cliquez sur Parcourir l'emplacement et sélectionnez l'emplacement du compartiment de téléchargement (amzn-s3-demo-bucket1).
3. Dans Sous-préfixe (facultatif), entrez * pour autoriser l'accès à l'ensemble du compartiment ou spécifiez un chemin `folder1/folder2/*` pour restreindre l'accès à un préfixe spécifique.

L'utilisation * définira la portée de la subvention `s3://bucket-name/*`, autorisant l'accès à l'ensemble du compartiment. Pour autoriser l'accès à un préfixe spécifique uniquement, entrez un chemin tel que `folder1/folder2/*`, qui définira la portée de la subvention `s3://bucket-name/folder1/folder2/*`.

4. Sous Autorisations et accès, sélectionnez Lire pour le compartiment de téléchargement.
5. Dans Type de bénéficiaire, choisissez Directory identity from IAM Identity Center.
6. Pour le type principal IAM, sélectionnez Utilisateur et entrez l'ID utilisateur de votre utilisateur IAM Identity Center.
7. Terminez le processus de création de subventions.
8. Répétez le processus pour créer une autorisation pour le compartiment de téléchargement (amzn-s3-demo-bucket2), mais sélectionnez les autorisations. Read-write

Étape 6 : Configuration de la politique CORS pour les compartiments S3

Configurez une politique CORS pour les deux compartiments S3 afin d'autoriser l'accès via : AWS Transfer Family WebApp

1. Ouvrez la console S3 et accédez à votre compartiment de téléchargement (amzn-s3-demo-bucket1).
2. Sélectionnez l'onglet Autorisations.
3. Faites défiler la page jusqu'à la section Partage Cross-origin des ressources (CORS) et cliquez sur Modifier.
4. Ajoutez la configuration CORS suivante, en la remplaçant par l'URL réelle *WebAppEndpoint* de votre point de WebApp terminaison :

Vous trouverez l'URL du point de terminaison de votre application Web dans la AWS Transfer Family console ci-dessous WebApps. Cela ressemblera à `https://webapp-*****.transfer-webapp.us-west-2.on.aws`.

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://WebAppEndpoint"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
```

```
        "x-amz-cf-id",  
        "x-amz-storage-class",  
        "access-control-expose-headers"  
    ],  
    "MaxAgeSeconds": 3000  
}  
]
```

5. Cliquez sur Save changes (Enregistrer les modifications).
6. Répétez le processus pour votre bucket de téléchargement (amzn-s3-demo-bucket2).

Étape 7 : tester la configuration

1. Ouvrez l'URL de votre application AWS Transfer Family Web. Vous pouvez trouver cette URL dans la AWS Transfer Family console, WebApps sous le champ Access Endpoint.
2. Connectez-vous à l'aide des informations d'identification utilisateur IAM Identity Center que vous avez configurées avec des autorisations d'accès.
3. Une fois connecté, vous devriez voir les deux emplacements S3 sur la page d'accueil.
4. Accédez au compartiment de téléchargement (amzn-s3-demo-bucket1) et vérifiez que vous pouvez télécharger des fichiers mais pas les charger.
5. Accédez au compartiment de téléchargement (amzn-s3-demo-bucket2) et vérifiez que vous pouvez télécharger des fichiers.

Conclusion

Vous avez correctement configuré AWS Transfer Family WebApp l'accès sélectif au compartiment S3 pour un seul utilisateur. Cette configuration permet à l'utilisateur de télécharger depuis un compartiment et de le télécharger vers un autre tout en préservant la sécurité grâce aux rôles IAM et aux autorisations d'accès S3.

Cette approche peut être étendue à plusieurs utilisateurs en créant des autorisations supplémentaires dans S3 Access Grants pour chaque utilisateur, ce qui permet un contrôle granulaire des autorisations d'accès aux compartiments. Pour plus d'informations sur la configuration de base de l'application Web, consultez [Tutoriel : Configuration d'une application Web Transfer Family de base](#).

Configuration d'un point de terminaison de serveur SFTP, FTPS ou FTP

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 protocoles SFTP, FTPS et FTP.

Rubriques

- [Options du fournisseur d'identité](#)
- [AWS Transfer Family matrice des types de terminaux](#)
- [Configuration d'un point de terminaison de serveur SFTP, FTPS ou FTP](#)
- [Considérations relatives aux Network Load Balancer FTP et FTPS](#)
- [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](#)
- [Accédez à vos systèmes de fichiers FSx for NetApp ONTAP avec 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	Amazon API Gateway	AWS Lambda
Protocoles pris en charge	SFTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP	SFTP, FTPS, FTP
Key-based authentication	Oui	Non	Oui	Oui

Action	AWS Transfer Family service géré	AWS Managed Microsoft AD	Amazon API Gateway	AWS Lambda
Authentification par mot de passe	Non	Oui	Oui	Oui
Gestion des identités et des accès AWS (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 Entra ID (anciennement 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 CloudFormation modèles pour vous aider à déployer rapidement un serveur Transfer Family qui utilise un fournisseur d'identité personnalisé. Pour en savoir plus, consultez [Modèles de fonctions Lambda](#).

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

Étape suivante

- [Création d'un SFTP-enabled serveur](#)
- [Création d'un FTPS-enabled serveur](#)
- [Création d'un FTP-enabled serveur](#)
- [Configuration d'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 spéciale dans votre VPC.	Sur Internet et depuis un VPC et des VPC-connected environnements, tels qu'un centre de données sur site ou un VPN. Direct Connect	Depuis un VPC et VPC-connected des environnements, tels qu'un centre de données sur site ou un VPN. Direct Connect	Depuis un VPC et VPC-connected des environnements, tels qu'un centre de données sur site ou un VPN. Direct Connect

Caractéristiques	Public	VPC - Internet	VPC - Interne	VPC_Endpoint (obsolète)
Adresse IP statique	Vous ne pouvez pas joindre une adresse IP statique. AWS fournit des adresses IP susceptibles de changer.	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 élastiques 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 VPC-hosted terminaux, les serveurs SFTP Transfer Family peuvent fonctionner sur le port 22 (par défaut), 2222,	Pour autoriser l'accès par adresse IP source, vous pouvez utiliser des groupes de sécurité attachés aux points de terminaison du serveur et des ACL réseau attachés 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 (ACL réseau) 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 des ACL réseau attachés au sous-réseau dans lequel se trouve le point de terminaison.

Caractéristiques	Public	VPC - Internet	VPC - Interne	VPC_Endpoint (obsolète)
	2223 ou 22000.			
Liste d'autorisations du pare-feu client	Vous devez autoriser le nom DNS 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 nom DNS du serveur ou les adresses IP élastiques associées au serveur.	Vous pouvez autoriser les adresses IP privées ou le nom DNS des points de terminaison.	Vous pouvez autoriser les adresses IP privées ou le nom DNS des points de terminaison.
Type d'adresse IP	IPv4 (par défaut) ou double pile (IPv4 et IPv6)	IPv4 uniquement (le double stack n'est pas pris en charge)	IPv4 (par défaut) ou double pile (IPv4 et IPv6)	IPv4 uniquement (le double stack n'est pas pris en charge)

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 type de point de terminaison VPC (`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 sur cette dépréciation, consultez. [Arrêt de l'utilisation de VPC_ENDPOINT](#)

- Pour plus d'informations sur la gestion des autorisations des points de terminaison VPC, consultez. [Limiter l'accès aux points de terminaison VPC pour les serveurs Transfer Family](#)

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

- Utilisez un point de terminaison VPC doté d'un accès interne, afin que le serveur ne soit accessible qu'aux clients de votre VPC ou à des VPC-connected environnements tels qu'un centre de données sur site ou un VPN. Direct Connect
- Pour permettre aux clients d'accéder au point de terminaison via Internet et de protéger votre serveur, utilisez un point de terminaison VPC doté d'un accès Internet. Modifiez ensuite les groupes de sécurité du VPC 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 serveur SFTP sous-jacent pour exécuter des commandes natives du système d'exploitation sur les serveurs Transfer Family Family.
- Utilisez un Network Load Balancer devant un point de terminaison VPC doté 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 du NLB, plutôt que l'adresse IP réelle du client.

Configuration d'un point de terminaison de serveur SFTP, FTPS ou FTP

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 (SFTP) Secure Shell (SSH) — Transfert de fichiers via SSH. Pour en savoir plus, consultez [the section called “Création d'un SFTP-enabled serveur”](#).

Note

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

- Protocole de transfert de fichiers sécurisé (FTPS) — Transfert de fichiers avec cryptage TLS. Pour en savoir plus, consultez [the section called “Création d'un FTPS-enabled serveur”](#).
- Protocole de transfert de fichiers (FTP) — Transfert de fichiers non chiffré. Pour en savoir plus, consultez [the section called “Création d'un FTP-enabled serveur”](#).
- Déclaration d'applicabilité 2 (AS2) — Transfert de fichiers pour le transport de données interentreprises structurées. Pour en savoir plus, consultez [the section called “Configurer AS2”](#). Pour AS2, vous pouvez créer rapidement une CloudFormation pile à des fins de démonstration. Cette procédure est décrite dans [Utilisez un modèle pour créer un stack Transfer Family AS2 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 le protocole FTP, nous vous recommandons de conserver des informations d'identification distinctes pour le protocole SFTP et le protocole FTPS. Cela est dû au fait que, contrairement au SFTP et au FTPS, le protocole FTP transmet les informations d'identification en texte clair. En isolant les informations d'identification FTP de celles du protocole SFTP ou FTPS, si les informations

d'identification FTP sont partagées ou exposées, vos charges de travail utilisant le protocole SFTP ou FTPS restent sécurisées.

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 clés SSH. Pour en savoir plus, 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 en savoir plus, consultez [Utilisation de AWS Directory Service pour Microsoft Active Directory](#).
- Un fournisseur d'identité personnalisé. Transfer Family propose plusieurs options pour utiliser un fournisseur d'identité personnalisé, comme décrit dans la [Travailler avec des fournisseurs d'identité personnalisés](#) rubrique.

Vous attribuez également au serveur un type de point de terminaison (accessible au public ou hébergé par VPC) 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 un service DNS (Domain Name System) 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-enabled serveur

Le protocole de transfert de fichiers (SFTP) Secure Shell (SSH) 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.

Notez ce qui suit

- Les serveurs SFTP de Transfer Family fonctionnent via le port 22. Pour les VPC-hosted terminaux, les serveurs SFTP Transfer Family peuvent également fonctionner via les ports 2222, 2223 ou 22000. Pour en savoir plus, consultez [Création d'un serveur dans un cloud privé virtuel](#).
- Les points de terminaison publics ne peuvent pas restreindre le trafic via des groupes de sécurité. Pour utiliser des groupes de sécurité avec votre serveur Transfer Family, vous devez héberger le point de terminaison de votre serveur dans un cloud privé virtuel (VPC) comme décrit dans [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, [consultez la section Utiliser la liste d'adresses IP autorisées pour sécuriser AWS Transfer Family](#) vos serveurs.

Pour créer un SFTP-enabled serveur

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 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.
 - AWS Directory Service for Microsoft Active Directory— Vous fournissez un 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 de AWS Directory Service pour Microsoft Active Directory](#).

 Note

- Cross-Account et les répertoires 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 Directory Service autorisations. Pour en savoir plus, consultez [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#).

- 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 une URL Amazon API Gateway 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

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 :

- Pour le type de point de terminaison, choisissez le type de point de terminaison accessible au public. Pour un point de terminaison hébergé par VPC, consultez. [Création d'un serveur dans un cloud privé virtuel](#)
- Pour le type d'adresse IP, choisissez IPv4 (par défaut) pour une rétrocompatibilité ou pour activer les connexions IPv4 et IPv6 Dual-stack à votre point de terminaison.

 Note

Dual-stack le mode permet à votre point de terminaison Transfer Family de communiquer avec les clients compatibles IPv4 et IPv6. Cela vous permet de passer progressivement d'un système IPv4 à un système basé sur IPv6 sans avoir à tout changer en même temps.

- c. (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](#).

- d. (Facultatif) Pour FIPS Enabled, cochez la case FIPS Enabled endpoint pour vous assurer que le endpoint est conforme aux Federal Information Processing Standards (FIPS).

 Note

FIPS-enabled les points de terminaison ne sont disponibles que dans les AWS régions d'Amérique 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 la norme FIPS, consultez la [norme fédérale de traitement de l'information \(FIPS\) 140-2](#).

- e. Choisissez Suivant.

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

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 les ID de flux de travail (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. Notre dernière politique de sécurité est celle par défaut : pour plus de détails, voir [Politiques de sécurité pour AWS Transfer Family serveurs](#).
- d. (Facultatif) Pour la clé d'hôte du serveur, entrez une clé privée RSA, ED25519 ou ECDSA qui sera utilisée pour identifier votre serveur lorsque des clients s'y connecteront via 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 d'hôte si vous souhaitez faire pivoter les clés ou si vous souhaitez disposer de différents types de clés, comme une clé RSA et une clé ECDSA.

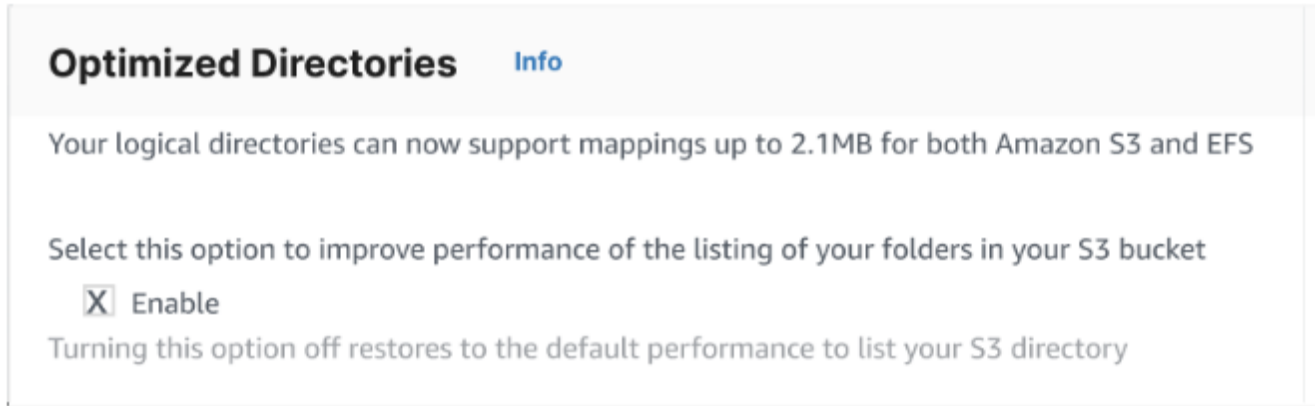
Note

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

- 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.
- 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 Amazon 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.

Lorsque vous créez votre serveur à l'aide de la console, les répertoires optimisés sont activés par défaut. Si vous créez votre serveur à l'aide de l'API, ce comportement n'est pas activé par défaut.



- 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'Pre-authentication affichage, entrez le message texte que vous souhaitez afficher à vos utilisateurs avant qu'ils ne s'authentifient.
- 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](#).
 - Reprise de session TLS : cette option n'est disponible que si vous avez activé le protocole FTPS pour ce serveur.
 - IP passive : cette option n'est disponible que si vous avez activé FTPS ou FTP comme 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 les fichiers, mais vous devez d'abord créer un utilisateur. Pour plus de détails sur la création d'utilisateurs, consultez [Gestion des utilisateurs pour les points de terminaison du serveur](#).

Création d'un FTPS-enabled serveur

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

Note

Pour des considérations importantes concernant les équilibreurs de charge réseau, voir [Évitez de placer les NLB et les NAT devant AWS Transfer Family serveurs](#).

Pour créer un FTPS-enabled serveur

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 via 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 dans ACM dans](#) le guide de l'AWS Certificate Manager utilisateur.

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

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

- RSA 2048 octets (RSA_2048)
- RSA 4 096 octets (RSA_4096)
- 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 certificat de SSL/TLS X.509 version 3 valide avec un nom de domaine complet ou une adresse IP spécifiée et contenir des informations sur l'émetteur.

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 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 de AWS Directory Service pour Microsoft Active Directory](#).

 Note

- Cross-Account et les répertoires 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 Directory Service autorisations. Pour en savoir plus, consultez [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#).

- 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 une URL Amazon API Gateway 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

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

 Note

Les terminaux accessibles au public ne sont pas pris en charge.

- b. (Facultatif) Pour FIPS Enabled, cochez la case FIPS Enabled endpoint pour vous assurer que le endpoint est conforme aux Federal Information Processing Standards (FIPS).

 Note

FIPS-enabled les points de terminaison ne sont disponibles que dans les AWS régions d'Amérique 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 la norme FIPS, consultez la [norme fédérale de traitement de l'information \(FIPS\) 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 fichiers Amazon EFS 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 - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains two sections: 'Logging' and 'Log group'. The 'Logging' section has an 'Info' icon 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 text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. The 'Log group' section has an 'Info' icon 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 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 les ID de flux de travail (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](#) [external link]

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

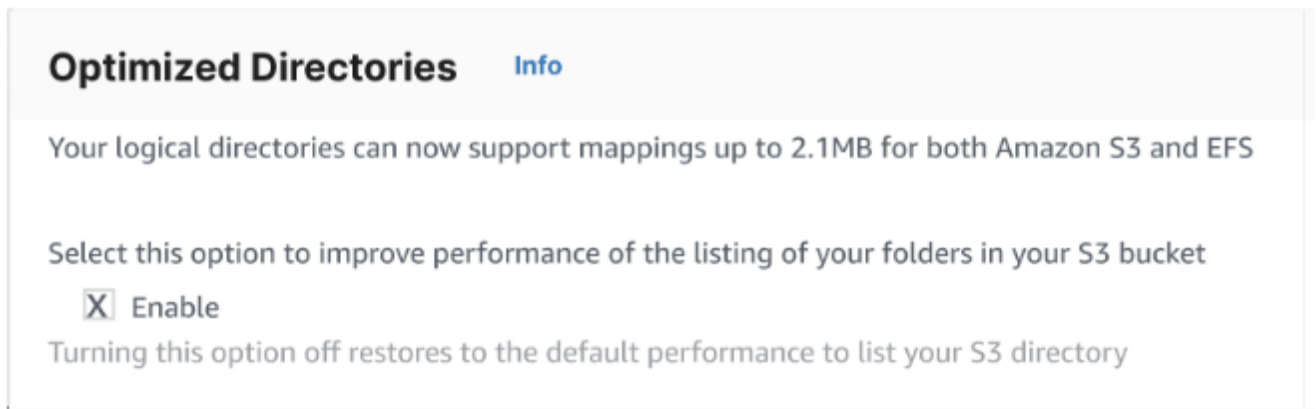
w- [dropdown] [refresh] [Create a new Workflow](#) [external link]

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. Notre dernière politique de sécurité est celle par défaut : pour plus de détails, voir [Politiques de sécurité pour AWS Transfer Family serveurs](#).
- d. Pour la clé d'hôte du serveur, laissez-la vide.
- 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 Amazon 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.

Lorsque vous créez votre serveur à l'aide de la console, les répertoires optimisés sont activés par défaut. Si vous créez votre serveur à l'aide de l'API, ce comportement n'est pas activé par défaut.



- g. Choisissez Suivant.
- 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 (MOTD) personnalisé aux utilisateurs qui se sont authentifiés avec succès.

Pour Afficher la bannière, dans la zone de texte de la bannière Pre-authentication d'affichage, 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 Post-authentication d'affichage, entrez le texte que vous souhaitez afficher à vos utilisateurs une fois qu'ils se sont authentifiés avec succès.

- 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.
 - Reprise de session TLS : fournit un mécanisme permettant de reprendre ou de partager une clé secrète négociée entre le contrôle et la connexion de données pour une session FTPS. Pour plus de détails, consultez la TlsSessionResumptionMode documentation dans cette [ProtocolDetails](#) rubrique.
 - IP passive : indique le mode passif, pour les protocoles FTP et FTPS. Saisissez une adresse IPv4 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.

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

Création d'un FTP-enabled serveur

Le protocole FTP (File Transfer Protocol) est un protocole réseau utilisé pour le transfert de données. Le protocole FTP utilise un canal distinct 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. Le protocole FTP utilise du texte clair et ne prend pas en charge le chiffrement du trafic.

Note

Lorsque vous activez le FTP, vous devez choisir l'option d'accès interne pour le VPC-hosted point de terminaison. 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.

Note

Pour des considérations importantes concernant les équilibreurs de charge réseau, voir [Évitez de placer les NLB et les NAT devant AWS Transfer Family serveurs](#).

Pour créer un FTP-enabled serveur

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 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 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 de AWS Directory Service pour Microsoft Active Directory](#).

 Note

- Cross-Account et les répertoires 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 Directory Service autorisations. Pour en savoir plus, consultez [Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory](#).

- 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 une URL Amazon API Gateway 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

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

 Note

Les terminaux accessibles au public ne sont pas pris en charge.

- b. Pour FIPS Enabled, laissez la case FIPS Enabled Endpoint cochée.

 Note

FIPS-enabled les points de terminaison ne sont pas pris en charge pour les serveurs FTP.

- 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 fichiers Amazon EFS via le protocole sélectionné.

Choisissez Suivant.

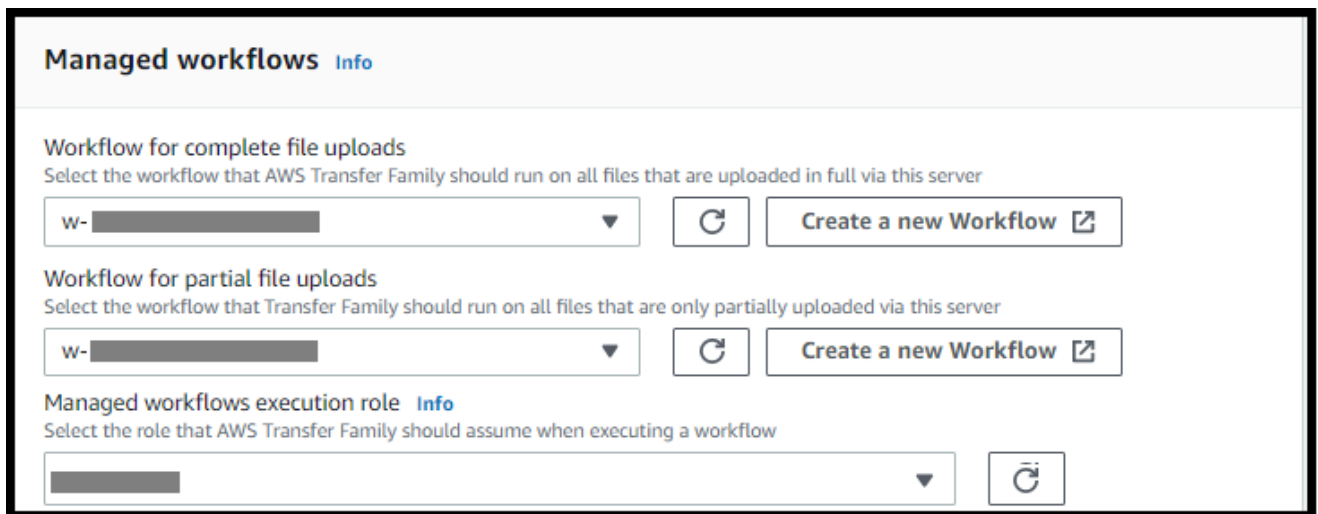
7. Dans Configurer les détails supplémentaires, procédez comme suit :

- 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 - currently active), and Step 6 (Review and create). The main content area is titled 'Configure additional details' and contains two sections: 'Logging' and 'Log group'. The 'Logging' section has an 'Info' icon 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 text input field containing '/aws/transfer/' followed by a dropdown arrow, a refresh button, and a 'Create log group' button with an external link icon. The 'Log group' section has an 'Info' icon 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-bordered box contains an information icon and the text: '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 les ID de flux de travail (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]

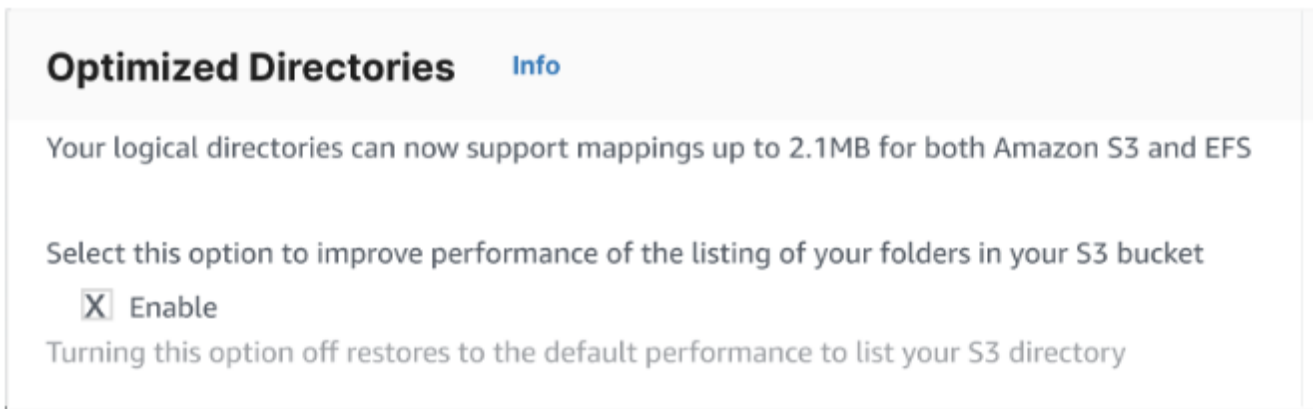
- c. Pour les options d'algorithme cryptographique, choisissez une politique de sécurité contenant les algorithmes cryptographiques activés pour être utilisés par votre serveur.

Note

Transfer Family attribue la dernière politique de sécurité à votre serveur FTP. Cependant, étant donné que le protocole FTP n'utilise aucun cryptage, les serveurs FTP n'utilisent aucun algorithme de politique de sécurité. À moins que votre serveur n'utilise également le protocole FTPS ou SFTP, la politique de sécurité reste inutilisée.

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

Lorsque vous créez votre serveur à l'aide de la console, les répertoires optimisés sont activés par défaut. Si vous créez votre serveur à l'aide de l'API, ce comportement n'est pas activé par défaut.



- g. Choisissez Suivant.
- 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 (MOTD) personnalisé aux utilisateurs qui se sont authentifiés avec succès.

Pour Afficher la bannière, dans la zone de texte de la bannière Pre-authentication d'affichage, 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 Post-authentication d'affichage, entrez le texte que vous souhaitez afficher à vos utilisateurs une fois qu'ils se sont authentifiés avec succès.

- 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.
 - Reprise de session TLS : fournit un mécanisme permettant de reprendre ou de partager une clé secrète négociée entre le contrôle et la connexion de données pour une session FTPS. Pour plus de détails, consultez la TlsSessionResumptionMode documentation dans cette [ProtocolDetails](#) rubrique.
 - IP passive : indique le mode passif, pour les protocoles FTP et FTPS. Saisissez une adresse IPv4 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.

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 fichiers Amazon EFS 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 “Arrêt de l'utilisation de VPC_ENDPOINT”](#).

Si vous utilisez Amazon Virtual Private Cloud (Amazon VPC) pour héberger vos AWS ressources, vous pouvez établir une connexion privée entre votre 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.

À l'aide d'Amazon VPC, vous pouvez lancer AWS des ressources dans un réseau virtuel personnalisé. Vous pouvez utiliser un 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'informations sur les VPC, consultez [Qu'est-ce qu'Amazon VPC ?](#) dans le guide de l'utilisateur Amazon VPC.

Dans les sections suivantes, vous trouverez des instructions sur la façon de créer et de connecter votre VPC à un serveur. En résumé, procédez comme suit :

1. Configurez un serveur à l'aide d'un point de terminaison VPC.
2. Connectez-vous à votre serveur à l'aide d'un client situé dans votre VPC via le point de terminaison du VPC. 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 rendre le point de terminaison de votre serveur accessible à Internet, vous pouvez associer des adresses IP élastiques à votre point de terminaison. Cela permet aux clients extérieurs à votre VPC de se connecter à votre serveur. Vous pouvez utiliser

les groupes de sécurité VPC pour contrôler l'accès aux utilisateurs authentifiés dont les demandes proviennent uniquement d'adresses autorisées.

 Note

AWS Transfer Family prend en charge les points de terminaison à double pile, permettant à votre serveur de communiquer à la fois via IPv4 et IPv6. Pour activer le support à double pile, sélectionnez l'option Activer le point de terminaison DNS à double pile lors de la création de votre point de terminaison VPC. Notez que votre VPC et vos sous-réseaux doivent être configurés pour prendre en charge IPv6 avant de pouvoir utiliser cette fonctionnalité. Dual-stack le support est particulièrement utile lorsque vous avez des clients qui doivent se connecter en utilisant l'un ou l'autre des protocoles.

Pour plus d'informations sur les points de terminaison de serveur à double pile (IPv4 et IPv6), consultez. [Support IPv6 pour les serveurs Transfer Family](#)

Rubriques

- [Créez un point de terminaison de serveur accessible uniquement au sein de votre VPC](#)
- [Créez un point de terminaison connecté à Internet pour votre serveur](#)
- [Modifier le type de point de terminaison de votre serveur](#)
- [Arrêt de l'utilisation de VPC_ENDPOINT](#)
- [Limiter l'accès aux points de terminaison VPC pour les serveurs Transfer Family](#)
- [Fonctionnalités réseau supplémentaires](#)
- [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 au sein de votre VPC

Dans la procédure suivante, vous créez 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-enabled serveur](#).
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.

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 Gestion des identités et des accès AWS (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 hébergé par VPC 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.

Pour plus de détails sur l'option Internet Facing, voir [Créez un point de terminaison connecté à Internet pour votre serveur](#). Un serveur créé dans un VPC pour un accès interne uniquement ne prend pas en charge les noms d'hôte personnalisés.

- c. Pour le VPC, choisissez un ID de VPC existant ou choisissez Create a VPC pour 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 ou plusieurs ID de groupe de sécurité existants 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 pour votre 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

Votre VPC est associé automatiquement 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 entrantes pour le groupe de sécurité, vous pouvez configurer le trafic SSH pour qu'il utilise les ports 22, 2222, 22000 ou une combinaison des deux. Le port 22 est configuré par défaut. Pour utiliser le port 2222 ou le port 22000, vous devez ajouter une règle entrante à votre groupe de sécurité. Pour le type, choisissez TCP personnalisé, puis entrez l'une **2222** ou **22000** l'autre plage de ports, et pour la source, entrez la même plage d'adresses CIDR que celle que vous avez pour votre règle du port 22 SSH.
- Pour les règles entrantes pour le groupe de sécurité, configurez le trafic FTP et FTPS pour utiliser la plage de ports **21** pour le canal de contrôle et **8192-8200** pour le canal de données.

 Note

Vous pouvez également utiliser le port 2223 pour les clients qui ont besoin d'ACKS TCP « superposés », ou de la possibilité pour le pack final de la prise de contact tridirectionnelle TCP de contenir également des données.

Certains logiciels clients peuvent être incompatibles avec le port 2223 : par exemple, un client qui demande au serveur d'envoyer la chaîne d'identification SFTP avant que le client ne le fasse.

VPC > Security Groups > sg-[redacted]-default > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info
sg-[redacted]	HTTP
sg-[redacted]	RDP
sg-[redacted]	HTTPS
sg-[redacted]	Custom TCP
sg-[redacted]	SSH

[Add rule](#)

- f. (Facultatif) Pour FIPS Enabled, cochez la case FIPS Enabled endpoint pour vous assurer que le endpoint est conforme aux Federal Information Processing Standards (FIPS).

Note

FIPS-enabled les points de terminaison ne sont disponibles que dans les AWS régions d'Amérique 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 la norme FIPS, consultez la [norme fédérale de traitement de l'information \(FIPS\) 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 créer automatiquement le rôle IAM, à condition que vous disposiez des autorisations nécessaires pour créer un nouveau rôle. Le rôle IAM créé est appelé `AWSTransferLoggingAccess`.
 - Choisissez un rôle existant pour choisir un rôle IAM existant dans votre compte. Sous Rôle de journalisation, choisissez le rôle. Ce rôle IAM 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-2024-01` 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 serveurs](#).

- c. (Facultatif : cette section concerne uniquement la migration des utilisateurs depuis un SFTP-enabled serveur existant.) Pour la clé d'hôte du serveur, entrez une clé privée RSA, ED25519 ou ECDSA qui sera utilisée pour identifier votre serveur lorsque des clients s'y connecteront via SFTP.
 - 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 les fichiers, mais vous devez d'abord créer un utilisateur. Pour plus de détails sur la création d'utilisateurs, consultez [Gestion des utilisateurs pour les points de terminaison du serveur](#).

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 le groupe de sécurité par défaut de votre VPC. 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

Seuls les protocoles SFTP et FTPS peuvent être utilisés sur un point de terminaison hébergé par un VPC 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-enabled serveur](#).
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.

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 Gestion des identités et des accès AWS (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 hébergé par VPC 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 console VPC (<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 [Configuration d'Amazon Route 53 avec vos AWS GovCloud \(US\) ressources](#) dans le Guide de l'AWS GovCloud (US) utilisateur.

- Alias DNS 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 fournisseur DNS. 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 le VPC, choisissez un ID de VPC existant ou choisissez Create a VPC pour créer un nouveau VPC.
- e. Dans la section Zones de disponibilité, choisissez jusqu'à trois zones de disponibilité et les sous-réseaux associés. Pour les adresses IPv4, 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.

Conseil : Vous devez utiliser un sous-réseau public pour vos zones de disponibilité ou configurer d'abord une passerelle Internet si vous souhaitez utiliser un sous-réseau privé.

- f. Dans la section Groupes de sécurité, choisissez un ou plusieurs ID de groupe de sécurité existants 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 pour votre 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

Votre VPC est associé automatiquement 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 entrantes pour le groupe de sécurité, vous pouvez configurer le trafic SSH pour qu'il utilise les ports 22, 2222, 22000 ou une combinaison des deux. Le port 22 est configuré par défaut. Pour utiliser le port 2222 ou le port 22000, vous devez ajouter une règle entrante à votre groupe de sécurité. Pour le type, choisissez TCP personnalisé, puis entrez l'une **2222** ou **22000** l'autre plage de ports, et pour la source, entrez la même plage d'adresses CIDR que celle que vous avez pour votre règle du port 22 SSH.
- Pour les règles entrantes pour le groupe de sécurité, configurez le trafic FTPS pour utiliser la plage de ports **21** pour le canal de contrôle et **8192-8200** pour le canal de données.

 Note

Vous pouvez également utiliser le port 2223 pour les clients qui ont besoin d'ACKS TCP « superposés », ou de la possibilité pour le pack final de la prise de contact tridirectionnelle TCP de contenir également des données.

Certains logiciels clients peuvent être incompatibles avec le port 2223 : par exemple, un client qui demande au serveur d'envoyer la chaîne d'identification SFTP avant que le client ne le fasse.

[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.

Inbound rules Info

Security group rule ID	Type Info
sgr- 	HTTP
sgr- 	RDP
sgr- 	HTTPS
sgr- 	Custom TCP
sgr- 	SSH

Add rule

- g. (Facultatif) Pour FIPS Enabled, cochez la case FIPS Enabled endpoint pour vous assurer que le endpoint est conforme aux Federal Information Processing Standards (FIPS).

 Note

FIPS-enabled les points de terminaison ne sont disponibles que dans les AWS régions d'Amérique 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 la norme FIPS, consultez la [norme fédérale de traitement de l'information \(FIPS\) 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 créer automatiquement le rôle IAM, à condition que vous disposiez des autorisations nécessaires pour créer un nouveau rôle. Le rôle IAM créé est appelé `AWSTransferLoggingAccess`.
 - Choisissez un rôle existant pour choisir un rôle IAM existant dans votre compte. Sous Rôle de journalisation, choisissez le rôle. Ce rôle IAM 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-2024-01` 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 serveurs](#).

- c. (Facultatif : cette section concerne uniquement la migration des utilisateurs depuis un SFTP-enabled serveur existant.) Pour la clé d'hôte du serveur, entrez une clé privée RSA, ED25519 ou ECDSA qui sera utilisée pour identifier votre serveur lorsque des clients s'y connecteront via SFTP.
- 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 les ID de flux de travail (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 **Adresse IPv4 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 dans un VPC est en ligne, seuls les sous-réseaux peuvent être modifiés et uniquement via l'API. [UpdateServer](#) 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 terminaison VPC.

 Note

Si un serveur existant dans un VPC est affiché sous la forme `VPC_ENDPOINT`, nous vous recommandons de le modifier pour le nouveau type de point de terminaison VPC. 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 de sécurité VPC 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 le type de point de terminaison public actuel ou 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 VPC hébergé.
 - 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 console VPC (<https://console.aws.amazon.com/vpc/>) pour allouer une ou plusieurs nouvelles adresses IP Elastic. 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 :

- Alias DNS 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 fournisseur DNS. 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 le VPC, choisissez un ID de VPC existant ou choisissez Create a VPC pour 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 console VPC () <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 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 point de terminaison public par un point de terminaison VPC, 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](#).

Arrêt de l'utilisation de VPC_ENDPOINT

AWS Transfer Family a cessé de permettre la création de 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, consultez [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 AWS Transfer Family la section « [SFTP prend en charge les groupes de sécurité VPC et les adresses IP élastiques](#) ». Ce nouveau point de terminaison est plus riche en fonctionnalités et plus rentable, et il est PrivateLink gratuit. Pour en savoir plus, consultez [Pricing AWS PrivateLink](#) (Tarification).

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 l'adresse IP autorisée AWS Transfer Family pour sécuriser votre accès aux serveurs SFTP](#).

Vous pouvez également héberger ce point de terminaison dans un environnement VPC partagé. Pour plus d'informations, voir [Supporte AWS Transfer Family désormais les environnements VPC à services partagés](#).

Outre le SFTP, vous pouvez utiliser le `EndpointType VPC` pour activer FTPS et FTP. Nous n'avons pas l'intention d'ajouter ces fonctionnalités et FTPS/FTP cette assistance

àEndpointType=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, de l'API, des SDK ou 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 ni le support FTPS ou FTP 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.

Limiter l'accès aux points de terminaison VPC pour les serveurs Transfer Family

Lorsque vous créez un AWS Transfer Family serveur avec un type de point de terminaison VPC, vos utilisateurs et principaux IAM ont besoin d'autorisations pour créer et supprimer des points de terminaison VPC. Toutefois, les politiques de sécurité de votre organisation peuvent restreindre ces autorisations. Vous pouvez utiliser les politiques IAM pour autoriser la création et la suppression de points de terminaison VPC spécifiquement pour Transfer Family tout en maintenant les restrictions pour les autres services.

Important

La politique IAM suivante permet aux utilisateurs de créer et de supprimer des points de terminaison VPC uniquement pour les serveurs Transfer Family, tout en refusant ces opérations pour les autres services :

```
{
  "Effect": "Deny",
  "Action": [
```

```

        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
    ],
    "Resource": ["*"],
    "Condition": {
        "ForAnyValue:StringNotLike": {
            "ec2:VpceServiceName": [
                "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
            ]
        },
        "StringNotLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
            ]
        }
    }
}

```

INPUT-YOUR-REGION Remplacez-le par votre AWS région (par exemple **us-east-1**) et *INPUT-YOUR-ROLE* par le rôle IAM auquel vous souhaitez accorder ces autorisations.

Fonctionnalités réseau supplémentaires

AWS Transfer Family fournit plusieurs fonctionnalités réseau avancées qui améliorent la sécurité et la flexibilité lors de l'utilisation de configurations VPC :

- Support de l'environnement VPC partagé : vous pouvez héberger le point de terminaison de votre serveur Transfer Family dans un environnement VPC partagé. Pour plus d'informations, consultez la section [Utilisation de points de terminaison hébergés par des VPC dans des VPC partagés avec AWS Transfer Family](#)
- Authentification et sécurité : vous pouvez utiliser un pare-feu d'application AWS Web pour protéger votre point de terminaison Amazon API Gateway. Pour plus d'informations, consultez [Sécurisation AWS Transfer Family avec AWS le Web Application Firewall et Amazon API Gateway](#).

Mise à jour du type de point de terminaison du AWS Transfer Family serveur de VPC_ENDPOINT à VPC

Vous pouvez utiliser l'API AWS Management Console CloudFormation, ou l'API Transfer Family pour mettre à jour le fichier 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 CloudFormation](#)
- [Mettre à jour le serveur `EndpointType` à l'aide de l'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 opérations d'[ListServers](#) API Amazon EC2 [DescribeRegions](#) et Transfer Family. Si vous avez de nombreux AWS comptes, vous pouvez les parcourir en utilisant un rôle IAM 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 VPC hébergé 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 CloudFormation

Cette section décrit comment procéder pour mettre CloudFormation à jour celui d'un serveur EndpointType versVPC. Utilisez cette procédure pour les serveurs Transfer Family que vous avez déployés avec CloudFormation. Dans cet exemple, le 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 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 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 la ressource VPCEndpoint sera supprimée. Le serveur de type point de terminaison VPC crée un point de terminaison VPC en votre nom, en remplacement de la ressource d'origine. VPCEndpoint

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 CloudFormation, puis sélectionnez Démarrer dans le menu Actions.

Mettre à jour le serveur EndpointType à l'aide de l'API

Vous pouvez utiliser la commande [describe-server](#) ou la AWS CLI commande [UpdateServer](#) API. L'exemple de script suivant arrête le serveur Transfer Family, le met à jour 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 `quemysftpserver.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 service DNS qui prend en charge AWS Transfer Family nativement.

Rubriques

- [Utilisez Amazon Route 53 comme fournisseur DNS](#)
- [Utiliser d'autres fournisseurs DNS](#)
- [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 :

- Alias DNS 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 fournisseur DNS. 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-enabled serveur](#). 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 fournisseur DNS

Lorsque vous créez un serveur, vous pouvez utiliser Amazon Route 53 comme fournisseur DNS. 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 guide du développeur Amazon Route 53.

Lorsque vous utilisez Route 53 pour fournir un routage DNS à votre serveur, AWS Transfer Family utilise le nom d'hôte personnalisé que vous avez saisi pour extraire sa zone hébergée. Lors de AWS Transfer Family 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. Un enregistrement CNAME est un autre nom de domaine.
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'enregistrement CNAME par le nom d'hôte de votre serveur.

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 fournisseurs DNS

Lorsque vous créez un serveur, vous pouvez également utiliser des fournisseurs DNS autres qu'Amazon Route 53. Si vous utilisez un autre fournisseur DNS, vous devez veiller à ce que le trafic en provenance de votre domaine soit 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.

- Pour les points de terminaison IPv4, le nom d'hôte ressemble à ceci dans la console :

`serverid.server.transfer.region.amazonaws.com`

- Pour les points de terminaison à double pile, le nom d'hôte ressemble à ceci dans la console :

`serverid.transfer-server.region.on.aws`

Note

Si votre serveur possède un point de terminaison VPC, le format du nom d'hôte est différent de celui décrit ci-dessus. Pour trouver votre point de terminaison VPC, sélectionnez le VPC sur la page de détails du serveur, puis sélectionnez l'ID du point de terminaison VPC sur le tableau de bord du VPC. Le point de terminaison est le premier nom DNS de ceux répertoriés.

Noms d'hôte personnalisés pour les serveurs créés sans console

Lorsque vous créez un serveur à l'aide AWS Cloud Development Kit (AWS CDK) ou via la CLI, vous devez ajouter une balise si vous souhaitez que ce serveur possède un nom d'hôte personnalisé. 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 enregistrement DNS 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 fournisseur DNS, 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 commande CLI 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 leurs identifiants 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/>.

Considérations relatives aux Network Load Balancer FTP et FTPS

Bien que nous vous recommandions d'éviter les équilibreurs de charge réseau placés devant AWS Transfer Family les serveurs, si votre implémentation FTP ou FTPS nécessite un NLB ou un NAT dans la route de communication en provenance du client, suivez les recommandations suivantes :

- Pour un NLB, utilisez le port 21 pour les contrôles de santé, au lieu des ports 8192-8200.
- Pour le AWS Transfer Family serveur, activez la reprise de session TLS en `TlsSessionResumptionMode = ENFORCED` configurant.

 Note

Il s'agit du mode recommandé, car il offre une sécurité renforcée :

- Exige que les clients utilisent la reprise de session TLS pour les connexions suivantes.
- Fournit des garanties de sécurité renforcées en garantissant des paramètres de chiffrement cohérents.
- Aide à prévenir les attaques de rétrogradation potentielles.
- Maintient la conformité aux normes de sécurité tout en optimisant les performances.

- Si possible, évitez d'utiliser un NLB pour tirer pleinement parti des limites de AWS Transfer Family performances et de connexion.

Pour obtenir des conseils supplémentaires sur les alternatives NLB, contactez l'équipe de gestion des AWS Transfer Family produits via le AWS Support. Pour plus d'informations sur l'amélioration de votre niveau de sécurité, consultez le billet de blog [Six conseils pour améliorer la sécurité de votre AWS Transfer Family serveur](#).

Les directives de sécurité pour les NLB sont fournies dans. [Évitez de placer les NLB et les NAT devant AWS Transfer Family serveurs](#)

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 protocole SFTP.
- OpenSSH (macOS et Linux)

 Note

Ce client fonctionne uniquement avec les serveurs qui sont activés pour le protocole de transfert de fichiers (SFTP) Secure Shell (SSH).

- WinSCP (Microsoft Windows uniquement)

- Cyberduck (Windows, macOS et Linux)
- FileZilla (Windows, macOS et Linux)

Les restrictions suivantes s'appliquent à tous les clients :

- Le protocole SCP n'est pas pris en charge, car il est considéré comme non sécurisé. Vous pouvez utiliser la commande `scp` OpenSSH comme décrit dans [Utilisation de la commande scp](#)
- Le nombre maximum de sessions SFTP multiplexées simultanées par connexion est de 10.
- Pour les connexions inactives, le délai d'expiration est de 1 800 secondes (30 minutes) pour tous les protocoles (SFTP/FTP/FTPS). S'il n'y a aucune activité après cette période, le client peut être déconnecté. Pour les connexions qui ne répondent pas :
 - Le protocole SFTP a un délai d'expiration de 300 secondes (5 minutes) lorsqu'un client ne répond pas du tout.
 - Les protocoles FTPS et FTP ont un délai d'attente d'environ 10 minutes qui est géré par la bibliothèque sous-jacente.
- Amazon S3 et Amazon EFS (en raison du protocole NFSv4) nécessitent que les noms de fichiers soient encodés. 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 via SSL (FTPS), seul le mode explicite est pris en charge. Le mode implicite n'est pas pris en charge.
- Pour le protocole de transfert de fichiers (FTP) et le FTPS, seul le mode passif est pris en charge.
- Pour les protocoles FTP et FTPS, seul le mode STREAM est pris en charge.
- Pour les protocoles FTP et FTPS, seul le Image/Binary mode est pris en charge.
- Pour le FTP et le FTPS, le protocole TLS - PROT C (non protégé) est le protocole TLS par défaut pour la connexion aux données, mais le protocole FTPS ne prend pas en charge le protocole PROT C. AWS Transfer Family Donc, pour FTPS, vous devez émettre un 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 prend en charge plusieurs connexions pour un seul transfert.

Voici une liste des commandes disponibles pour FTP et FTPS :

Commandes disponibles					
LABOR	EXPLOIT	LE PLUS	PASSER	RETR	TEMPÊTE
AUTH	LANG	MKD	PASV	RMD	STOU
CDUP	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PORT	RNTO	SYST
DELE	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	OPTE	SORTIR	STAT	USER

 Note

APPE n'est pas pris en charge.

Pour le SFTP, les opérations suivantes ne sont actuellement pas prises en charge pour les utilisateurs qui utilisent le répertoire de base logique sur des serveurs utilisant Amazon Elastic File System (Amazon EFS).

Commandes SFTP non prises en charge			
SSH_FXP_R EADLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT lorsque le fichier demandé est un lien symbolique	SSH_FXP_R EALPATH 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 clés SSH pour les utilisateurs gérés par des services](#).

Rubriques

- [SFTP/FTPS/FTP Commandes disponibles](#)
- [Trouvez votre point de terminaison Amazon VPC](#)
- [Évitez les setstat erreurs](#)
- [Utiliser OpenSSH](#)
- [Utiliser WinSCP](#)
- [Utilisez Cyberduck](#)
- [Utiliser FileZilla](#)
- [Utiliser un client Perl](#)
- [Utiliser le LFTP](#)
- [Traitement après le téléchargement](#)
- [Messages SFTP](#)

SFTP/FTPS/FTP Commandes disponibles

Le tableau suivant décrit les commandes disponibles pour AWS Transfer Family, pour les protocoles SFTP, FTPS et FTP.

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

Commande	Amazon S3	Amazon EFS
cd	Pris en charge	Pris en charge

Commande	Amazon S3	Amazon EFS
chgrp	Non pris en charge	Supporté (root 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
ls/dir	Pris en charge	Pris en charge
mkdir	Pris en charge	Pris en charge
put	Pris en charge	Pris en charge
pwd	Pris en charge	Pris en charge
rename	Pris en charge uniquement pour les fichiers  Note Le changement de nom qui remplacerait un fichier existant n'est pas pris en charge.	Pris en charge  Note Le changement de nom qui remplacerait un fichier ou un répertoire existant n'est pas pris en charge.
rm	Pris en charge	Pris en charge

Commande	Amazon S3	Amazon EFS
<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 terminaison Amazon VPC

Si le type de point de terminaison de votre serveur Transfer Family est VPC, il n'est pas facile d'identifier le point de terminaison à utiliser pour le transfert de fichiers. Dans ce cas, utilisez la procédure suivante pour trouver votre point de terminaison Amazon VPC.

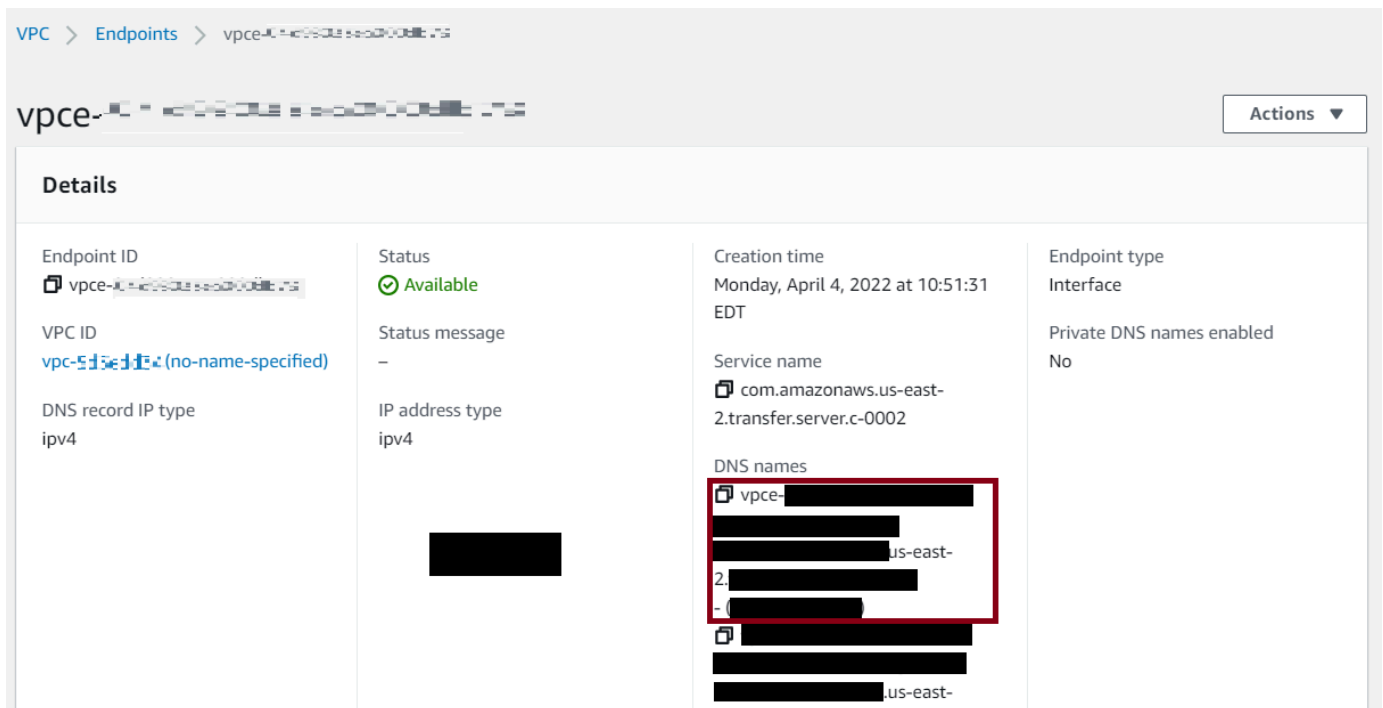
Pour trouver votre point de terminaison Amazon VPC

1. Accédez à la page de détails de votre serveur.
2. Dans le volet 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 bord Amazon VPC, sélectionnez l'ID du point de terminaison VPC.
4. Dans la liste des noms DNS, le point de terminaison de votre serveur est le premier répertorié.



Évitez les **setstat** erreurs

Certains clients de transfert de fichiers SFTP peuvent tenter de modifier les attributs des fichiers distants, notamment l'horodatage et les autorisations, à l'aide de commandes telles que SETSTAT lors du téléchargement du 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 l'UpdateServerAPI CreateServer or, utilisez l'ProtocolDetailsoption SetStatOption permettant d'ignorer l'erreur générée lorsque le client tente d'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 commande SETSTAT et charge des fichiers sans avoir à apporter de modifications à votre client SFTP.
- 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 effectue un appel SETSTAT.

Pour les détails de l'API relatifs à cette option, consultez [ProtocolDetails](#).

Utiliser OpenSSH

Cette section contient des instructions pour transférer des fichiers depuis la ligne de commande à l'aide d'OpenSSH.

Note

Ce client fonctionne uniquement avec un SFTP-enabled serveur.

Rubriques

- [Utilisation d'OpenSSH](#)
- [Utilisation de la commande scp](#)

Utilisation d'OpenSSH

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

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 privée SSH. *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. À moins que vous n'ayez déjà modifié ce fichier, le protocole 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 ou le port 22000, 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 /amzn-s3-demo-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 service DNS de votre environnement.

Utilisation de la commande **scp**

Transfer Family ne prend pas en charge le protocole SCP. Toutefois, vous pouvez utiliser la commande `scp` OpenSSH si vous avez besoin de cette fonctionnalité.

Pour utiliser SCP sur SFTP, il est recommandé d'utiliser OpenSSH version 9.0 ou ultérieure. Dans les versions 9 et ultérieures d'OpenSSH, `scp` la commande utilise par défaut le protocole SFTP pour les transferts de fichiers au lieu de l'ancien protocole SCP.

 Important

Assurez-vous que votre serveur Transfer Family a été configuré pour utiliser l'accès aux annuaires optimisé S3.

Utiliser WinSCP

Suivez les instructions ci-dessous pour transférer des fichiers depuis la ligne de commande en utilisant WinSCP.

 Note

Si vous utilisez WinSCP 5.19, vous pouvez vous connecter directement à Amazon S3 à l'aide AWS de vos informations d'identification et de vos fichiers. upload/download Pour plus de détails, consultez [Connexion au service Amazon S3](#).

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

1. Ouvrez le client WinSCP.
2. Dans la boîte de dialogue de connexion, pour Protocole de fichier, choisissez un protocole : SFTP ou FTP.

Si vous avez choisi FTP, pour le chiffrement, choisissez l'une des options suivantes :

- Pas de cryptage pour le FTP
- TLS/SSL Chiffrement 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 les détails des serveurs SFTP, FTPS et FTP](#).

Si votre serveur utilise un point de terminaison VPC, consultez. [Trouvez votre point de terminaison Amazon VPC](#)

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.

Conseil : 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 de AWS Directory Service pour Microsoft Active Directory](#)
- [Travailler avec des fournisseurs d'identité personnalisés](#)

6. Choisissez Avancé pour ouvrir la boîte de dialogue Paramètres avancés du site. Dans la section SSH, choisissez Authentification.
7. Pour le fichier de clé privée, recherchez et sélectionnez le fichier de clé privée SSH dans votre système de fichiers.

Si WinSCP propose de convertir votre clé privée SSH au format PPK, 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 le transfert resume/transfer vers un nom de fichier temporaire pour, choisissez Désactiver.

 Important

Si vous laissez cette option activée, cela augmente les coûts de téléchargement, ce qui réduit 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.

Conseil : 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 les méthodes glisser-déposer pour copier des fichiers entre la fenêtre cible et la fenêtre 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'horodatage WinSCP (ou à les utiliser comme décrit [Évitez les setstat erreurs](#) dans) avant d'effectuer des transferts de fichiers. Pour ce faire, dans la boîte de dialogue des paramètres de WinSCP 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 fichiers SSH), FTP-SSL(Explicit AUTH TLS) 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 les détails des serveurs SFTP, FTPS et FTP](#).

Si votre serveur utilise un point de terminaison VPC, consultez. [Trouvez votre point de terminaison Amazon VPC](#)

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 est sélectionné, pour la clé privée SSH, choisissez ou entrez la clé privée SSH.
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 le chiffrement, choisissez l'une des options suivantes :

- Utilisez uniquement le protocole FTP ordinaire (non sécurisé) — pour le FTP
 - Utilisez le protocole FTP explicite sur TLS, si disponible, pour le protocole 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 les détails des serveurs SFTP, FTPS et FTP](#).

- Si vous utilisez le protocole SFTP, entrez : `sftp://hostname`
- Si vous utilisez le protocole FTPS, entrez : `ftps://hostname`

Assurez-vous de le remplacer par le point *hostname* de terminaison de votre serveur actuel.

Si votre serveur utilise un point de terminaison VPC, consultez. [Trouvez votre point de terminaison Amazon VPC](#)

6. Pour le numéro de port, entrez ce qui suit :

- **22**pour SFTP
- **21**pour FTP/FTPS

7. Si SFTP est sélectionné, pour Type d'ouverture de session, choisissez Fichier clé.

Pour Fichier clé, choisissez ou entrez la clé privée SSH.

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](#).

Utiliser le LFTP

LFTP est un client FTP gratuit qui permet aux utilisateurs d'effectuer des transferts de fichiers via l'interface de ligne de commande depuis la plupart des machines Linux.

Pour les téléchargements de fichiers volumineux, le protocole LFTP présente un problème connu lié aux paquets hors service, ce qui entraîne l'échec du transfert de fichiers.

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.

Key	Value
Content-Type	text/plain
x-amz-meta-user-agent	AWSTransfer
x-amz-meta-user-agent-id	sftp_user@s-

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 Identifiant]/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 rôle IAM 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 Gestion des identités et des accès AWS (IAM), consultez la section Identifiants [uniques du guide](#) de l'Gestion des identités et des accès AWS utilisateur.

Messages SFTP

Cette section décrit les messages côté client que vous pouvez recevoir pendant ou après vos transferts de fichiers SFTP lorsque vous utilisez un serveur Transfer Family. Pour plus d'informations sur un événement SFTP, consultez les journaux de vos clients SFTP. Vous pouvez utiliser ces informations pour résoudre d'éventuelles erreurs ou les transmettre à votre équipe réseau afin qu'elle vous aide à identifier le problème.

Messages SFTP côté client

Activité	Description
AUTH_FAILURE	L'utilisateur a échoué à s'authentifier. Il peut s'agir de n'importe quel type de défaillance provenant d'un fournisseur d'identité personnel ou d'un utilisateur géré par un service. Les détails de l'événement aident à clarifier la cause première de l'échec.
CLOSE	Indique qu'un fichier ou un répertoire ouvert est correctement fermé.
CONNECTED/DISCONNECTED	Indique le succès normal de la connexion et les déconnexions.
CRÉER_SYMLINK	Un lien symbolique a été créé (avec ou sans succès).
DELETE	Un fichier a été supprimé (avec ou sans succès).
ERROR	Une erreur générale et inattendue. La description associée contient des informations qui peuvent vous aider, vous ou vos administrateurs réseau, à identifier le problème spécifique.
RAISON_DE SORTIE	Émis lorsqu'une erreur inattendue a entraîné la fin de votre session SFTP. Le message associé à l'événement décrit la cause.
MKDIR	Un répertoire a été créé (avec ou sans succès).
OPEN	Un fichier a été ouvert en lecture ou en écriture (avec ou sans succès)
FERMETURE PARTIELLE	Le client s'est déconnecté du serveur alors qu'un fichier était encore ouvert et aucun

Activité	Description
	message CLOSE n'a été reçu. Transfer Family stocke la partie reçue du fichier (qui peut en fait être le fichier complet) et émet l'événement PARTIAL_CLOSE pour avertir le client du problème. L'intégration des flux de travail reçoit également un onPartialClose événement pour gérer le fichier de manière appropriée.
RENAME	Un fichier a été renommé (avec ou sans succès)
RMDIR	Un répertoire a été supprimé (avec ou sans succès)
SETSTAT	Les attributs d'un fichier sont modifiés (avec ou sans succès).
	 Note Transfer Family ne prend pas en charge SETSTAT si vous utilisez Amazon S3 pour le stockage. La Évitez les setstat erreurs section fournit des détails sur la manière d'éviter SetStat les erreurs en désactivant le paramètre . Cela vous évite de recevoir un fail unsupported error : au lieu de cela, vous recevez success but do nothing un message.
TLS_RESUME_FAILURE	Le serveur est configuré pour appliquer la reprise de session TLS et le client ne le prend pas en charge.

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.

Vous pouvez également stocker la clé publique SSH (Secure Shell) dans les propriétés de chaque utilisateur. Cela est nécessaire pour l'authentification par clé. La clé privée est stockée localement sur l'ordinateur de votre utilisateur. Lorsque votre utilisateur envoie une demande d'authentification à votre serveur via un client, celui-ci confirme d'abord que l'utilisateur a accès à la clé privée SSH associée. Le serveur authentifie ensuite correctement l'utilisateur.

Note

Pour le déploiement et la gestion automatisés des utilisateurs utilisant plusieurs clés SSH, consultez [Modules Transfer Family Terraform](#).

En outre, vous spécifiez le répertoire personnel, ou répertoire de destination, d'un utilisateur et vous lui attribuez un rôle Gestion des identités et des accès AWS (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 des serveurs SFTP. 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.

Comparaison entre Amazon EFS et 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 identifiants d'utilisateur, de groupe et de groupe secondaire POSIX
- Les deux public/private touches de support

- Les deux prennent en charge les répertoires personnels
- Les deux prennent en charge les répertoires logiques

Note

Pour Amazon S3, l'essentiel de la prise en charge des annuaires logiques se fait 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`.

AWS Transfer Family prend en charge la spécification d'une `HomeDirectory` valeur lors de l'utilisation du `LOGICAL HomeDirectoryType`. Cela s'applique aux utilisateurs gérés par le service, à l'accès à Active Directory et aux implémentations de fournisseurs d'identité personnalisés lorsque `HomeDirectoryDetails` ceux-ci sont fournis dans la réponse.

Important

Lorsque vous spécifiez a `HomeDirectory` avec `LOGICAL HomeDirectoryType`, la valeur doit correspondre à l'un de vos mappages de répertoires logiques. Le service valide cela lors de la création et des mises à jour des utilisateurs afin d'éviter que les configurations ne fonctionnent pas.

Comportement par défaut

Par défaut, s'il n'est pas spécifié, HomeDirectory il est défini sur «/» pour le mode LOGIQUE. Ce comportement est inchangé et reste compatible avec les définitions utilisateur existantes.

- Assurez-vous de faire correspondre votre entrée HomeDirectory à une entrée et non à une cible. Pour en savoir plus, consultez [Règles d'utilisation des répertoires logiques](#).
- Pour plus de détails sur la structure d'un répertoire virtuel, voir [Structure du répertoire virtuel](#).

Considérations relatives au fournisseur d'identité personnalisé

Lorsque vous utilisez un fournisseur d'identité personnalisé, vous pouvez désormais spécifier un HomeDirectory dans la réponse lorsque vous utilisez LOGICAL HomeDirectoryType. L'appel TestIdentityProvider d'API produira des résultats corrects lorsque l'IDP personnalisé spécifie un HomeDirectory en mode LOGIQUE.

Exemple de réponse IDP personnalisée avec HomeDirectory et LOGICAL HomeDirectoryType :

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectory": "/marketing",
  "HomeDirectoryDetails": "[{\"Entry\":\"\\\\\\\\\", \"Target\":\"\\\\\\\\/bucket/home\\\\\\\\\"}, {\"Entry\":\"\\\\\\\\/marketing\\\\\\\\\", \"Target\":\"\\\\\\\\/marketing-bucket/campaigns\\\\\\\\\"}]"
}
```

Quotas de groupe Active Directory

AWS Transfer Family a une limite par défaut de 100 groupes Active Directory par serveur. Si votre cas d'utilisation nécessite plus de 100 groupes, envisagez d'utiliser une solution de fournisseur d'identité personnalisée, comme décrit dans [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

Cette limite s'applique aux serveurs utilisant les fournisseurs d'identité suivants :

- AWS Service d'annuaire pour Microsoft Active Directory
- AWS Service d'annuaire pour les services de domaine Entra ID

Si vous devez demander une augmentation de la limite de service, consultez [Service AWS les quotas](#) dans le Références générales AWS. Si votre cas d'utilisation nécessite plus de 100 groupes, envisagez d'utiliser une solution de fournisseur d'identité personnalisée, comme décrit dans [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

Pour obtenir des informations de dépannage relatives aux limites de groupe Active Directory, consultez [Limites de groupe Active Directory dépassées](#).

Rubriques

- [Travailler avec des utilisateurs gérés par des services](#)
- [Travailler avec des fournisseurs d'identité personnalisés](#)
- [Utilisation de AWS Directory Service pour Microsoft Active Directory](#)
- [Utilisation du AWS Directory Service pour les services de domaine Entra ID](#)

Travailler avec des utilisateurs gérés par des services

Vous pouvez ajouter des utilisateurs gérés par le service Amazon S3 ou Amazon EFS à votre serveur, en fonction du paramètre de domaine du serveur. Pour de plus amples informations, veuillez consulter [Configuration d'un point de terminaison de serveur SFTP, FTPS ou FTP](#).

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.

Pour ajouter un utilisateur géré par un service par programmation, consultez l'[exemple](#) de l'API. [CreateUser](#)

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 service Amazon EFS](#)
- [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 se trouvant 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, 0—9 A-Z, trait de soulignement « _ », tiret « - », point « . » et signe « @ ». Le nom d'utilisateur ne peut pas commencer par un tiret « - », un point « . » ou par le signe « @ ».
5. Pour Access, choisissez le rôle IAM que vous avez créé précédemment et qui donne accès à votre compartiment Amazon S3.

Vous avez créé ce rôle IAM à l'aide de la procédure décrite dans [Création d'un rôle et d'une politique IAM](#). Ce rôle IAM inclut une politique IAM qui permet d'accéder à votre compartiment Amazon S3. Cela inclut également une relation de confiance avec le AWS Transfer Family service, définie dans une autre politique IAM. 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 dans IAM : vous permet de choisir une stratégie de session existante. Choisissez View pour voir un objet JSON contenant les détails de la politique.
- Auto-generate stratégie basée sur le dossier d'accueil : génère une politique de session pour vous. Choisissez View pour voir un objet JSON contenant les détails de la politique.

 Note

Si vous choisissez une Auto-generate politique basée sur le dossier de base, ne sélectionnez pas Restreint pour cet utilisateur.

Pour en savoir plus sur les politiques de session [Création d'un rôle et d'une politique IAM](#), consultez [Création d'une politique de session pour un compartiment Amazon S3](#), ou [Approches dynamiques de gestion des autorisations](#).

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, vérifiez que votre rôle IAM donne accès à ce répertoire root.

 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 de Auto-generate stratégie basée sur le dossier de base, car le dossier de base n'est pas une valeur définie pour les utilisateurs restreints.

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

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 clés SSH, consultez [Génération de clés SSH 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 service Amazon EFS

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

- Pour plus d'informations sur la propriété des fichiers Amazon EFS, consultez la section [Propriété des fichiers Amazon EFS](#).
- Pour plus de détails sur la configuration de répertoires pour vos utilisateurs EFS, consultez [Configurer les utilisateurs Amazon EFS pour Transfer Family](#).

Pour ajouter un utilisateur géré par le service Amazon EFS 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 serveur Amazon EFS 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, 0—9 A-Z, 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 Amazon EFS.
 - Pour les utilisateurs supplémentaires, entrez l'ID utilisateur POSIX et l'ID de groupe de l'utilisateur. Ces identifiants 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 les identifiants de groupes secondaires, entrez un ou plusieurs identifiants de groupe POSIX supplémentaires pour chaque utilisateur, séparés par des virgules.
 - d. Pour Access, choisissez le rôle IAM qui :
 - Permet à l'utilisateur d'accéder uniquement aux ressources Amazon EFS (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 rôle IAM pour sélectionner le système de fichiers Amazon EFS avec accès au montage et read/write autorisations. 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 fichiers Amazon EFS 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 :
 - Les utilisateurs d'Amazon EFS ne peuvent accéder à aucun fichier ou répertoire en dehors de ce dossier.
 - Les utilisateurs d'Amazon EFS ne peuvent pas voir le nom du système de fichiers Amazon EFS (fs-xxxxxxx).

 Note

Lorsque vous sélectionnez l'option Restreint, les liens symboliques ne sont pas résolus pour les utilisateurs d'Amazon EFS.

- (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 fichiers Amazon EFS est utilisé. Dans ce cas, assurez-vous que votre rôle IAM donne accès à ce répertoire racine.

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

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 clés SSH, consultez [Génération de clés SSH 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 pouvez rencontrer lors de votre première connexion SFTP sur 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 pour consulter le répertoire personnel de l'utilisateur, le message suivant peut s'afficher, indiquant où se ***USER-HOME-DIRECTORY*** trouve le répertoire personnel de l'utilisateur SFTP :

```
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 publique SSH.

- [Afficher la liste des utilisateurs](#)
- [Afficher ou modifier les informations de l'utilisateur](#)
- [Suppression d'un utilisateur](#)
- [Ajouter une clé publique SSH](#)
- [Supprimer la clé publique SSH](#)

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 rôle IAM que vous avez créé précédemment et qui donne accès à votre compartiment Amazon S3.

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

7. (Facultatif) Dans le champ Politique, sélectionnez l'une des options suivantes :

- Aucun
- Politique existante
- Sélectionnez une politique dans IAM pour choisir une politique existante. Choisissez View pour voir un objet JSON contenant les détails de la politique.

Pour en savoir plus sur les règles de session, consultez [Création d'un rôle et d'une politique IAM](#). 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, vérifiez que votre rôle IAM donne accès à ce répertoire root.

 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 publique SSH 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 Add SSH public key (Ajouter une clé publique SSH) pour ajouter une nouvelle clé publique SSH à un utilisateur.

 Note

Les clés SSH ne sont utilisées que par les serveurs qui sont activés pour le protocole de transfert de fichiers (SFTP) Secure Shell (SSH). Pour plus d'informations sur la façon de générer une paire de clés SSH, consultez [Génération de clés SSH pour les utilisateurs gérés par des services](#).

6. Dans SSH public key (Clé publique SSH), entrez la partie clé publique SSH de la paire de clés SSH.

Votre clé est validée par le service avant que vous puissiez ajouter votre nouvel utilisateur. La clé SSH se présente sous la forme `ssh-rsa string`. Pour générer une paire de clés SSH, consultez [Génération de clés SSH pour les utilisateurs gérés par des services](#).

7. Sélectionnez Ajouter une clé.

Pour supprimer une clé publique SSH 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 la case correspondant à sa clé SSH et choisissez Supprimer.

Travailler avec des fournisseurs d'identité personnalisés

AWS Transfer Family propose plusieurs options permettant aux fournisseurs d'identité personnalisés d'authentifier et d'autoriser les utilisateurs pour des transferts de fichiers sécurisés. Voici les principales approches :

- [Solution de fournisseur d'identité personnalisée](#)—Cette rubrique décrit la solution de fournisseur d'identité personnalisé Transfer Family, à l'aide d'une boîte à outils hébergée dans GitHub.

Note

Dans la plupart des cas d'utilisation, il s'agit de l'option recommandée. Plus précisément, si vous devez prendre en charge plus de 100 groupes Active Directory, la solution de fournisseur d'identité personnalisé offre une alternative évolutive sans limitation de groupe. Cette solution est décrite dans le billet de blog intitulé [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

- [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#)—Cette rubrique décrit comment utiliser une AWS Lambda fonction pour soutenir une méthode Amazon API Gateway.

Vous pouvez fournir une interface RESTful 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'une 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 en savoir plus, consultez [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#).

- [Approches dynamiques de gestion des autorisations](#)—Cette rubrique décrit les approches permettant de gérer les autorisations des utilisateurs de manière dynamique à l'aide de politiques de session.

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 (Amazon EFS). Pour en savoir plus, 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.

- Transfer Family propose un article de blog et un atelier qui vous guideront dans la création d'une solution de transfert de fichiers. Cette solution s'appuie sur les SFTP/FTPS points de terminaison gérés et sur Amazon Cognito et DynamoDB AWS Transfer Family pour la gestion des utilisateurs.

Le billet de blog est disponible sur [Utilisation d'Amazon Cognito en tant que fournisseur d'identité avec Amazon AWS Transfer Family S3](#). Vous pouvez consulter les détails de l'atelier [ici](#).

Note

Pour les fournisseurs d'identité personnalisés, le nom d'utilisateur doit comporter au moins 3 caractères et au maximum 100 caractères. Vous pouvez utiliser les caractères suivants dans le nom d'utilisateur : a—z, 0—9 A-Z, trait de soulignement « _ », tiret « - », point « . » et le signe « @ ». Le nom d'utilisateur ne peut pas commencer par un tiret « - », un point « . » ou par le signe « @ ».

Lors de la mise en œuvre d'un fournisseur d'identité personnalisé, tenez compte des meilleures pratiques suivantes :

- Déployez la solution dans la même Compte AWS région que vos serveurs Transfer Family.

- Mettez en œuvre le principe du moindre privilège lors de la configuration des rôles et des politiques IAM.
- Utilisez des fonctionnalités telles que la liste des adresses IP autorisées et la journalisation standardisée pour renforcer la sécurité.
- Testez minutieusement votre fournisseur d'identité personnalisé dans un environnement hors production avant le déploiement.

Rubriques

- [Solution de fournisseur d'identité personnalisée](#)
- [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#)
- [Utilisation d'Amazon API Gateway pour intégrer votre fournisseur d'identité](#)
- [Utilisation de plusieurs méthodes d'authentification](#)
- [Support IPv6 pour les fournisseurs d'identité personnalisés](#)

Solution de fournisseur d'identité personnalisée

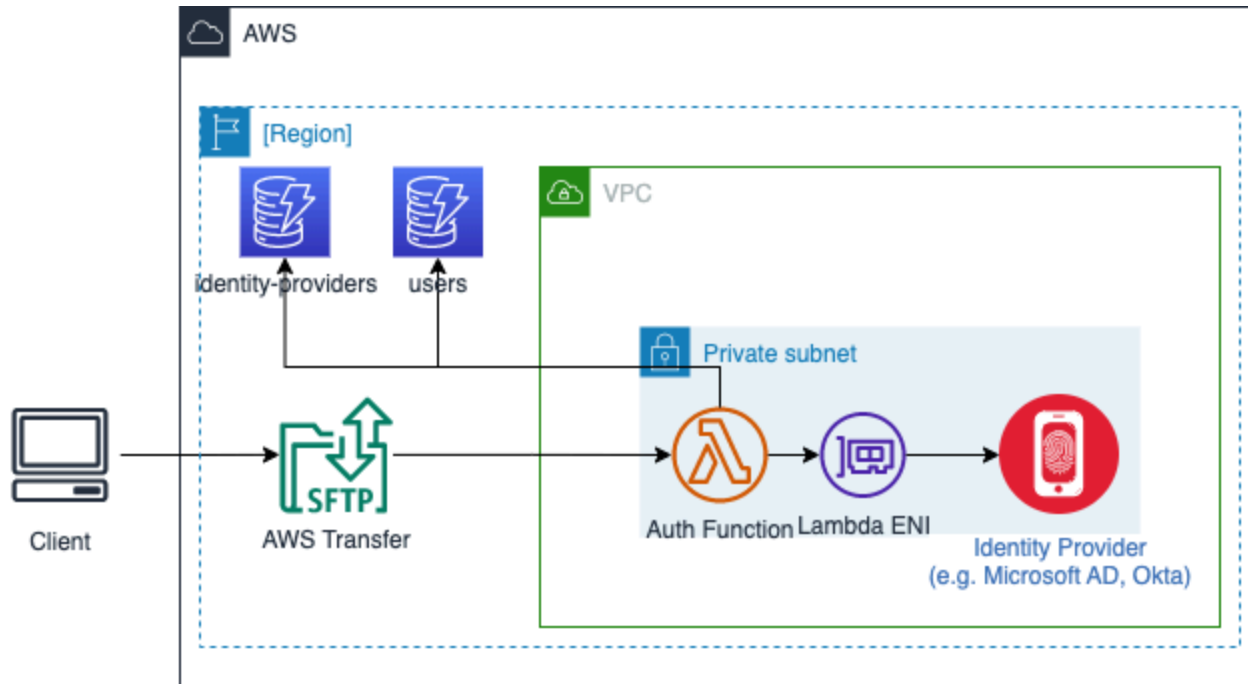
La solution de fournisseur d'identité AWS Transfer Family personnalisé est une solution modulaire de fournisseur d'identité personnalisé qui répond à de nombreux cas d'utilisation courants d'authentification et d'autorisation rencontrés par les entreprises lors de la mise en œuvre du service. Cette solution fournit une base réutilisable pour la mise en œuvre de fournisseurs d'identité personnalisés avec une configuration de session par utilisateur granulaire et sépare les logiques d'authentification et d'autorisation, offrant ainsi une base flexible et facile à entretenir pour divers cas d'utilisation.

Avec la solution de fournisseur d'identité AWS Transfer Family personnalisé, vous pouvez traiter les cas d'utilisation courants de l'authentification et de l'autorisation en entreprise. Cette solution modulaire offre :

- Une base réutilisable pour la mise en œuvre de fournisseurs d'identité personnalisés
- Configuration granulaire des sessions par utilisateur
- Logique d'authentification et d'autorisation séparées

Détails de mise en œuvre de la boîte à outils d'identité personnalisée

La solution fournit une base flexible et maintenable pour différents cas d'utilisation. Pour commencer, consultez le kit d'outils sur <https://github.com/aws-samples/toolkit-for-aws-transfer-family>, puis suivez les instructions de déploiement de la section [Getting started](#).



Note

Si vous avez déjà utilisé des modèles et des exemples de fournisseurs d'identité personnalisés, envisagez plutôt d'adopter cette solution. À l'avenir, les modules spécifiques aux fournisseurs seront standardisés sur cette solution. Une maintenance continue et des améliorations de fonctionnalités seront appliquées à cette solution.

Cette solution contient des modèles standard pour implémenter un fournisseur personnalisé qui prend en compte les détails, notamment la journalisation et l'endroit où stocker les métadonnées de session supplémentaires nécessaires AWS Transfer Family, telles que le `HomeDirectoryDetails` paramètre. Cette solution fournit une base réutilisable pour implémenter des fournisseurs d'identité personnalisés avec une configuration de session par utilisateur précise, et dissocie la logique d'authentification du fournisseur d'identité de la logique réutilisable qui crée une configuration qui est renvoyée à Transfer Family pour terminer l'authentification et établir les paramètres de la session.

Le code et les ressources de support de cette solution sont disponibles à l'adresse <https://github.com/aws-samples/toolkit-for-aws-transfer-family>.

La boîte à outils contient les fonctionnalités suivantes :

- Un [AWS Serverless Application Model](#) modèle qui fournit les ressources nécessaires. Vous pouvez éventuellement déployer et configurer Amazon API Gateway pour l'intégrer AWS WAF, comme décrit dans le billet de blog [Securing AWS Transfer Family with AWS Web Application Firewall and Amazon API Gateway](#).
- Un schéma [Amazon DynamoDB](#) pour stocker les métadonnées de configuration relatives aux fournisseurs d'identité, y compris les paramètres de session utilisateur HomeDirectoryDetails tels que Role, et. Policy
- Une approche modulaire qui vous permet d'ajouter de nouveaux fournisseurs d'identité à la solution à l'avenir, sous forme de modules.
- Récupération d'attributs : récupérez éventuellement les attributs du rôle IAM et du profil POSIX (UID et GID) auprès des fournisseurs d'identité pris en charge, notamment AD, LDAP et Okta.
- Support pour plusieurs fournisseurs d'identité connectés à un seul serveur Transfer Family et à plusieurs serveurs Transfer Family utilisant le même déploiement de la solution.
- Built-in Vérification des listes d'adresses IP autorisées, telles que les listes d'adresses IP autorisées qui peuvent éventuellement être configurées par utilisateur ou par fournisseur d'identité.
- Journalisation détaillée avec niveau de journalisation configurable et support de suivi pour faciliter le dépannage.

Avant de commencer à déployer la solution de fournisseur d'identité personnalisé, vous devez disposer des AWS ressources suivantes.

- Un Amazon Virtual Private Cloud (VPC) avec des sous-réseaux privés, avec une connectivité Internet via une passerelle NAT ou un point de terminaison de passerelle DynamoDB.
- Autorisations IAM appropriées pour effectuer les tâches suivantes :
 - Déployez le custom-idp.yaml CloudFormation modèle,
 - Créez des AWS CodePipeline projets
 - Créez des AWS CodeBuild projets
 - Création de rôles et de politiques IAM

⚠ Important

Vous devez déployer la solution sur celui-ci Compte AWS , Région AWS qui contient vos serveurs Transfer Family cibles.

Fournisseurs d'identité pris en charge

La liste suivante contient des informations sur les fournisseurs d'identité pris en charge par la solution de fournisseur d'identité personnalisée.

Fournisseur	Flux de mots de passe	Flux de clés publiques	Multi-factor	Récupération d'attributs	Détails
Active Directory et LDAP	Oui	Oui	Non	Oui	La vérification de l'utilisateur peut être effectuée dans le cadre du flux d'authentification par clé publique.
Argon2 (hachage local)	Oui	Non	Non	Non	Les hachages Argon2 sont stockés dans le dossier utilisateur pour les cas d'utilisation de l'authentification « locale » basée sur

Fournisseur	Flux de mots de passe	Flux de clés publiques	Multi-factor	Récupération d'attributs	Détails
					un mot de passe.
Amazon Cognito	Oui	Non	Oui*	Non	Time-base d One-Time Authentification multifactorielle basée sur un mot de passe (TOTP) uniquement. * SMS-based Le MFA n'est pas pris en charge.
Entra ID (anciennement Azure AD)	Oui	Non	Non	Non	
Okta	Oui	Oui	Oui*	Oui	TOTP-based MFA uniquement.
Clé publique	Non	Oui	Non	Non	Les clés publiques sont stockées dans le dossier utilisateur de DynamoDB.

Fournisseur	Flux de mots de passe	Flux de clés publiques	Multi-factor	Récupération d'attributs	Détails
Secrets Manager	Oui	Oui	Non	Non	

Utilisation AWS Lambda pour intégrer votre fournisseur d'identité

Cette rubrique explique comment créer 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.

Dans la plupart des cas d'utilisation, la méthode recommandée pour configurer un fournisseur d'identité personnalisé consiste à utiliser le [Solution de fournisseur d'identité personnalisée](#).

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, consultez [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 activez le protocole SFTP pour votre serveur Transfer Family.

- Assurez-vous que la valeur par défaut, Utiliser AWS Lambda pour connecter votre fournisseur d'identité, est sélectionnée.
- 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 de terminaison de serveur SFTP, FTPS ou FTP](#).

Politique basée sur les ressources Lambda

Vous devez disposer d'une politique qui fait référence au serveur Transfer Family et aux ARN Lambda. Par exemple, vous pouvez utiliser la politique suivante avec votre fonction Lambda qui se connecte à votre fournisseur d'identité. La politique est ignorée au format 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:lambda:region:123456789012:function:my-lambda-auth-function\",
      \"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
        \"arn:aws:transfer:region:123456789012:server/server-id\"}}}}
  ]}"
```

Note

Dans l'exemple de politique ci-dessus, remplacez chacune *user input placeholder* par vos propres informations.

Structure des messages d'événements

La structure du message d'événement envoyé par le serveur SFTP à la fonction Lambda d'autorisation pour un IDP personnalisé 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 des événements est similaire pour le FTP et le FTPS : la seule différence est que ces valeurs sont utilisées pour le `protocol` paramètre, plutôt que SFTP.

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

- [Valeurs Lambda valides](#)
- [Exemples de fonctions Lambda](#)
- [Tester votre configuration](#)
- [Modèles de fonctions Lambda](#)

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.

Value	Description	Obligatoire
Role	Spécifie le nom de ressource Amazon (ARN) du rôle IAM qui contrôle l'accès de vos utilisateurs à votre compartiment Amazon S3 ou à votre système de fichiers Amazon 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 votre système de fichiers Amazon S3 ou Amazon EFS. Le rôle IAM doit également contenir une relation d'approbation qui permet au serveur d'accéder à vos ressources lors du traitement des demandes de transfert de votre utilisateur. Pour plus de détails sur l'établissement d'une relation de confiance, voir Étape 1 :	Obligatoire

Value	Description	Obligatoire
	Établir une relation d'approbation.	
PosixProfile	L'identité POSIX complète, y compris l'ID utilisateur (Uid), l'ID de groupe (Gid) et tout identifiant de groupe secondaire (SecondaryGids), qui contrôle l'accès de vos utilisateurs à vos systèmes de fichiers Amazon EFS. Les autorisations POSIX définies sur les fichiers et répertoires de votre système de fichiers déterminent le niveau d'accès accordé à vos utilisateurs lors du transfert de fichiers depuis et vers vos systèmes de fichiers Amazon EFS.	Nécessaire pour le stockage de sauvegarde Amazon EFS
PublicKeys	Liste des valeurs de clé publique SSH 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

Value	Description	Obligatoire
Policy	Une politique de session pour votre utilisateur afin que vous puissiez utiliser le même rôle IAM pour plusieurs utilisateurs. Cette stratégie étend l'accès de l'utilisateur à des parties de son compartiment Amazon S3. Pour plus d'informations sur l'utilisation des politiques de session avec des fournisseurs d'identité personnalisés, consultez les exemples de politiques de session présentés dans cette rubrique.	Facultatif

Value	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 sur <code>PATH</code>, l'utilisateur voit le bucket Amazon S3 ou les chemins Amazon EFS absolus tels quels dans ses clients de protocole de transfert de fichiers. • Si vous le définissez sur <code>LOGICAL</code>, vous devez fournir des mappages dans le <code>HomeDirectoryDetails</code> paramètre pour que les chemins Amazon S3 ou Amazon EFS soient visibles pour vos utilisateurs.	Facultatif

Value	Description	Obligatoire
HomeDirectoryDetails	Des mappages de répertoires logiques qui spécifient quels chemins et clés Amazon S3 ou Amazon EFS 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 correspond Target au chemin Amazon S3 ou Amazon EFS réel.	Obligatoire s'HomeDirectoryType il a une valeur de LOGICAL

Value	Description	Obligatoire
HomeDirectory	Le répertoire de destination d'un utilisateur lorsqu'il se connecte au serveur à l'aide du client. Le format dépend de votre backend de stockage : • Pour Amazon S3 : / bucket-name/user-home-directory Exemple : /amzn-s3-demo-bucket/users/john • Pour Amazon EFS : / fs-12345/user-home-directory Exemple : /fs-faa1a123/users/john  Important Le nom du compartiment ou l'ID du système de fichiers Amazon EFS doit être inclus dans le chemin. L'omission de ces informations entraînera des erreurs « Fichier introuvable » lors des transferts de fichiers.	Facultatif

Note

`HomeDirectoryDetail` est une représentation sous forme de chaîne d'une carte JSON. Cela contraste avec un véritable objet de carte JSON et `PublicKeys` un tableau JSON de chaînes. Consultez les exemples de code pour les détails spécifiques à la langue.

⚠ HomeDirectory Exigences relatives au format

Lorsque vous utilisez le `HomeDirectory` paramètre, assurez-vous d'inclure le format de chemin complet :

- Pour le stockage Amazon S3 : incluez toujours le nom du compartiment dans le format `/bucket-name/path`
- Pour le stockage Amazon EFS : incluez toujours l'ID du système de fichiers dans le format `/fs-12345/path`

L'une des causes fréquentes des erreurs « Fichier introuvable » est l'omission du nom du compartiment ou de l'ID du système de fichiers EFS dans le `HomeDirectory` chemin. Le réglage `HomeDirectory` sur « Juste / sans l'identifiant de stockage » entraînera la réussite de l'authentification, mais l'échec des opérations sur les fichiers.

Exemples de fonctions Lambda

Cette section présente quelques exemples de fonctions Lambda, à la fois en NodeJS et en Python.

Note

Dans ces exemples, l'utilisateur, le rôle, le profil POSIX, le mot de passe et les détails 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 format depends on your storage backend:
      // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
      users/john')
      // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
      HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
      replace with your bucket name
      // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
      for EFS
    };

    // 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 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

```

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 format depends on your storage backend:
            # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
            # users/john')
            # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
            'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
            # replace with your bucket name
            # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
            # uncomment for EFS
            '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 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 CloudFormation pile.

CLI

Pour tester votre configuration à l'aide de la 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 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 CloudFormation pile.

Si l'authentification de l'utilisateur réussit, le test renvoie une réponse `StatusCode: 200 HTTP`, 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 objet JSON qui a été « stringifié » (converti en une chaîne JSON 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\": \"\"
}
```

Modèles de fonctions Lambda

Vous pouvez déployer une 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-enabled AWS Transfer Family serveur CloudFormation en spécifiant une politique FIPS-enabled de sécurité dans votre modèle. Les politiques de sécurité disponibles sont décrites dans [Politiques de sécurité pour AWS Transfer Family serveurs](#)

Pour créer une CloudFormation pile à utiliser pour l'authentification

1. Ouvrez la CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
2. Suivez les instructions pour déployer une 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.
- [Okta-mfa modèle de pile](#) : modèle de base utilisé AWS Lambda avec un AWS Transfer Family serveur pour intégrer Okta, avec authentification multifactorielle, en tant que fournisseur d'identité personnalisé.
- [Modèle Azure Active Directory](#) : les détails de cette pile sont décrits dans le billet de blog [S'authentifier AWS Transfer Family avec 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.

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'une 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.

Dans la plupart des cas d'utilisation, la méthode recommandée pour configurer un fournisseur d'identité personnalisé consiste à utiliser le [Solution de fournisseur d'identité personnalisée](#).

Limitations liées à l'utilisation d'une API Gateway pour intégrer votre fournisseur d'identité

- Cette configuration ne prend pas en charge les domaines personnalisés.
- Cette configuration ne prend pas en charge une URL API Gateway privée.

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 en savoir plus, 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 vous permet de créer et de fournir des API de manière hautement sécurisée. Avec API Gateway, vous pouvez créer un point de terminaison HTTPS afin que toutes les opérations d'API entrantes soient transmises avec une sécurité accrue. Pour plus de détails sur le service API Gateway, consultez le [guide du développeur d'API Gateway](#).

API Gateway propose une méthode d'autorisation nommée `AWS_IAM`, qui vous donne la même authentification basée sur Gestion des identités et des accès AWS (IAM) que celle AWS utilisée en interne. Si vous activez l'authentification avec `AWS_IAM`, seuls les appelants disposant d'autorisations explicites pour appeler une API peuvent accéder à la méthode API Gateway de cette API.

Pour utiliser votre méthode API Gateway en tant que fournisseur d'identité personnalisé pour Transfer Family, activez IAM pour votre méthode API Gateway. Dans le cadre de ce processus, vous fournissez un rôle IAM 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 requêtes HTTP et HTTPS qui sont transmises à Amazon API Gateway. Pour en savoir plus, consultez [Ajouter un pare-feu pour applications Web](#).

Ne pas activer la mise en cache d'API Gateway

N'activez pas la mise en cache pour votre méthode API Gateway lorsque vous l'utilisez comme fournisseur d'identité personnalisé pour Transfer Family. La mise en cache est inappropriée et non valide pour les demandes d'authentification pour les raisons suivantes :

- Chaque demande d'authentification est unique et nécessite une réponse en direct, et non une réponse en cache
- La mise en cache n'apporte aucun avantage puisque Transfer Family n'envoie jamais de demandes dupliquées ou répétées à l'API Gateway.
- L'activation de la mise en cache entraînera la réponse de l'API Gateway avec des données incompatibles, ce qui se traduira par des réponses non valides aux demandes d'authentification

Pour utiliser votre méthode API Gateway pour une authentification personnalisée avec Transfer Family

1. Créez une CloudFormation pile. Pour cela :

Note

Les modèles de pile ont été mis à jour pour utiliser des BASE64-encoded mots de passe : pour plus de détails, voir [Améliorations apportées aux CloudFormation modèles](#).

- a. Ouvrez la CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
- b. Suivez les instructions pour déployer une 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 AWS Lambda basée sur des données 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 comme 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 SSH (Secure Shell) codé en dur. 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 méthode d'API basée sur API Gateway. Vous pouvez ensuite utiliser votre méthode API 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 (ARN) de la pile, l'ARN du rôle IAM créé par la pile et l'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 sur votre Amazon Logs. CloudWatch. Nous vous déconseillons d'utiliser ce journal dans votre environnement de production. Pour plus d'informations, consultez la section [Configurer CloudWatch la journalisation des API dans API Gateway](#) dans le Guide du développeur d'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 l'API du modèle de base Transfer Custom Identity Provider générée par le CloudFormation modèle. Vous devrez peut-être sélectionner votre région pour voir vos passerelles.
- c. Dans le volet Ressources, sélectionnez GET. La capture d'écran suivante montre la configuration correcte de la méthode.

The screenshot displays the AWS API Gateway console interface for configuring a GET method. On the left, a sidebar shows the resource hierarchy: `/` > `/servers` > `/serverid` > `/users` > `/config`. The `GET` method is selected. The main panel shows the 'Method request settings' for the GET method. The settings are as follows:

Setting	Value									
Authorization	AWS_IAM									
API key required	False									
Request validator	None									
SDK operation name	Generated based on method and path									
Request paths (0)	No request paths defined									
URL query string parameters (2)	<table border="1"> <thead> <tr> <th>Name</th> <th>Required</th> <th>Caching</th> </tr> </thead> <tbody> <tr> <td>protocol</td> <td>False</td> <td>Inactive</td> </tr> <tr> <td>sourceip</td> <td>False</td> <td>Inactive</td> </tr> </tbody> </table>	Name	Required	Caching	protocol	False	Inactive	sourceip	False	Inactive
Name	Required	Caching								
protocol	False	Inactive								
sourceip	False	Inactive								
HTTP request headers (1)	<table border="1"> <thead> <tr> <th>Name</th> <th>Required</th> <th>Caching</th> </tr> </thead> <tbody> <tr> <td>PasswordBase64</td> <td>False</td> <td>Inactive</td> </tr> </tbody> </table>	Name	Required	Caching	PasswordBase64	False	Inactive			
Name	Required	Caching								
PasswordBase64	False	Inactive								
Request body (0)	No request body defined									

À ce stade, votre passerelle API est prête à être déployée.

3. Pour Actions, choisissez Deploy 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'adresse URL Invoke qui apparaît en haut de l'écran. Vous en aurez peut-être besoin pour l'étape suivante.

The screenshot displays the AWS Transfer Family console interface. At the top, the breadcrumb navigation shows 'API Gateway > APIs > Transfer Custom Identity Provider basic template API > Stages'. The main heading is 'Stages'. On the left, a sidebar lists the stage 'prod'. The main content area is divided into several sections:

- Stage details info**: Contains fields for 'Stage name' (prod), 'API cache' (Inactive), 'Rate' (10000), 'Burst' (5000), 'Web ACL' (-), and 'Client certificate' (-). The 'Invoke URL' field is highlighted with a red box and contains the value 'https://[redacted].execute-api.us-east-1.amazonaws.com/prod'. Below this, it shows 'Active deployment' as 't8aqrm on December 12, 2023, 10:49 (UTC-05:00)'.
- Logs and tracing info**: Contains fields for 'CloudWatch logs' (Error and info logs), 'Detailed metrics' (Inactive), and 'X-Ray tracing' (Inactive).
- Stage variables**: A tabbed section showing 'Stage variables (0/0)' with a search bar and a table. The table is empty, and a message states 'No variables associated with the stage.'.

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 texte Provide an Amazon API Gateway URL, collez l'adresse URL Invoke du point de terminaison API Gateway que vous avez créé à l'étape 3 de cette procédure.
- c. Pour Rôle, choisissez le rôle IAM créé par le CloudFormation modèle. Ce rôle permet à Transfer Family d'invoquer votre méthode de passerelle d'API.

Le rôle d'invocation contient le nom de 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 de terminaison de serveur SFTP, FTPS ou FTP](#).

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 ressource RESTful. Ajoutez également `sourceIp` et `protocol` en tant que paramètres de chaîne de requête URL dans la demande de méthode, comme indiqué dans l'image suivante.

Resources

Create resource

/

/servers

/servers/{serverId}

/servers/{serverId}/users

/servers/{serverId}/users/{username}

/servers/{serverId}/users/{username}/config

GET

API actions

Deploy API

/servers/{serverId}/users/{username}/config - GET - Method execution

Update documentation

Delete

ARN

arn:aws:execute-api:us-east-1:123456789012:*/servers/{serverId}/users/{username}/config

Resource ID

aw4ihv

Client

Method request

Method response

Integration request

Integration response

Lambda integration

Method request

Integration request

Integration response

Method response

Test

Method request settings

Edit

Authorization

AWS_IAM

Request validator

None

API key required

False

SDK operation name

Generated based on method and path

Request paths (0)

< 1 >

Name

▼

Caching

▼

No request paths

No request paths defined

URL query string parameters (2)

< 1 >

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, 0—9 A-Z, trait de soulignement « _ », tiret « - », point « . » et le signe « @ ». Le nom d'utilisateur ne peut pas commencer par un tiret « - », un point « . » ou par le 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 fichiers Amazon EFS 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 ressource RESTful.

Votre méthode API Gateway doit toujours renvoyer le code d'état HTTP200. Tout autre code d'état HTTP indique qu'une erreur s'est produite lors de l'accès à l'API.

Exemple de réponse Amazon S3

Le corps de réponse d'exemple est un document JSON 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": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

Note

La politique est ignorée au format JSON sous forme de chaîne. Par exemple :

```
"Policy":
```

```
"{
  \"Version\": \"2012-10-17\",
  \"Statement\":
    [
      {\"Condition\":
        {\"StringLike\":
          {\"s3:prefix\":
            [\"user/*\", \"user/\"]}},
        \"Resource\": \"arn:aws:s3:::amzn-s3-demo-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\": \"/amzn-s3-demo-bucket1\"}]",
  "PublicKeys": ["" ]
}
```

Exemple de réponse Amazon EFS

Le corps de réponse d'exemple est un document JSON au format suivant pour Amazon EFS.

```
{
  "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 publiques SSH. 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 objet JSON 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 format JSON. 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 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 recommandons de conserver des informations d'identification distinctes pour le protocole de transfert de fichiers (SFTP) Secure Shell (SSH) et le protocole de transfert de fichiers via SSL (FTPS). Nous recommandons de conserver des informations d'identification distinctes pour le protocole FTP car, contrairement au protocole SFTP et au protocole FTPS, le protocole FTP transmet les informations d'identification en texte clair. En isolant les informations d'identification FTP de celles du protocole SFTP ou FTPS, si les informations d'identification FTP sont partagées ou exposées, vos charges de travail utilisant le protocole SFTP ou FTPS restent sécurisées.

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 absolu Amazon EFS visible par vos utilisateurs.
- `HomeDirectoryType` set to `LOGICAL` — Ne définit aucun `HomeDirectory` champ. Nous avons plutôt défini un `HomeDirectoryDetails` champ qui fournit les `Entry/Target` mappages 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 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 CloudFormation modèle utilisant cette fonction Lambda, accédez au compartiment [Amazon S3 fourni par](#). AWS Transfer Family

Améliorations apportées aux CloudFormation modèles

Des améliorations ont été apportées à l'interface API Gateway dans les CloudFormation modèles publiés. Les modèles utilisent désormais des BASE64-encoded mots de passe avec l'API Gateway. 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 US-ASCII caractères 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 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 et assurez-vous d'avoir cette ligne :

```
"password":  
  "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(  
    \'",\"'\")",
```

- Recherchez RequestParameters et assurez-vous d'avoir 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 CloudFormation pile, consultez la section [Modification d'un modèle de pile](#) dans le AWS CloudFormation guide de l'utilisateur.

Utilisation de plusieurs méthodes d'authentification

Le serveur Transfer Family contrôle la logique AND 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, ce qui signifie qu'elles contiennent tous les éléments requis (rôle, répertoire de base, politique et profil POSIX 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 lorsque vous utilisez le mot de passe OU la clé ou le mot de passe ET la clé.

Le SSH/SFTP protocole met d'abord le client logiciel au défi 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.

Pour les options de fournisseur d'identité personnalisées, vous pouvez spécifier l'une des options suivantes pour l'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 UNIQUEMENT** : les utilisateurs doivent fournir leur mot de passe pour se connecter.
- **Clé UNIQUEMENT** : les utilisateurs doivent fournir leur clé privée pour se connecter.
- **Mot de passe ET clé** : 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.

Support IPv6 pour les fournisseurs d'identité personnalisés

AWS Transfer Family les fournisseurs d'identité personnalisés prennent entièrement en charge les connexions IPv6. Lorsque vous implémentez un fournisseur d'identité personnalisé, votre fonction Lambda peut recevoir et traiter des demandes d'authentification provenant de clients IPv4 et IPv6 sans aucune configuration supplémentaire. La fonction Lambda reçoit l'adresse IP du client dans le `sourceIp` champ de la demande, qui peut être une adresse IPv4 (par exemple `203.0.113.42`) ou une adresse IPv6 (par exemple, `2001:db8:85a3:8d3:1319:8a2e:370:7348`). L'implémentation de votre fournisseur d'identité personnalisé doit gérer les deux formats d'adresse de manière appropriée.

Important

Si votre fournisseur d'identité personnalisé effectue la IP-based validation ou la journalisation, assurez-vous que votre implémentation gère correctement les formats d'adresse IPv6. Les adresses IPv6 sont plus longues que les adresses IPv4 et utilisent un format de notation différent.

 Note

Lorsque vous gérez des adresses IPv6 dans votre fournisseur d'identité personnalisé, assurez-vous d'utiliser des fonctions d'analyse d'adresses IPv6 appropriées plutôt que de simples comparaisons de chaînes. Les adresses IPv6 peuvent être représentées dans différents formats canoniques (par exemple `fd00:b600::ec2` ou `fd00:b600:0:0:0:0:0:ec2`). Utilisez les bibliothèques ou fonctions d'adresses IPv6 appropriées dans votre langage d'implémentation pour valider et comparer correctement les adresses IPv6.

Exemple Gestion des adresses IPv4 et IPv6 dans un fournisseur d'identité personnalisé

```
def lambda_handler(event, context):
    # Extract the source IP address from the request
    source_ip = event.get('sourceIp', '')

    # Log the client IP address (works for both IPv4 and IPv6)
    print(f"Authentication request from: {source_ip}")

    # Example of IP-based validation that works with both IPv4 and IPv6
    if is_ip_allowed(source_ip):
        # Continue with authentication
        # ...
    else:
        # Reject the authentication request
        return {
            "Role": "",
            "HomeDirectory": "",
            "Status": "DENIED"
        }
```

Pour plus d'informations sur la mise en œuvre de fournisseurs d'identité personnalisés, consultez [Utilisation AWS Lambda pour intégrer votre fournisseur d'identité](#).

Utilisation de AWS Directory Service pour 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 Directory Service utilisateurs et aux groupes un accès sécurisé via SFTP, FTPS et FTP aux données stockées dans Amazon Simple Storage Service (Amazon S3) ou Amazon Elastic File System (Amazon EFS). Si vous utilisez Active Directory pour stocker les informations d'identification de vos utilisateurs, vous pouvez désormais activer plus facilement 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. Le blog sur le AWS stockage contient un article qui détaille une solution pour utiliser Active Directory avec Transfer Family : [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

 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 infrastructure RADIUS-based MFA 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 Directory Service console.
2. Utilisez la console Transfer Family pour créer un serveur utilisé AWS Managed Microsoft AD comme fournisseur d'identité.
3. Configurez l' AWS annuaire à l'aide d'un connecteur Active Directory.

4. Ajoutez l'accès depuis un ou plusieurs de vos Directory Service groupes.
5. 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](#)
- [Connexion à Microsoft Active Directory sur site](#)
- [Octroi de l'accès à des groupes](#)
- [Tester les utilisateurs](#)
- [Supprimer l'accès au serveur pour un groupe](#)
- [Connexion au serveur via 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

Note

AWS Transfer Family a une limite par défaut de 100 groupes Active Directory par serveur. Si votre cas d'utilisation nécessite plus de 100 groupes, envisagez d'utiliser une solution de fournisseur d'identité personnalisée, comme décrit dans [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

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 ressources Amazon S3 ou Amazon EFS via les protocoles activés à l'aide de AWS Transfer Family.

Utilisez la PowerShell commande Windows suivante pour récupérer le SID d'un groupe, en le *YourGroupName* remplaçant par 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 Directory Service des autorisations à votre rôle

Vous devez également disposer d'autorisations d' Directory Service API pour les 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, consultez [Autorisations d'Directory Service API : 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 en savoir plus, consultez [Tester les utilisateurs](#). En cas de problème avec le user/group domaine, vous recevez le message d'erreur « Aucun accès associé trouvé pour les groupes d'utilisateurs ».

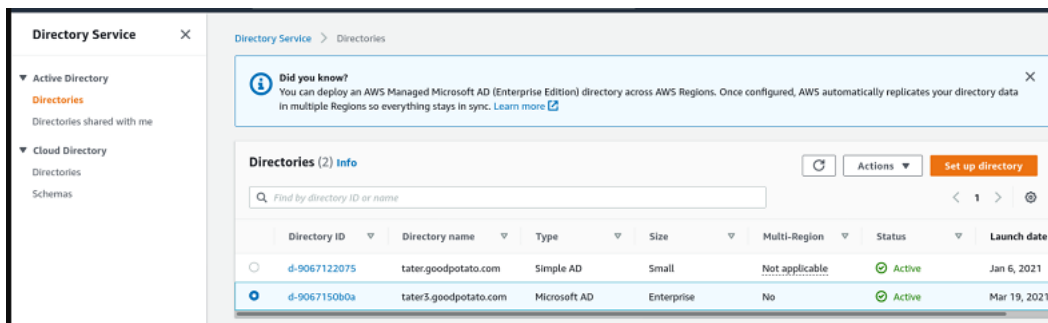
Choisir AWS Managed Microsoft AD comme fournisseur d'identité

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 Directory Service console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/directoryservicev2/>.

Utilisez la 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 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 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

- Cross-Account et les répertoires 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 Directory Service autorisations. Pour en savoir plus, 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-enabled serveur](#)
 - [Création d'un FTPS-enabled serveur](#)
 - [Création d'un FTP-enabled serveur](#)

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 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.

Connexion à Microsoft Active Directory sur site

Cette section décrit comment configurer un AWS annuaire à l'aide d'un AD Connector.

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 votre VPC et vos sous-réseaux.
5. Sélectionnez Suivant, puis renseignez les champs comme suit :
 - Nom DNS du répertoire : entrez le nom de domaine que vous utilisez pour votre Microsoft Active Directory.
 - Adresses IP DNS : entrez vos adresses IP Microsoft Active Directory.
 - Nom d'utilisateur et mot de passe du compte serveur : entrez les détails du compte de service à utiliser.
6. Complétez les écrans pour créer le service d'annuaire.

L'étape suivante consiste à créer un serveur Transfer Family utilisant le protocole SFTP et le type de fournisseur d'identité AWS Directory Service. Dans la liste déroulante Répertoire, sélectionnez le répertoire que vous avez ajouté lors de la procédure précédente.

Octroi de l'accès à des 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

AWS Transfer Family a une limite par défaut de 100 groupes Active Directory par serveur. Si votre cas d'utilisation nécessite plus de 100 groupes, envisagez d'utiliser une solution de fournisseur d'identité personnalisée, comme décrit dans [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

 Note

Les utilisateurs doivent appartenir directement au groupe auquel vous accordez l'accès. Par exemple, supposons que Bob est un utilisateur et appartient au groupe A, et que le groupe A lui-même est inclus dans le groupe B.

- 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 le SID du AWS Managed Microsoft AD répertoire auquel vous souhaitez accéder à ce serveur.

 Note

Pour plus d'informations sur la manière de trouver le SID de votre groupe, consultez [the section called “Avant de commencer à utiliser AWS Directory Service for Microsoft Active Directory”](#).

5. Pour Access, choisissez un rôle Gestion des identités et des accès AWS (IAM) 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 Amazon 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 du groupe.

 Note

Pour plus d'informations sur la façon de trouver le SID, 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.

The screenshot displays the AWS Transfer Family console interface. At the top, the 'Endpoint configuration' section shows the 'Availability Zone' as 'us-east-1a', the 'Subnet ID' as 'subnet-...', and the 'Private IPv4 Address' as '172.31.80.36'. Below this, the 'Accesses (1)' section features a search bar, an 'Actions' dropdown menu, and an 'Associate access' button. A table lists the access details with columns for 'External Id', 'Home directory', and 'Role'. The first entry shows a checked checkbox, 'S...', '/padbucket3', and 'ADGuy_S3_And_EFS'. The 'Additional details' section at the bottom includes an 'Edit' button and information about the 'Logging role' (Server activity not logged to Amazon CloudWatch), 'Server host key', 'Security Policy' (TransferSecurityPolicy-2018-11), and '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 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": null,
    "publicKeys": null,
    "role": "arn:aws:iam::195886157073:role/ADGuy_SS_And_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 via SSH (Secure Shell)

Après avoir configuré votre serveur et vos utilisateurs, vous pouvez vous connecter au serveur via 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

Directory Service dispose des options suivantes pour se connecter à un Active Directory autogéré :

- One-way forest trust (sortant AWS Managed Microsoft AD et entrant pour Active Directory local) ne fonctionne que pour le domaine racine.
- Pour les domaines enfants, vous pouvez utiliser l'une des options suivantes :
 - Utiliser 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 AWS Directory Service pour les services de domaine Entra ID

Pour les clients qui ont uniquement besoin d'un transfert SFTP et qui ne souhaitent pas gérer de domaine, il existe Simple Active Directory. Les clients qui souhaitent bénéficier des avantages d'Active Directory et de la haute disponibilité dans un service entièrement géré peuvent également utiliser AWS Managed Microsoft AD. Enfin, pour les clients qui souhaitent tirer parti de leur forêt Active Directory existante pour leur transfert SFTP, il existe le connecteur Active Directory.

Notez ce qui suit :

- Pour tirer parti de votre forêt Active Directory existante pour vos besoins de transfert SFTP, 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 en savoir plus, consultez [Utilisation de AWS Directory Service pour Microsoft Active Directory](#).

Cette rubrique décrit comment utiliser un connecteur Active Directory et les [services de domaine Entra ID \(anciennement Azure AD\)](#) pour authentifier les utilisateurs de SFTP Transfer avec l'identifiant Entra.

Rubriques

- [Avant de commencer à utiliser AWS Directory Service pour les services de domaine Entra ID](#)
- [Étape 1 : Ajouter les services de domaine Entra ID](#)
- [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 les services de domaine Entra ID

Note

AWS Transfer Family a une limite par défaut de 100 groupes Active Directory par serveur. Si votre cas d'utilisation nécessite plus de 100 groupes, envisagez d'utiliser une solution de fournisseur d'identité personnalisée, comme décrit dans [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

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
- Le VPC doit disposer d'une connexion Internet
- Une passerelle client et une passerelle privée virtuelle pour une connexion VPN de site à site avec Microsoft Entra

Pour Microsoft Entra, vous avez besoin des éléments suivants :

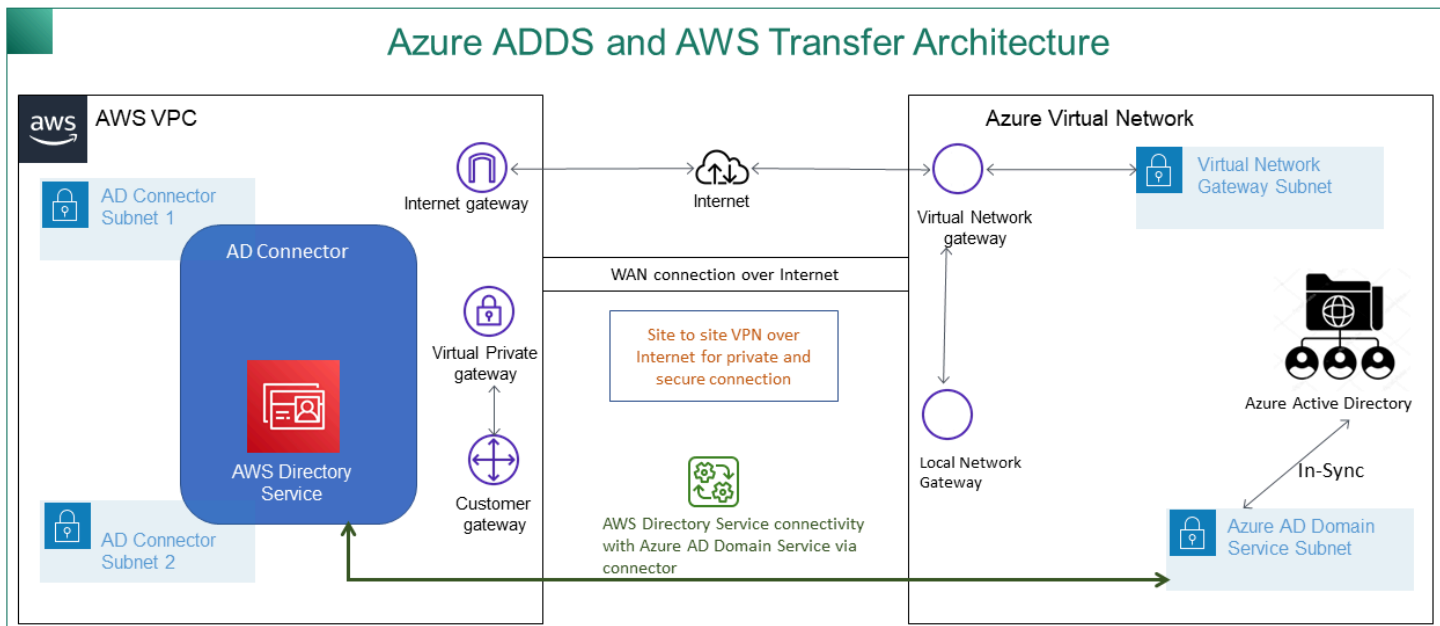
- Un identifiant Entra et un service de domaine Active Directory
- Un groupe de ressources Entra
- Un réseau virtuel Entra
- Connectivité VPN entre votre Amazon VPC et votre groupe de ressources Entra

Note

Cela peut se faire par le biais de tunnels IPSEC natifs ou d'appareils VPN. Dans cette rubrique, nous utilisons des tunnels IPSEC entre une passerelle réseau virtuelle Entra et une passerelle réseau locale. Les tunnels doivent être configurés pour autoriser le trafic entre les points de terminaison de votre service de domaine Entra et les sous-réseaux qui hébergent votre AWS VPC.

- Une passerelle client et une passerelle privée virtuelle pour une connexion VPN de site à site avec Microsoft Entra

Le schéma suivant montre la configuration requise avant de commencer.



Étape 1 : Ajouter les services de domaine Entra ID

Entra ID 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 pour utiliser des outils tels que la politique de groupe, les administrateurs doivent activer les services de domaine Entra ID. Si vous n'avez pas encore ajouté Entra DS, ou si votre implémentation existante n'est pas associée au domaine que vous souhaitez que votre serveur de transfert SFTP utilise, vous devez ajouter une nouvelle instance.

Pour plus d'informations sur l'activation des services de domaine Entra ID, voir [Tutoriel : Création et configuration d'un domaine géré par les services de domaine Microsoft Entra ID](#).

Note

Lorsque vous activez Entra DS, assurez-vous qu'il est configuré pour le groupe de ressources et le domaine Entra auxquels vous connectez votre serveur de transfert SFTP.


bob.us

 Azure AD Domain Services

«
Refresh
Delete

Overview

 Activity log

 Access control (IAM)

 Tags

 Settings

 Properties

 Configuration issues for your managed domain were detected. Run configuration diagnostics


bob.us

 Running

[View health](#)

Étape 2 : Création d'un compte de service

Entra doit disposer d'un compte de service faisant partie d'un groupe d'administrateurs dans Entra DS. Ce compte est utilisé avec le connecteur AWS Active Directory. Assurez-vous que ce compte est synchronisé avec Entra DS.

[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

bobatusa

bobsmith@xyz.com

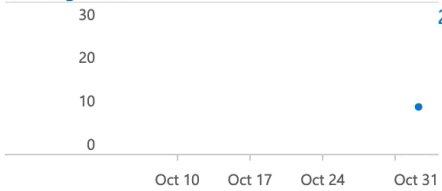


 Creation time
 10/6/2021, 1:32:27 AM

Identity

Name	First name	Last name
bobatusa	Bob	Smith
User Principal Name	User type	
bobsmith@xyz.com	Member	

User Sign-ins



Group memberships



Activity

- Sign-in logs
- Audit logs

Tip

Multi-factor l'authentification pour Entra ID n'est pas prise en charge pour les serveurs Transfer Family qui utilisent le protocole SFTP. Le serveur Transfer Family ne peut pas fournir le jeton MFA une fois qu'un utilisateur s'est authentifié auprès du protocole SFTP. Assurez-vous de désactiver le 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 Entra DS et créé un compte de service avec des tunnels VPN IPSEC entre votre AWS VPC et le réseau virtuel Entra, vous pouvez tester la connectivité en envoyant un ping à l'adresse IP DNS d'Entra DS depuis AWS n'importe quelle instance EC2.

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 votre VPC et vos sous-réseaux.
5. Sélectionnez Suivant, puis renseignez les champs comme suit :
 - Nom DNS du répertoire : entrez le nom de domaine que vous utilisez pour votre Entra DS.
 - Adresses IP DNS : entrez vos adresses IP Entra DS.

- 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 de transfert SFTP.

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](#)

Find by directory ID or name

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 protocole SFTP et le type de fournisseur d'identité 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

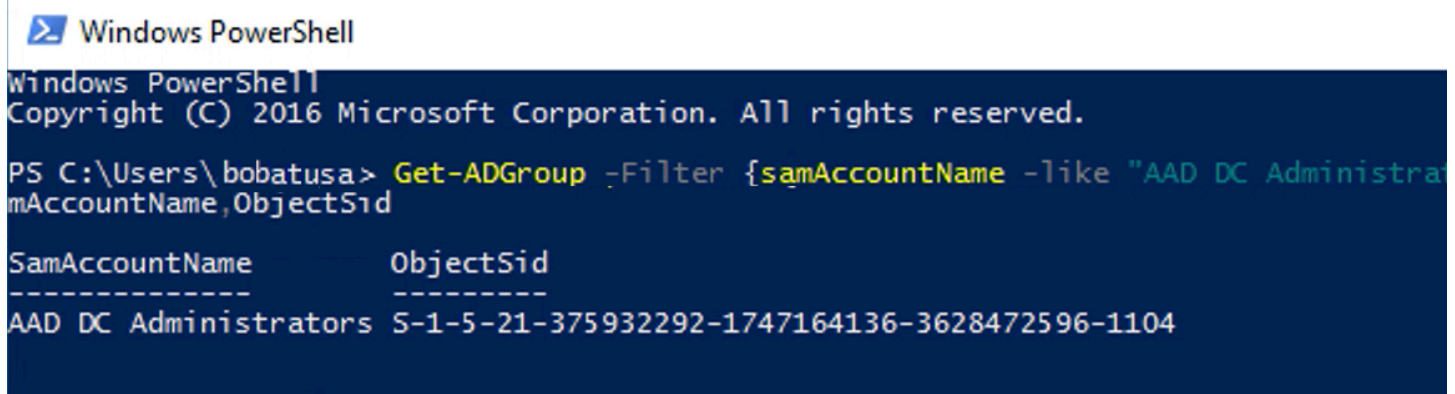
Les utilisateurs doivent appartenir directement au groupe auquel vous accordez l'accès. Par exemple, supposons que Bob est un utilisateur et appartient au groupe A, et que le groupe A lui-même est inclus dans le groupe B.

- 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 du groupe.

Utilisez la PowerShell commande Windows suivante pour récupérer le SID d'un groupe, en le *YourGroupName* remplaçant par le nom du groupe.

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select  
SamAccountName, ObjectSid
```



```
> Windows PowerShell  
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
  
PS C:\Users\bobatusa> Get-ADGroup -Filter {samAccountName -like "AAD DC Administrators"} -Properties * | Select SamAccountName, ObjectSid  
  
SamAccountName      ObjectSid  
-----  
AAD DC Administrators S-1-5-21-375932292-1747164136-3628472596-1104
```

Accorder l'accès aux groupes

1. Ouvrir <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 que vous avez reçu à la sortie de la procédure précédente.
4. Pour Access, choisissez un Gestion des identités et des accès AWS 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 Amazon 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	Identity provider
Protocols over which clients can connect to your server's endpoint SFTP	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	/smb/finance	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.

Utilisation de répertoires logiques pour simplifier vos structures de répertoires Transfer Family

Les répertoires logiques simplifient la structure des répertoires de votre AWS Transfer Family serveur. Avec les répertoires logiques, vous pouvez créer une structure de répertoire virtuel avec des noms faciles à utiliser par les utilisateurs lorsqu'ils se connectent à votre compartiment Amazon S3 ou à votre système de fichiers Amazon EFS. Cela empêche les utilisateurs de voir les chemins de répertoire, les noms des compartiments et les noms des systèmes de fichiers réels.

Note

Vous devez utiliser des politiques de session afin que vos utilisateurs finaux ne puissent effectuer que les opérations que vous les autorisez à effectuer.

Vous devez utiliser des répertoires logiques pour créer un répertoire virtuel convivial pour vos utilisateurs finaux et supprimer les noms de compartiments. Les mappages de répertoires logiques permettent uniquement aux utilisateurs d'accéder à leurs chemins logiques et sous-répertoires désignés, et interdisent les chemins relatifs qui traversent les racines logiques. Transfer Family valide tous les chemins susceptibles d'inclure des éléments relatifs et bloque activement la résolution de ces chemins avant que nous ne les transmettions à Amazon S3 ; cela empêche vos utilisateurs d'aller au-delà de leurs mappages logiques. Même si Transfer Family empêche vos utilisateurs finaux d'accéder à des répertoires situés en dehors de leur répertoire logique, nous vous recommandons également d'utiliser des rôles ou des politiques de session uniques pour appliquer le moindre privilège au niveau du stockage.

Comprendre le chroot et la structure des répertoires

Une opération chroot vous permet de définir le répertoire racine d'un utilisateur à n'importe quel emplacement de votre hiérarchie de stockage. Cela limite les utilisateurs à leur répertoire d'accueil ou racine configuré, empêchant ainsi l'accès aux répertoires de niveau supérieur.

Prenons le cas où un utilisateur Amazon S3 est limité à `amzn-s3-demo-bucket/home/${transfer:UserName}`. Sans chroot, certains clients peuvent autoriser les utilisateurs à accéder à `/amzn-s3-demo-bucket/home`, ce qui nécessite une déconnexion et une connexion pour retourner dans leur répertoire approprié. L'exécution d'une opération de chroot permet d'éviter ce problème.

Vous pouvez créer des structures de répertoires personnalisées dans plusieurs compartiments et préfixes. Cela est utile si votre flux de travail nécessite une structure de répertoire spécifique que les préfixes de compartiment ne peuvent fournir à eux seuls. 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.

Règles d'utilisation des répertoires logiques

Cette section décrit certaines règles et autres considérations relatives à l'utilisation de répertoires logiques.

Limites de mappage

- Un seul mappage est autorisé lorsqu'il l'Entry est "/" (aucun chevauchement de chemins n'est autorisé).
- Les annuaires logiques prennent en charge des mappages allant jusqu'à 2,1 Mo pour les utilisateurs IDP et AD personnalisés, et 2 000 entrées pour les utilisateurs gérés par des services. 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.

Exigences relatives au chemin cible

- Utilisez `${transfer:UserName}` une variable si le chemin du bucket ou du système de fichiers a été paramétré en fonction du nom d'utilisateur.
- Les cibles peuvent être configurées pour pointer vers différents compartiments ou systèmes de fichiers Amazon S3, à condition que le rôle IAM associé dispose des autorisations nécessaires pour accéder à ces emplacements de stockage.
- Toutes les cibles doivent commencer par une barre oblique (/) mais ne peuvent pas se terminer par une barre oblique. Par exemple, `/amzn-s3-demo-bucket/images` c'est correct, tandis que `amzn-s3-demo-bucket/images` ce n'est pas le cas.

Considérations relatives au stockage

- Amazon S3 est un magasin d'objets dans lequel les dossiers n'existent qu'en tant que concept virtuel. Lorsque vous utilisez le stockage Amazon S3, Transfer Family indique les préfixes sous forme de répertoires dans les opérations STAT, même s'il n'existe aucun objet de zéro octet marqué d'une barre oblique. Un objet zéro octet approprié avec une barre oblique finale est également signalé comme un répertoire dans les opérations STAT. 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.

- Pour les applications qui doivent faire la distinction entre les fichiers et les dossiers, utilisez Amazon Elastic File System (Amazon EFS) comme option de stockage 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`.

Valeurs de l'annuaire des utilisateurs

- Le paramètre permettant de spécifier des valeurs de répertoire logiques dépend de votre 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`.
- Lorsque vous utilisez `LOGICAL HomeDirectoryType`, vous pouvez spécifier une `HomeDirectory` valeur pour les mises en œuvre des utilisateurs gérés par le service, de l'accès Active Directory et du fournisseur d'identité personnalisé lorsqu' `HomeDirectoryDetails` elles sont fournies dans la réponse. Si ce n'est pas spécifié, la `HomeDirectory` valeur par défaut est. /

Pour plus de détails sur la façon d'implémenter des répertoires logiques, consultez [Implémentation de répertoires logiques](#).

Implémentation de répertoires logiques

Important

Exigences relatives au répertoire racine

- Si vous n'utilisez pas les paramètres d'optimisation des performances d'Amazon S3, votre répertoire racine doit exister au démarrage.

- Pour Amazon S3, cela signifie créer un objet de zéro octet qui se termine par une barre oblique (/).
- Pour éviter cette exigence, pensez à activer l'optimisation des performances d'Amazon S3 lorsque vous créez ou mettez à jour votre serveur.
- Lorsque vous spécifiez a HomeDirectory avec LOGICAL HomeDirectoryType, la valeur doit correspondre à l'un de vos mappages de répertoires logiques. Le service valide cela lors de la création et des mises à jour des utilisateurs afin d'éviter que les configurations ne fonctionnent pas.

Configuration logique du répertoire de base

Lorsque vous utilisez LOGICAL comme votre HomeDirectoryType, notez ce qui suit :

- La HomeDirectory valeur doit correspondre à l'un de vos mappages de répertoires logiques existants.
- Le système le valide automatiquement lors de la création et des mises à jour des utilisateurs.
- Cette validation permet d'éviter les configurations susceptibles de provoquer des problèmes d'accès.

Activer les répertoires logiques

Pour utiliser des répertoires logiques pour un utilisateur, définissez le HomeDirectoryType paramètre sur LOGICAL. Procédez ainsi lorsque vous créez un nouvel utilisateur ou que vous mettez à jour un utilisateur existant.

```
"HomeDirectoryType": "LOGICAL"
```

Activer **chroot** pour les utilisateurs

Pour chroot créer une structure de répertoire composée d'un répertoire unique Entry et d'un Target appariement pour chaque utilisateur. L'entrée/représente le dossier racine, tandis que Target indique l'emplacement réel dans votre bucket ou votre système de fichiers.

Exemple for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/jane"}]
```

Exemple pour 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":  
"/amzn-s3-demo-bucket${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 S3 ou systèmes de fichiers EFS, y compris dans plusieurs compartiments ou systèmes de fichiers, à condition que le mappage des rôles IAM de l'utilisateur soit autorisé à y accéder.

Dans l'exemple de structure virtuelle suivant, lorsque l'utilisateur se connecte à 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 Amazon EFS, vous avez toujours besoin de l'administrateur pour créer les mappages logiques ou le `/` répertoire.

```
[  
{"Entry": "/pics", "Target": "/amzn-s3-demo-bucket1/pics"},  
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},  
]
```



```
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},  
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/  
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": "/amzn-s3-demo-bucket/pics"  
},  
{  
  "Entry": "/doc",  
  "Target": "/amzn-s3-demo-bucket/mydocs"  
},  
{  
  "Entry": "/temp",  
  "Target": "/amzn-s3-demo-bucket2/temporary"  
}
```

Vous ne pouvez télécharger des fichiers que dans ces compartiments. Lorsque vous vous connectez pour la première fois `ftp`, vous êtes déposé dans le répertoire racine, `/`. Si vous tentez 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 structure AWS SFTP avec un chroot et des répertoires logiques](#) dans le blog AWS de stockage.

Exemples 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 \  
  --server-id s-11112222333344445 \  
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-  
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-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 \  
  --server-id s-11112222333344445 \  
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-  
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs  
\"}]"
```

Notez ce qui suit :

- Si /amzn-s3-demo-bucket1/pics les répertoires /amzn-s3-demo-bucket2/test/mydocs n'existent pas déjà, l'utilisateur (ou un administrateur) doit les créer.

Note

Ces annuaires sont créés automatiquement par le serveur Transfer Family si vous avez configuré des annuaires optimisés.

- Lorsqu'elle **marymajor** se connecte au serveur et exécute la `ls -l` commande, Mary 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 que Mary ajoute `pics` et `doc` sont ajoutés aux chemins Amazon S3 `/amzn-s3-demo-bucket1/pics` et `/amzn-s3-demo-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.

Cet exemple fournit une configuration alternative pour un chemin d'accès d'origine logique.

```
aws transfer create-user \
  --user-name marymajor \
  --server-id s-11112222333344445 \
  --role arn:aws:iam::1234abcd5678:role/marymajor-role \
  --home-directory-type LOGICAL \
  --home-directory /home/marymajor \
  --home-directory-mappings "[{\"Entry\":\"/home/marymajor/pics\", \"Target\":\"/amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/home/marymajor/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs\"}]" \
  --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

Notez ce qui suit :

- Les mappages fournissent un chemin commun `/home/marymajor`, qui constitue la première partie des deux chemins logiques. Les fichiers peuvent ensuite être ajoutés aux `doc` dossiers `pics` et.
- Comme dans l'exemple précédent, le répertoire de base est `/home/marymajor` en lecture seule.

Configuration de répertoires logiques pour Amazon EFS

Si votre serveur Transfer Family utilise Amazon EFS, 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\\\": \"\\\\/amzn-s3-demo-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\\\\": \\\\"/amzn-s3-demo-bucket/theRealFolder\\\\"}]\\\"",
```

```
    \"PublicKeys\": \"[ssh-rsa myrsapubkey]\"},  
    \"StatusCode\": 200  
}
```

Note

La `\"Url\"` : ligne est renvoyée uniquement si vous utilisez une méthode API Gateway comme fournisseur d'identité personnalisé.

Accédez à vos systèmes de fichiers FSx for NetApp ONTAP avec Transfer Family

Table des matières

- [Présentation de](#)
- [Conditions préalables](#)
 - [Exigences relatives à FSx for NetApp ONTAP](#)
 - [Autorisations IAM requises](#)
- [Comment fonctionne le stockage FSx avec Transfer Family](#)
 - [Identité de l'utilisateur du système de fichiers](#)
- [Création d'un point d'accès S3 pour FSx](#)
 - [Désignation des points d'accès](#)
 - [Création d'un point d'accès pour FSx for ONTAP NetApp](#)
 - [Configuration des autorisations du système de fichiers](#)
- [Utilisation d'alias de point d'accès S3 avec FSx](#)
 - [À propos des alias de point d'accès](#)
 - [Trouver l'alias de votre point d'accès](#)
- [Configuration de Transfer Family pour le stockage FSx](#)
 - [Création d'un rôle IAM](#)
- [Gestion des utilisateurs pour le stockage FSx](#)
 - [Création d'un utilisateur](#)
 - [Configuration de mappages de répertoires multiples](#)

- [Configuration des clients de transfert de fichiers](#)
 - [Configuration de WinSCP](#)
 - [Autres clients SFTP](#)
- [Résolution des problèmes de stockage FSx](#)
 - [Problèmes liés au fonctionnement des fichiers](#)

Présentation de

Transfer Family prend en charge Amazon FSx for NetApp ONTAP via les points d'accès S3. Amazon FSx for NetApp ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités basé sur NetApp le célèbre système de fichiers ONTAP. Lorsque vous configurez Transfer Family avec un système de fichiers FSx, vos utilisateurs se connectent aux points de terminaison Transfer Family à l'aide de clients de transfert de fichiers standard. Transfer Family achemine les opérations sur les fichiers via un point d'accès S3 connecté à votre volume FSx, tandis que vos données restent sur le système de fichiers FSx. Pour en savoir plus sur FSx for NetApp ONTAP, consultez [Qu'est-ce qu'Amazon FSx for ONTAP ? NetApp](#)

Cette intégration vous permet de :

- Transférez des fichiers à l'aide des protocoles SFTP, FTPS ou FTP vers un stockage de fichiers de niveau professionnel
- Accédez aux mêmes données via plusieurs protocoles (SFTP, NFS, SMB)
- Utilisez les fonctionnalités de FSx telles que les instantanés, les sauvegardes et la hiérarchisation des données

Important

Certaines opérations sur les fichiers ne sont pas prises en charge lors de l'utilisation de systèmes de fichiers FSx avec Transfer Family, notamment les opérations de renommage et d'ajout. Pour les opérations de téléchargement, la taille des fichiers est limitée à 5 Go. Pour une liste complète des limitations, consultez la section [Compatibilité des points d'accès](#).

Conditions préalables

Avant de configurer Transfer Family avec Amazon FSx, vous devez satisfaire aux exigences suivantes.

Exigences relatives à FSx for NetApp ONTAP

Pour utiliser FSx for NetApp ONTAP avec Transfer Family, vous devez :

- Un système de fichiers FSx for NetApp ONTAP exécutant ONTAP version 9.17.1 ou ultérieure
- Le système de fichiers et le point d'accès S3 dans la même AWS région
- Le même AWS compte possédant à la fois le système de fichiers et le point d'accès

Pour en savoir plus, consultez [Getting started with Amazon FSx for NetApp ONTAP](#).

Autorisations IAM requises

Vous pouvez configurer chaque point d'accès S3 avec des autorisations et des contrôles réseau distincts que S3 applique à toute demande effectuée à l'aide de ce point d'accès. Les points d'accès S3 prennent en charge les politiques de ressources IAM que vous pouvez utiliser pour contrôler l'utilisation du point d'accès par ressource, par utilisateur ou selon d'autres conditions. Pour qu'une application ou un utilisateur puisse accéder à des fichiers via un point d'accès, le point d'accès et le volume sous-jacent doivent autoriser la demande. Pour plus d'informations, consultez la section [Politiques des points d'accès IAM](#).

Les points d'accès Amazon S3 pour FSx utilisent un modèle d'autorisation à double couche qui combine les autorisations IAM avec les autorisations au niveau du système de fichiers. Cette approche garantit que les demandes d'accès aux données sont correctement autorisées à la fois au niveau du AWS service et au niveau du système de fichiers sous-jacent.

Pour qu'une application ou un utilisateur puisse accéder aux données via un point d'accès, la politique du point d'accès S3 et le volume FSx sous-jacent doivent autoriser la demande.

Pour créer et configurer cette intégration, vous devez disposer des autorisations suivantes :

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`
- `s3:PutAccessPointPolicy`(si vous créez une politique de point d'accès facultative)

Comment fonctionne le stockage FSx avec Transfer Family

Lorsque vous configurez Transfer Family avec un système de fichiers FSx, les composants suivants fonctionnent ensemble pour permettre les transferts de fichiers :

1. Un utilisateur se connecte au serveur Transfer Family à l'aide d'un client SFTP, FTPS ou FTP.
2. Transfer Family authentifie l'utilisateur à l'aide d'identités gérées par le service, d'un fournisseur d'identité personnalisé ou. AWS Directory Service for Microsoft Active Directory Une fois authentifié, Transfer Family assume le rôle IAM associé à l'utilisateur.
3. Pour chaque opération sur un fichier, Transfer Family agit comme un client API S3 standard, en envoyant des demandes au point d'accès S3 en utilisant le rôle IAM assumé par l'utilisateur et en vérifiant les autorisations par rapport à la politique du point d'accès S3.
4. Le système de fichiers FSx vérifie que l'utilisateur du système de fichiers associé au point d'accès est autorisé à effectuer l'opération demandée. L'opération de fichier est ensuite effectuée sur le volume FSx.

Pour qu'une opération sur un fichier réussisse, les deux couches d'autorisation doivent autoriser la demande.

Note

L'attachement d'un point d'accès S3 à un volume FSx ne modifie pas le comportement du volume en cas d'accès direct via NFS ou SMB. L'accès au protocole de fichier existant continue de fonctionner sans modification.

Identité de l'utilisateur du système de fichiers

Chaque point d'accès utilise une identité d'utilisateur du système de fichiers que vous spécifiez lors de la création du point d'accès. Cette identité autorise toutes les demandes d'accès aux fichiers effectuées via ce point d'accès. L'utilisateur du système de fichiers est un compte utilisateur sur le système de fichiers Amazon FSx sous-jacent. Si l'utilisateur du système de fichiers dispose d'un accès en lecture seule, seules les demandes de lecture effectuées via le point d'accès sont autorisées et les demandes d'écriture sont bloquées. Si l'utilisateur du système de fichiers dispose d'un accès en lecture-écriture, les demandes de lecture et d'écriture adressées au volume attaché à l'aide du point d'accès sont autorisées.

Création d'un point d'accès S3 pour FSx

Avant de configurer Transfer Family, vous devez créer un point d'accès S3 connecté à votre volume FSx. Les points d'accès S3 sont appelés points de terminaison réseau attachés à une source de données telle qu'un bucket ou un volume Amazon FSx for ONTAP. Vous pouvez créer et associer un point d'accès à un FSx pour NetApp ONTAP à l'aide de la console, de la AWS CLI ou de l'API Amazon FSx. Une fois qu'il est attaché, vous pouvez utiliser les API des objets S3 pour accéder aux données de vos fichiers. Vos données demeurent dans le système de fichiers Amazon FSx et restent directement accessibles pour vos charges de travail existantes. Vous continuez à gérer votre stockage en utilisant toutes les fonctionnalités de gestion du stockage de FSx for NetApp ONTAP, notamment les sauvegardes, les instantanés, les quotas d'utilisateurs et de groupes et la compression.

Pour plus d'informations, consultez [Création de points d'accès](#).

Désignation des points d'accès

Lorsque vous nommez votre point d'accès, suivez les instructions suivantes :

- Les noms des points d'accès doivent être uniques au sein de votre AWS compte et de votre région.
- Les noms ne peuvent pas se terminer par `-ext-s3alias` (réservés aux alias).
- Évitez d'inclure des informations sensibles dans les noms, car elles sont publiées dans le DNS.

Pour une liste complète des règles de dénomination, voir [Règles de dénomination, restrictions et limitations des points d'accès](#).

Création d'un point d'accès pour FSx for ONTAP NetApp

Utilisez la procédure suivante pour créer un point d'accès S3 pour un volume FSx for NetApp ONTAP.

Pour créer un point d'accès (console)

1. Ouvrez la console Amazon FSx à l'adresse. <https://console.aws.amazon.com/fsx/>
2. Dans le volet de navigation, sélectionnez Systèmes de fichiers.
3. Choisissez votre système de fichiers FSx for NetApp ONTAP.
4. Choisissez l'onglet Volumes.
5. Sélectionnez le volume que vous souhaitez associer.

6. Pour Actions, choisissez Create S3 access point.
7. Pour Nom du point d'accès, entrez un nom descriptif (par exemple, `transfer-family-ap`).
8. Pour le type d'identité utilisateur du système de fichiers, choisissez l'une des options suivantes :
 - Identité UNIX : pour les volumes dotés d'un style de sécurité UNIX
 - Identité Windows : pour les volumes dotés d'un style de sécurité NTFS
9. (Facultatif) Pour la politique de point d'accès, entrez une stratégie IAM qui définit quels principaux IAM peuvent effectuer quelles opérations sur les objets accessibles via ce point d'accès. Pour plus d'informations, consultez la section [Gestion de l'accès aux points d'accès](#).
10. Choisissez Créer.
11. Après la création, notez l'alias du point d'accès à utiliser dans la configuration de Transfer Family.

Note

Lorsque vous AWS Transfer Family accédez aux ressources S3 pour le compte de vos SFTP/FTPS utilisateurs connectés, les demandes proviennent de AWS Transfer Family l'infrastructure et non de votre VPC. De ce fait, les points d'accès S3 configurés avec une origine de réseau VPC rejeteront ces demandes. Cependant, même si vous utilisez un point d'accès configuré avec une origine de réseau Internet, tout le trafic entre Transfer Family et le point d'accès reste privé et passe par AWS le réseau principal ; il ne traverse pas l'Internet public.

Configuration des autorisations du système de fichiers

L'utilisateur du système de fichiers que vous spécifiez détermine les opérations que les utilisateurs de Transfer Family peuvent effectuer. Vous devez configurer les autorisations appropriées sur votre volume FSx.

Exemple UNIX :

```
# Create a directory for Transfer Family users
mkdir -p /vol1/transfer-users

# Set ownership to match the access point user
chown 1001:1001 /vol1/transfer-users
```

```
# Set permissions
chmod 755 /vol1/transfer-users
```

Exemple Windows :

```
# Create a directory for Transfer Family users
New-Item -Path "D:\vol1\transfer-users" -ItemType Directory

# Set permissions for the file system user associated with the access point
# Replace DOMAIN\TransferUser with your Windows user identity
icacls "D:\vol1\transfer-users" /grant "DOMAIN\TransferUser:(OI)(CI)M" /T

# Verify permissions
icacls "D:\vol1\transfer-users"
```

Utilisation d'alias de point d'accès S3 avec FSx

Lorsque vous utilisez des systèmes de fichiers FSx avec Transfer Family, vous devez utiliser des alias de point d'accès S3. Transfer Family ne prend pas en charge l'utilisation des ARN des points d'accès ou d'autres méthodes de référence pour le stockage FSx.

Important

AWS Transfer Family ne prend en charge les alias de point d'accès S3 que lors de l'utilisation de systèmes de fichiers FSx. Vous ne pouvez pas utiliser les ARN des points d'accès ou les URI de type hébergé virtuellement.

Important

Le point d'accès doit se trouver dans la même région que le volume.

À propos des alias de point d'accès

Lorsque vous créez un point d'accès S3 attaché à un volume FSx, Amazon S3 génère automatiquement un alias de point d'accès. Cet alias est un identifiant unique que vous pouvez utiliser partout où vous utilisez un nom de compartiment S3.

Pour les points d'accès attachés aux volumes FSx, l'alias utilise le format suivant :

```
access-point-name-metadata-ext-s3alias
```

Exemple d'alias :

```
my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias
```

 Note

Le `-ext-s3alias` suffixe est réservé aux alias des points d'accès FSx. Vous ne pouvez pas utiliser ce suffixe dans les noms de points d'accès.

Trouver l'alias de votre point d'accès

Vous pouvez trouver l'alias du point d'accès après avoir créé le point d'accès.

Pour trouver l'alias du point d'accès (console)

1. Ouvrez la console Amazon FSx à l'adresse. <https://console.aws.amazon.com/fsx/>
2. Dans le volet de navigation, sélectionnez Systèmes de fichiers.
3. Choisissez votre système de fichiers.
4. Choisissez l'onglet Volumes et sélectionnez le volume pour lequel vous avez créé le point d'accès.
5. Accédez à la colonne des détails du point d'accès S3.
6. L'alias est affiché dans la colonne Alias.

Pour trouver l'alias du point d'accès (CLI)

Utilisez la commande `describe-s3-access-point-attachments`.

```
aws fsx describe-s3-access-point-attachments \  
  --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

La réponse inclut l'alias :

```
{
```

```
"S3AccessPointAttachments": [  
  {  
    "S3AccessPoint": {  
      "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-fsx-  
ap",  
      "Alias": "my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias"  
    }  
  }  
]
```

Lorsque vous configurez les utilisateurs de Transfer Family, utilisez l'alias du point d'accès dans les mappages du répertoire de base.

Format du répertoire de base :

```
/access-point-alias/path/to/directory
```

Exemple :

```
/my-fsx-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias/users/jsmith
```

Configuration de Transfer Family pour le stockage FSx

Après avoir créé le point d'accès S3, configurez un serveur Transfer Family pour l'utiliser.

Création d'un rôle IAM

Vous devez créer un rôle IAM qui accorde à Transfer Family l'accès au point d'accès S3.

Important

Les politiques IAM nécessitent le format ARN du point d'accès, et non l'alias. Utilisez le format `arn:aws:s3:region:account-id:accesspoint/access-point-name` dans vos déclarations de ressources de politique IAM. L'alias du point d'accès (se terminant par `-ext-s3alias`) est uniquement utilisé pour les mappages de répertoires personnels.

Pour créer le rôle IAM

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

2. Dans le volet de navigation, choisissez Rôles, puis Create role.
3. Pour Type d'entité de confiance, choisissez Service AWS .
4. Pour Cas d'utilisation, choisissez Transférer.
5. Choisissez Suivant.
6. Choisissez Créer une politique et saisissez votre politique (voir exemple de politique ci-dessous).
7. Attachez la politique au rôle et choisissez Create role.

Exemple de politique IAM :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFileOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap/object/*"
    },
    {
      "Sid": "AllowDirectoryOperations",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:us-east-2:111122223333:accesspoint/my-fsx-ap"
    }
  ]
}
```

Gestion des utilisateurs pour le stockage FSx

Créez des utilisateurs Transfer Family avec des mappages de répertoire de base utilisant l'alias du point d'accès S3.

Création d'un utilisateur

Lorsque vous créez un utilisateur pour le stockage FSx, utilisez l'alias du point d'accès dans les mappages du répertoire de base.

Pour créer un utilisateur géré par le service (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. Choisissez votre serveur.
4. Dans la section Utilisateurs, choisissez Ajouter un utilisateur.
5. Dans Nom d'utilisateur, entrez un nom d'utilisateur.
6. Pour Rôle, choisissez le rôle IAM que vous avez créé.
7. Pour le répertoire personnel, choisissez Restreint.
8. Pour les mappages du répertoire de base, ajoutez un mappage à l'aide de l'alias du point d'accès :

```
[{"Entry": "/", "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgfyfouse1a-ext-s3alias/users/jsmith"}]
```

Pour créer un utilisateur (CLI)

Utilisez la commande `create-user`. Remplacez l'alias du point d'accès par votre alias.

```
aws transfer create-user \  
  --server-id s-0123456789abcdef0 \  
  --user-name jsmith \  
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \  
  --home-directory-type LOGICAL \  
  --home-directory-mappings '[  
    {  
      "Entry": "/",
```

```

        "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/
jsmith"
    }
  ]'

```

Configuration de mappages de répertoires multiples

Vous pouvez mapper plusieurs répertoires virtuels vers différents chemins sur le volume FSx.

Exemple : répertoires de chargement et de téléchargement séparés

```

aws transfer create-user \
  --server-id s-0123456789abcdef0 \
  --user-name jsmith \
  --role arn:aws:iam::111122223333:role/TransferFamilyFSxRole \
  --home-directory-type LOGICAL \
  --home-directory-mappings '[
    {
      "Entry": "/inbox",
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/
jsmith/inbox"
    },
    {
      "Entry": "/outbox",
      "Target": "/my-fsx-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias/users/
jsmith/outbox"
    }
  ]'

```

Configuration des clients de transfert de fichiers

Lorsque vous utilisez des systèmes de fichiers FSx avec Transfer Family, vous devez configurer vos clients de transfert de fichiers pour désactiver les fonctionnalités non prises en charge.

Configuration de WinSCP

WinSCP utilise par défaut une fonctionnalité de renommage temporaire qui n'est pas prise en charge par les points d'accès S3 pour FSx.

 Warning

Si vous ne désactivez pas la fonction de renommage temporaire dans WinSCP, les téléchargements de fichiers échoueront.

Pour désactiver le renommage temporaire dans WinSCP

1. Ouvrez WinSCP.
2. Dans la boîte de dialogue de connexion, choisissez Modifier pour modifier les paramètres de votre session.
3. Choisir Advanced (Avancé).
4. Dans le menu de navigation de gauche, sous Transfert, sélectionnez Endurance.
5. Pour Activer le transfert resume/transfer vers un nom de fichier temporaire, choisissez Désactiver.
6. Cliquez sur OK pour enregistrer les paramètres.

Vous pouvez également désactiver ce paramètre pour une session existante :

1. Connectez-vous à votre serveur Transfer Family.
2. Choisissez Options, puis Préférences.
3. Choisissez Transfer, puis Endurance.
4. Pour Activer le transfert resume/transfer vers un nom de fichier temporaire, choisissez Désactiver.
5. Choisissez OK.

Autres clients SFTP

Pour les autres clients SFTP, désactivez les fonctionnalités suivantes si elles sont disponibles :

- Chargements de fichiers temporaires (téléchargement vers un fichier temporaire, puis renommage)
- Reprendre les transferts à l'aide de fichiers temporaires
- Téléversements atomiques à l'aide d'opérations de renommage
- Mode d'ajout pour les téléchargements

Consultez la documentation de votre client pour connaître les étapes de configuration spécifiques.

Résolution des problèmes de stockage FSx

Cette section explique comment identifier et résoudre les problèmes courants liés à l'utilisation de Transfer Family avec les systèmes de fichiers FSx.

Problèmes liés au fonctionnement des fichiers

Autorisation refusée

Si vous recevez des messages d'erreur relatifs à l'autorisation refusée :

1. Vérifiez que le rôle IAM dispose des autorisations appropriées pour l'alias du point d'accès. Vous pouvez le faire en testant directement avec les API S3.
2. Vérifiez que la politique de point d'accès autorise le rôle IAM.
3. Vérifiez que l'utilisateur du système de fichiers dispose d'autorisations sur le chemin cible.
4. Vérifiez que le mappage du répertoire de base utilise le bon alias de point d'accès.

Le téléchargement échoue avec WinSCP

Si les téléchargements de fichiers échouent avec WinSCP, désactivez le renommage temporaire :

1. Dans WinSCP, choisissez Options, puis Préférences.
2. Choisissez Transfer, puis Endurance.
3. Pour Activer le transfert resume/transfer vers un nom de fichier temporaire, choisissez Désactiver.

Pour de plus amples informations, veuillez consulter [the section called “Configuration des clients de transfert de fichiers”](#).

Le téléchargement du fichier échoue

Si le téléchargement de fichiers échoue :

1. Vérifiez que la taille du fichier est inférieure à 5 Go.
2. Vérifiez que le volume FSx dispose d'un espace de stockage suffisant.
3. Surveillez CloudWatch les mesures de régulation.

Applications Web Transfer Family

Vous pouvez créer des applications Web pour activer une interface simple permettant de transférer des données vers et depuis Amazon Simple Storage Service (S3) via un navigateur Web. Cela ne vous oblige pas à créer ou à approvisionner AWS Transfer Family des serveurs.

Avant l'introduction des applications Web Transfer Family, les utilisateurs finaux devaient utiliser un client, une solution personnalisée ou une solution tierce pour accéder à leurs données dans Amazon S3. Cela s'explique par des exigences de sécurité strictes pour les clients et les partenaires, et par le fait que les applications des clients sont difficiles à utiliser pour les utilisateurs non techniques.

Avec le lancement des applications Web, vous pouvez désormais étendre un portail personnalisé, sécurisé et hautement disponible permettant à vos utilisateurs finaux de parcourir, de charger et de télécharger des données dans Amazon S3. Les applications Web sont intégrées de manière native à AWS IAM Identity Center Amazon S3 Access Grants. Cela signifie que seuls vos utilisateurs authentifiés peuvent consulter les données auxquelles ils sont autorisés à accéder. Les applications Web sont conçues à l'aide [de Storage Browser pour Amazon S3](#) et offrent les mêmes fonctionnalités à l'utilisateur final dans une offre entièrement gérée, sans avoir à écrire de code ou à héberger votre propre application.

Pour plus d'informations sur les autres applications Services AWS que vous utilisez avec les applications Web Transfer Family, consultez la documentation suivante :

- [Gestion de l'accès avec S3 Access Grants dans le guide de l'utilisateur d'Amazon Simple Storage Service](#)
- [AWS IAM Identity Center Guide de l'utilisateur](#)
- [Atelier sur les subventions d'accès Amazon S3](#)
- [Annonce d'applications AWS Transfer Family Web pour des transferts de fichiers Amazon S3 entièrement gérés](#)

Les ressources suivantes sont disponibles pour vous aider à démarrer avec les applications Web Transfer Family.

- Le guide de l'utilisateur propose une procédure détaillée, étape par étape, pour configurer une application Web Transfer Family ici : [Tutoriel : Configuration d'une application Web Transfer Family de base](#).

- Le centre de ressources AWS Getting Started propose un didacticiel ici : [Commencer à utiliser l'application AWS Transfer Family Web](#).
- Consultez [Commencer à utiliser l'application AWS Transfer Family Web](#).

Régions AWS pour les applications Web Transfer Family

AWS Transfer Family les applications Web sont disponibles dans toutes les régions prises en charge par Transfer Family, comme indiqué dans le [tableau des AWS régions](#), à l'exception de l'Asie-Pacifique (Nouvelle Zélande) AWS European Sovereign Cloud et.

Les points de terminaison VPC pour les applications Web sont pris en charge partout Régions AWS où les applications Web sont disponibles.

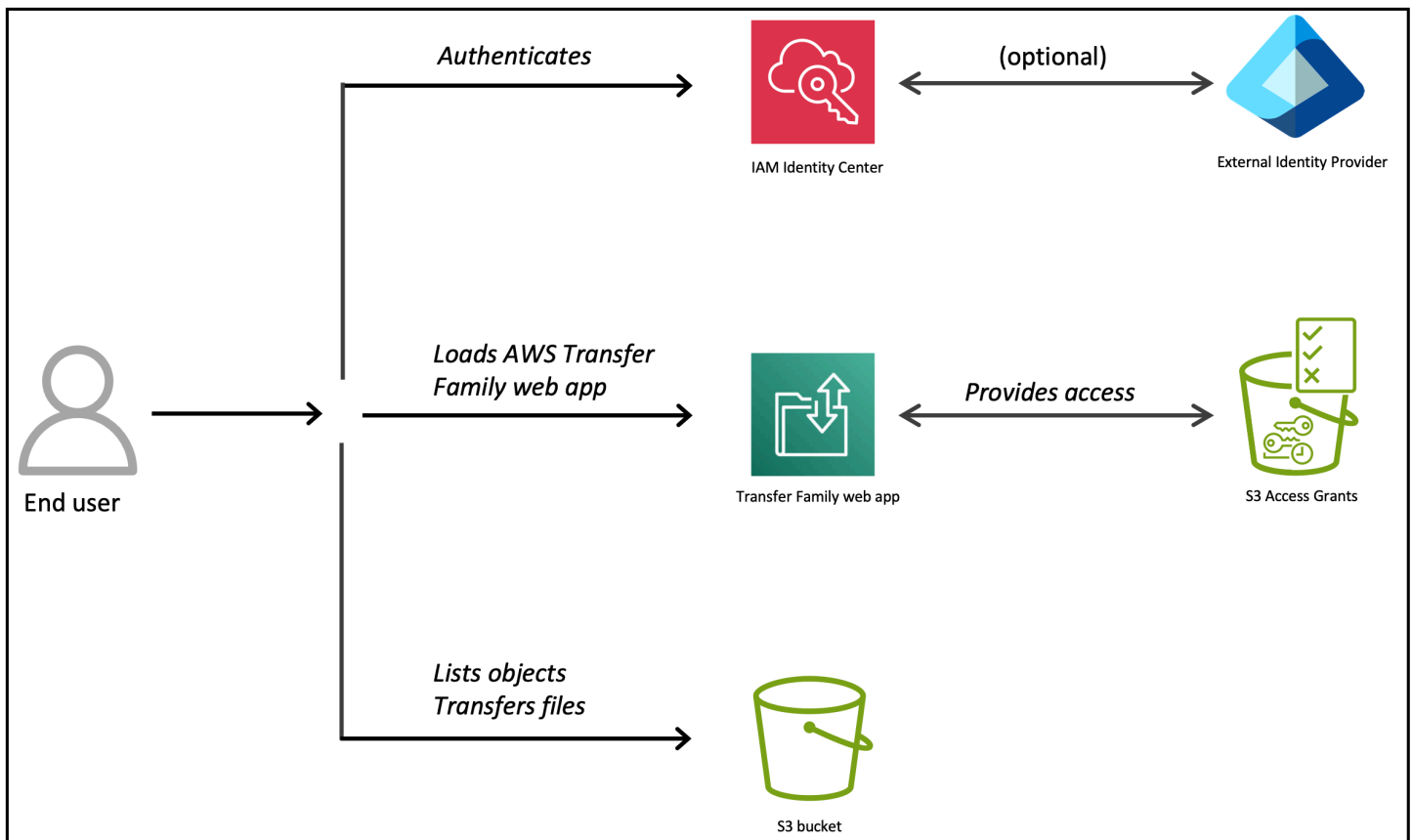
Compatibilité du navigateur pour AWS Transfer Family applications Web

Les applications Web Transfer Family sont compatibles avec les navigateurs suivants.

Navigateur	Version	Compatibilité
Microsoft Edge	Les trois dernières versions	Compatible
Mozilla Firefox	Les trois dernières versions	Compatible
Google Chrome	Les trois dernières versions	Compatible
Apple Safari	Les trois dernières versions	Compatible

Comment créer une application Web Transfer Family

Le schéma suivant illustre l'architecture de l'application Web Transfer Family.



Sur la base du schéma, vous pouvez voir que les applications Web Transfer Family interagissent avec les éléments suivants Services AWS :

- Amazon S3 pour le stockage et Amazon S3 Access Grants pour obtenir des informations d'identification de session.
- AWS IAM Identity Center en tant que fournisseur d'identité fédéré.
- Amazon CloudFront si vous configurez une URL personnalisée pour votre application Web.

Notez les limites suivantes lorsque vous utilisez des applications Web.

- Nombre maximum de résultats de recherche par requête : 10 000
- Les compartiments Amazon S3 utilisés par l'application Web Transfer Family doivent se trouver dans le même compte que l'application Web elle-même. Cross-account les buckets ne sont actuellement pas pris en charge.
- Étendue de recherche maximale par requête : 10 000 fichiers recherchés
- Taille de téléchargement maximale par fichier : 160 Go (149 GiB)
- Taille maximale du fichier à copier : 5,36 Go (5 GiB)

- Les noms de dossiers commençant ou se terminant par des points (.) ne sont pas pris en charge

Conditions préalables

Dans Gestion des identités et des accès AWS, configurez les rôles nécessaires. Collez les blocs de code que nous fournissons dans les instructions. Pour plus d'informations sur la configuration des rôles nécessaires, consultez [Configuration des rôles IAM pour les applications Web Transfer Family](#).

- Créez un rôle de porteur d'identité.
- Créez un rôle IAM à utiliser par S3 Access Grants. S3 Access Grants assume ce rôle IAM pour vendre des informations d'identification temporaires au bénéficiaire pour le site Amazon S3 enregistré.

Processus de création d'une application Web Transfer Family

Pour créer votre application Web et permettre à vos utilisateurs finaux de fonctionner, vous devez effectuer les tâches suivantes :

1. Configurez IAM Identity Center pour qu'il agisse en tant que fournisseur d'identité fédéré. Effectuez les tâches suivantes dans IAM Identity Center. Pour plus de détails sur la configuration d'IAM Identity Center, consultez [Configurer votre fournisseur d'identité pour les applications Web Transfer Family](#).
 - a. Créez une instance IAM Identity Center, si vous n'en avez pas déjà une.
 - b. Déterminez votre source d'identité. Il peut s'agir du répertoire IAM Identity Center par défaut ou d'un fournisseur tiers (par exemple Okta).
 - c. Créez ou identifiez les utilisateurs ou les groupes qui utiliseront votre application Web.
 - d. Si vous utilisez le répertoire IAM Identity Center comme source d'identité, notez les identifiants d'utilisateur ou de groupe que vous créez. Vous en aurez besoin ultérieurement lorsque vous créerez une autorisation d'accès à l'aide de S3 Access Grants.
2. Dans Amazon S3, configurez les autorisations d'accès Amazon S3. Pour plus d'informations sur S3 Access Grants, consultez [Configurer les subventions d'accès Amazon S3 pour les applications Web Transfer Family](#).
 - Créez une instance S3 Access Grants si vous n'en avez pas déjà une Région AWS.
 - Enregistrez votre position à l'aide du rôle IAM.
 - Créez l'autorisation d'accès.

3. Dans Transfer Family, effectuez les tâches suivantes.
 - a. Créez l'application Web Transfer Family. Pour plus d'informations sur la création de l'application Web Transfer Family, consultez [Configuration d'une application Web Transfer Family](#).
-  **Important**

Configurez le partage Cross-origin des ressources (CORS) pour tous les compartiments Amazon S3 utilisés par votre application Web. Pour plus d'informations sur la configuration de CORS, consultez [Configurer le partage Cross-origin des ressources \(CORS\) pour votre bucket](#).
- b. Attribuez des utilisateurs ou des groupes à l'application Web. Pour plus d'informations sur la façon d'attribuer des utilisateurs et des groupes, consultez [Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family](#).
 - c. (Facultatif) Mettez à jour le point de terminaison d'accès de votre application Web avec une URL personnalisée. Pour plus d'informations sur la création d'une URL personnalisée, consultez [Mettez à jour votre point de terminaison d'accès avec une URL personnalisée](#).
 - d. Fournissez à vos utilisateurs finaux l'URL du point de terminaison d'accès afin qu'ils puissent se connecter et interagir avec votre application Web.

Configurer votre fournisseur d'identité pour les applications Web Transfer Family

La section suivante décrit comment configurer votre fournisseur d'identité.

Pour commencer, vous devez disposer d'une source d'identité. Vous pouvez utiliser un annuaire IAM Identity Center ou un fournisseur d'identité externe. AWS Directory Service for Microsoft Active Directory Transfer Family utilise IAM Identity Center en tant que fournisseur d'identité fédéré, un système qui stocke les informations d'identification des utilisateurs et authentifie les utilisateurs de plusieurs organisations.

Si vous n'utilisez pas d'annuaire IAM Identity Center comme source d'identité, consultez les rubriques suivantes :

- [Gérer un fournisseur d'identité externe](#)

- [Se connecter à un annuaire Microsoft AD](#)
- [Instances d'organisation et de compte d'IAM Identity Center](#)
- [Tutoriels sur les sources d'identité IAM Identity Center](#)

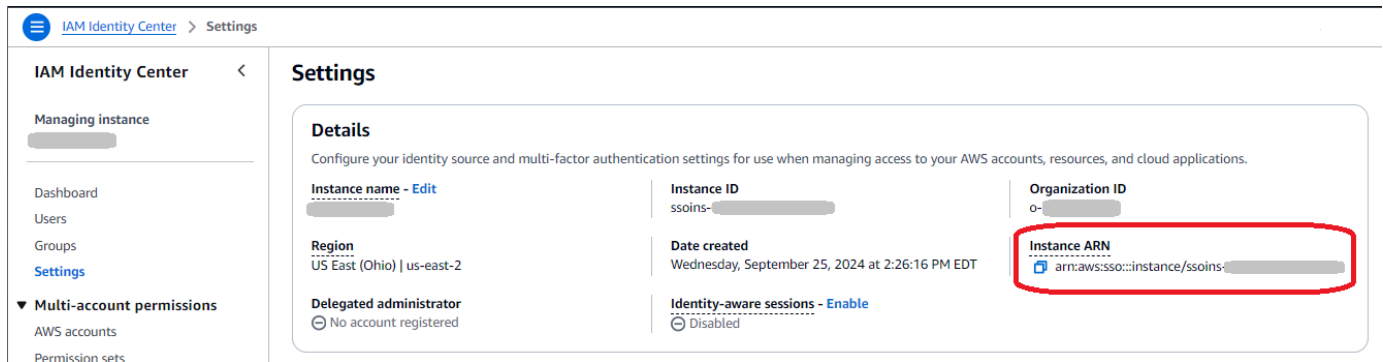
 Note

Vous ne pouvez avoir qu'une seule source d'identité dans IAM Identity Center, par instance, par Région AWS. Pour plus de détails, consultez la section [Conditions préalables et considérations relatives à l'IAM Identity Center](#).

Si vous envisagez d'utiliser le répertoire IAM Identity Center comme source d'identité et que vous souhaitez une configuration rapide, vous pouvez ignorer cette rubrique et passer [Création d'une application Web Transfer Family](#) à la section Création d'une instance IAM Identity Center à partir de l'assistant.

Pour configurer AWS IAM Identity Center à utiliser avec les applications Web Transfer Family

1. Connectez-vous à la AWS IAM Identity Center console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/singlesignon/>.
2. Vous pouvez créer et utiliser une instance de compte ou une instance d'organisation de AWS IAM Identity Center.
 - Pour plus de détails sur les instances de compte, voir [Créer une instance de compte de AWS IAM Identity Center](#). Avec une instance de compte d'IAM Identity Center, vous pouvez déployer des applications AWS gérées prises en charge et des applications gérées par le client basées sur OpenID Connect (OIDC). Les instances de compte prennent en charge les déploiements isolés d'applications en une seule instance Compte AWS, en tirant parti des fonctionnalités du portail d'identité et d'accès du personnel d'IAM Identity Center.
 - Pour plus de détails sur les instances d'organisation, consultez la section [Instances d'organisation d'IAM Identity Center](#). Vous pouvez gérer de manière centralisée l'accès des utilisateurs et des groupes à l'aide d'une seule instance d'organisation.
3. Sur la page des paramètres du centre d'identité IAM, notez l'ARN de votre instance. Vous aurez besoin de cette valeur lorsque vous créerez une instance Amazon S3 Access Grant.



4. Créez un ou plusieurs utilisateurs et, éventuellement, des groupes, à utiliser avec votre application Web Transfer Family. Si vous utilisez un annuaire IAM Identity Center comme fournisseur d'identité, vous pouvez également ajouter des utilisateurs directement depuis l'application Web elle-même. Pour de plus amples informations, veuillez consulter [Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family](#).

Configuration des rôles IAM pour les applications Web Transfer Family

Vous aurez besoin de deux rôles : un à utiliser comme rôle de porteur d'identité pour votre application Web, et un second à utiliser pour configurer une autorisation d'accès. Un rôle de porteur d'identité est un rôle qui inclut l'identité d'un utilisateur authentifié dans ses sessions. Il est utilisé pour demander à S3 Access Grants l'accès aux données au nom de l'utilisateur.

Note

Vous pouvez ignorer la procédure de création d'un rôle de porteur d'identité. Pour plus d'informations sur la création par le service Transfer Family du rôle de porteur d'identité, consultez [Création d'une application Web Transfer Family](#).

Vous pouvez ignorer la procédure de création d'un rôle d'autorisation d'accès. Dans la procédure de création d'une autorisation d'accès, à l'étape où vous enregistrez un emplacement S3, choisissez Create new role.

Créez un rôle de porteur d'identité

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.

2. Choisissez Rôles, puis Créer un rôle.
3. Choisissez Politique de confiance personnalisée, puis collez le code suivant.

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

4. Choisissez Suivant, puis ignorez Ajouter des autorisations et sélectionnez à nouveau Suivant.
5. Entrez un nom, par exemple `web-app-identity-bearer`.
6. Choisissez Créer un rôle pour créer le rôle du porteur d'identité.
7. Choisissez le rôle que vous venez de créer dans la liste, puis dans le panneau Politiques d'autorisations, choisissez Ajouter des autorisations > Créer une politique intégrée.
8. Dans l'éditeur de politiques, sélectionnez JSON, puis collez le bloc de code suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
        "s3:ListAccessGrantsInstances"
      ],
      "Resource": "*"
    }
  ]
}
```

9. Pour le nom de la stratégie, entrez `AllowS3AccessGrants`, puis sélectionnez **Créer une politique**.

Ensuite, vous créez le rôle que S3 Access Grants assume pour vendre des informations d'identification temporaires au bénéficiaire.

Note

Si vous autorisez le service à créer le rôle de porteur d'identité pour vous, ce rôle crée une confusion dans la protection des adjoints. Son code est donc différent de celui affiché ici.

Création d'un rôle d'autorisation d'accès

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à <https://console.aws.amazon.com/iam/> l'adresse.
2. Choisissez **Rôles**, puis **Créer un rôle**. Ce rôle doit être autorisé à accéder à vos données S3 dans le Région AWS.
3. Choisissez **Politique de confiance personnalisée**, puis collez le code suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

4. Choisissez **Suivant** pour ajouter une politique minimale, comme décrit dans [Enregistrer un emplacement](#). Bien que cela ne soit pas recommandé, vous pouvez ajouter la politique `AmazonS3FullAccess`, qui peut être trop permissive par rapport à vos besoins.

5. Choisissez Next, puis entrez un nom (par exemple `access-grants-location`).
6. Choisissez Create role pour créer le rôle.

 Note

Si vous autorisez le service à créer le rôle d'autorisation d'accès pour vous, ce rôle crée une confusion dans la protection des adjoints. Son code est donc différent de celui affiché ici.

Configuration d'une application Web Transfer Family

Cette section décrit les procédures de création d'une application Web Transfer Family. Pour attribuer des utilisateurs et des groupes autorisés à l'utiliser, voir [Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family](#).

 Note

Répétez ces procédures pour ajouter des applications Web supplémentaires. Vous pouvez réutiliser les rôles IAM que vous avez créés précédemment. Assurez-vous d'ajouter les points de terminaison d'accès pour les nouvelles applications Web à la politique de partage Cross-origin des ressources (CORS) de chaque compartiment.

Création d'une application Web Transfer Family

 Note

Si vous n'utilisez pas le répertoire IAM Identity Center pour votre fournisseur d'identité, n'essayez pas de créer une application Web tant que vous n'avez pas déjà configuré IAM Identity Center et configuré un fournisseur d'identité tiers, comme décrit dans. [Configurer votre fournisseur d'identité pour les applications Web Transfer Family](#)

Procédez comme suit pour créer une application Web Transfer Family.

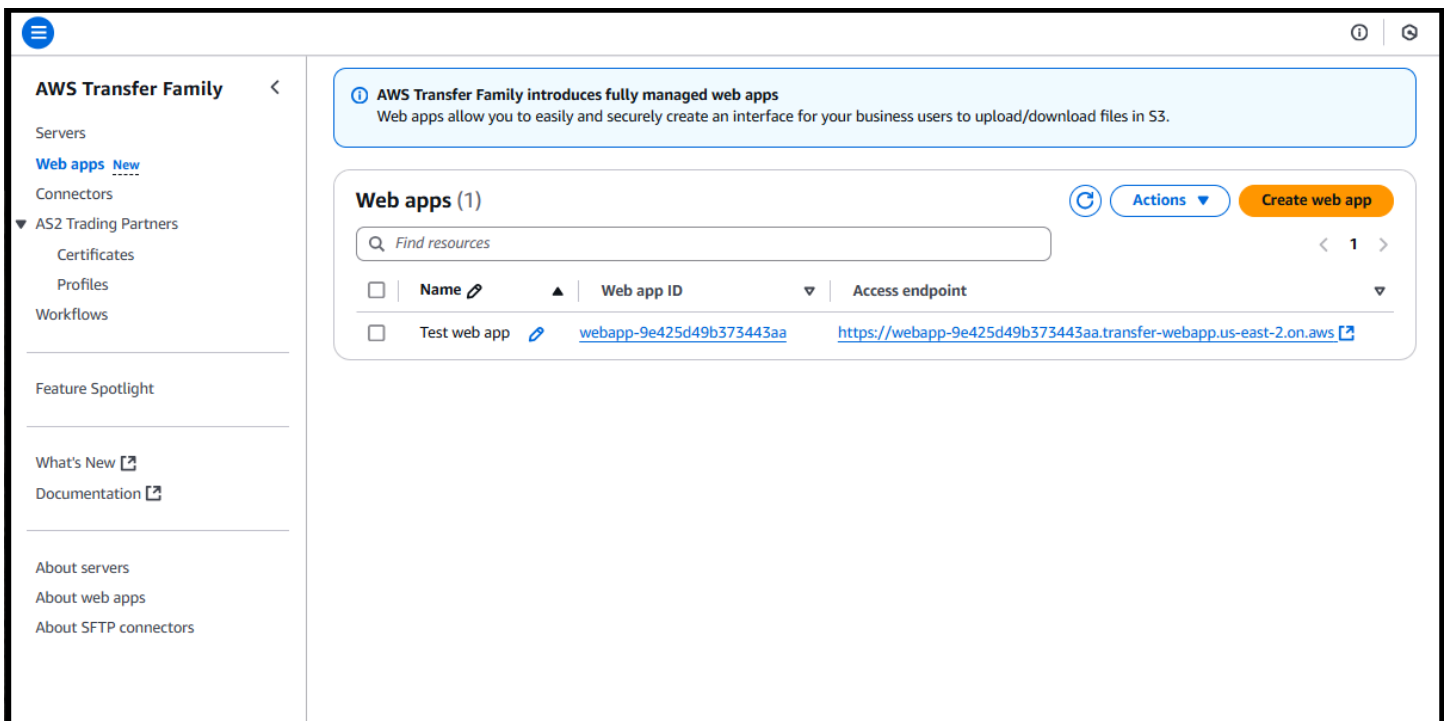
Pour créer une application Web Transfer Family

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 volet de navigation de gauche, sélectionnez Web apps.
3. Choisissez Créer une application Web.

Pour l'accès à l'authentification, le volet est rempli comme suit.

- Si vous avez déjà créé une organisation ou une instance de compte dans AWS IAM Identity Center, le message suivant s'affiche : Votre AWS Transfer Family application s'est connectée à une instance de compte d'IAM Identity Center.
 - Si vous possédez déjà une instance de compte et que vous êtes membre d'une instance d'organisation, vous avez la possibilité de choisir l'instance à connecter.
 - Si vous ne possédez pas encore d'instance de compte ou si vous êtes membre d'une instance d'organisation, les options vous sont proposées pour créer une instance de compte.
4. Pour le type de point de terminaison, choisissez le type de point de terminaison accessible au public. Pour un point de terminaison hébergé par un VPC, consultez. [Création d'une application Web Transfer Family dans un VPC](#)
 5. Dans le volet Type d'autorisation, vous pouvez utiliser un rôle créé précédemment ou demander au service d'en créer un pour vous.
 - Si vous avez déjà créé un rôle de porteur d'identité, choisissez Utiliser un rôle existant et choisissez votre rôle dans le menu Sélectionner un rôle existant.
 - Pour que le service crée un rôle pour vous, choisissez Créer et utilisez un nouveau rôle de service.
 6. Dans le volet des unités de l'application Web, choisissez une valeur. Une unité d'application Web permet l'activité d'une application Web pendant un maximum de 250 sessions uniques. Lorsque vous créez une application Web, vous fournissez le nombre d'unités dont vous avez besoin en fonction des pics de charge de travail attendus. La modification des unités de votre application Web a un impact sur votre facturation. Pour plus d'informations sur la tarification, consultez la section [AWS Transfer Family Tarification](#).
 7. Si vous utilisez Transfer Family dans un AWS GovCloud (US) Region, vous pouvez cocher la case point de terminaison compatible FIPS dans le volet FIPS Enabled. Pour toutes les autres options Régions AWS, cette option n'est pas disponible.

8. (Facultatif) Ajoutez une balise pour vous aider à organiser vos applications Web. Nous vous suggérons d'ajouter une balise avec Name comme clé et un nom descriptif comme valeur.
9. Choisissez Suivant. Sur cet écran, vous pouvez éventuellement fournir un titre pour votre application Web. Si vous ne fournissez pas de titre, le titre par défaut de Transfer Web App est fourni. Vous pouvez également télécharger des fichiers image pour votre logo et votre favicon.
10. Choisissez Suivant, puis sélectionnez Créer une application Web.



Note

Assurez-vous de configurer une politique de partage Cross-origin des ressources (CORS) pour tous les compartiments accessibles depuis le point de terminaison de l'application Web.

Adressage IP

Les applications Web Transfer Family utilisent des points de terminaison à double pile, prenant en charge la connectivité IPv4 et IPv6. Pour l'authentification, les applications Web utilisent AWS IAM Identity Center, qui prend également en charge l'IPv6 via des points de terminaison à double pile.

Si votre compte comportait des applications Web dans une région lorsque le support des terminaux IAM Identity Center à double pile a été lancé, toutes les applications Web de ce compte et de cette région continuent d'utiliser le point de terminaison IPv4-only IAM Identity Center à des fins de rétrocompatibilité. Cela s'applique aux applications Web existantes et nouvellement créées. Les comptes qui ne disposaient pas d'applications Web au moment du lancement utilisent le point de terminaison à double pile IAM Identity Center. Si vous devez modifier le point de terminaison IAM Identity Center utilisé par votre application Web, contactez le AWS Support.

Note

Pour déterminer le point de terminaison utilisé par votre application Web, inspectez l'URL lorsque vous êtes redirigé vers la page de connexion d'IAM Identity Center :

- IPv4-only: [Region].signin.aws.amazon.com
- Dual-stack: [Region].sso.signin.aws

Si votre entreprise utilise des pare-feux ou des passerelles réseau, autorisez à la fois les points de terminaison IPv4 existants et les nouveaux points de terminaison IAM Identity Center à double pile afin de garantir un accès ininterrompu quel que soit le point de terminaison utilisé par vos applications Web. Pour obtenir la liste complète des domaines et des points de terminaison d'URL à autoriser, consultez la section [Mettre à jour les pare-feux et les passerelles pour autoriser l'accès au portail d'accès dans le guide de l'utilisateur AWS d'IAM Identity Center](#).

Pour les applications Web hébergées dans un VPC, vous pouvez choisir le type d'adresse IP pour le point de terminaison de votre VPC : IPv4 uniquement ou double pile (IPv4 et IPv6). La valeur par défaut est Dual-Stack pour des raisons de rétrocompatibilité. Choisissez IPv4 si votre VPC l'IPv4-only est ou si vous n'avez pas besoin d'une connectivité IPv6. Vous pouvez modifier le type d'adresse IP après sa création en mettant à jour l'application Web.

Création d'une application Web Transfer Family dans un VPC

Cette section décrit les procédures de création d'une application Web Transfer Family dans un VPC. Vous pouvez héberger le point de terminaison de votre application Web dans un cloud privé virtuel (VPC) afin de transférer des données vers et depuis un compartiment Amazon S3 sans passer par Internet public. Pour attribuer des utilisateurs et des groupes autorisés à utiliser votre application Web, consultez [Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family](#).

 Note

Pour garantir un flux de données privé de bout en bout lors de l'utilisation d'un point de terminaison VPC de l'application Web Transfer Family, vous devez implémenter trois composants supplémentaires. Tout d'abord, configurez un PrivateLink point de terminaison pour les opérations de l'API Amazon S3 Control, qui est nécessaire pour les appels d'API Amazon S3 Access Grants. Ensuite, configurez un point de terminaison pour accéder aux données Amazon S3 à l'aide d'un point de terminaison PrivateLink Amazon S3 Gateway (pour le trafic provenant de votre VPC) ou d'un point de terminaison d'interface Amazon S3 (pour le trafic provenant de réseaux locaux via VPN ou Direct Connect). Troisièmement, bloquez l'accès à votre compartiment Amazon S3 en mettant à jour les politiques du compartiment afin d'autoriser uniquement le trafic provenant de ces points de terminaison VPC. Cette combinaison garantit que tous les transferts de données restent au sein de votre infrastructure réseau privée et ne transitent jamais par l'Internet public.

Création d'une application Web Transfer Family

Conditions préalables

- AWS IAM Identity Center configuré avec un fournisseur d'identité configuré. Consultez [Configurer votre fournisseur d'identité pour les applications Web Transfer Family](#).
- Configuration du VPC et des composants réseau. Reportez-vous à la section [Créer un VPC](#).
- Configuration du point de terminaison d'API pour les opérations Amazon S3 Control. Consultez la section [Accès aux points de terminaison de l'interface Amazon S3](#).
- Configuration des points de terminaison VPC pour Amazon S3 (passerelle ou interface). Consultez la section [Types de points de terminaison VPC pour Amazon S3](#). Si vous utilisez un point de terminaison d'interface, vous devez activer le DNS privé. Pour un exemple, consultez [Présentation de la prise en charge du DNS privé pour Amazon S3 avec AWS PrivateLink](#).

 Note

AWS IAM Identity Center ne prend pas en charge les points de terminaison VPC ; toutes les demandes d'authentification transitent par l'Internet public. En outre, les applications Web Transfer Family nécessitent un accès à Internet pour charger du contenu statique (tel que JavaScript des fichiers CSS et HTML). Les exigences relatives à l'accès public à Internet sont

distinctes de celles relatives à l'accès aux données. Votre point de terminaison VPC garantit que les connexions sont acheminées via votre infrastructure VPC.

Pour créer une application Web 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 volet de navigation de gauche, sélectionnez Web apps.
 3. Choisissez Créer une application Web. Pour l'accès à l'authentification, le volet est rempli comme suit.
 - Si vous avez déjà créé une organisation ou une instance de compte dans AWS IAM Identity Center, le message suivant s'affiche : Votre AWS Transfer Family application s'est connectée à une instance de compte d'IAM Identity Center.
 - Si vous possédez déjà une instance de compte et que vous êtes membre d'une instance d'organisation, vous avez la possibilité de choisir l'instance à connecter.
 - Si vous ne possédez pas encore d'instance de compte ou si vous êtes membre d'une instance d'organisation, les options vous sont proposées pour créer une instance de compte.
 4. Dans la section Configuration du point de terminaison, choisissez la manière dont vos utilisateurs accéderont à votre application Web :
 - Accessible au public : le point de terminaison de votre application Web est accessible au public via HTTPS. Cette option ne nécessite aucune configuration VPC, ce qui la rend simple à configurer et adaptée aux applications destinées à un large public.
 - Hébergé par VPC : le point de terminaison de votre application Web est hébergé dans votre Virtual Private Cloud (VPC), fournissant un accès au réseau privé via votre réseau VPC ou des connexions VPN. AWS Direct Connect Cette option offre une sécurité renforcée grâce à l'isolation du réseau et est recommandée pour les applications internes.
- Lors de la configuration d'un point de terminaison hébergé par VPC, vous devez spécifier :
- VPC : sélectionnez un VPC existant ou créez-en un nouveau. Un bouton Créer un VPC est disponible.
 - Type d'adresse IP : choisissez le type d'adresse IP pour votre point de terminaison VPC. Sélectionnez IPv4 pour la IPv4-only connectivité, ou Dual-stack pour la connectivité IPv4 et IPv6. La valeur par défaut est Dual-stack.

- Zones de disponibilité : Choisissez les zones de disponibilité dans lesquelles votre terminal sera déployé.
- Sous-réseaux : sélectionnez les sous-réseaux dans chaque zone de disponibilité choisie.
- Groupes de sécurité : sélectionnez ou créez des groupes de sécurité pour contrôler l'accès en fonction des adresses IP sources. S'il n'est pas spécifié, le groupe de sécurité par défaut du VPC est utilisé. Gérez les groupes de sécurité via la console VPC. Configurez vos groupes de sécurité VPC pour autoriser le trafic entrant en provenance de votre réseau via HTTPS sur le port TCP 443. Cela est nécessaire pour l'authentification IAM Identity Center et le chargement du contenu statique de l'application Web.

 Note

Le point de terminaison d'accès ne peut pas être personnalisé pour les points de terminaison VPC. Pour ajouter une URL personnalisée, utilisez le point de terminaison public.

Post-creation étapes

- Assurez-vous de configurer une politique de partage Cross-origin des ressources (CORS) pour tous les compartiments accessibles depuis le point de terminaison de l'application Web. Consultez [Cross-origin politique de partage des ressources \(CORS\)](#).
- Mettez à jour votre politique de compartiment pour autoriser uniquement le trafic provenant de votre VPC via le point de terminaison de votre VPC. Consultez [Restriction de l'accès à un point de terminaison d'un VPC spécifique](#).
- Attribuez ou ajoutez des utilisateurs ou des groupes à l'application Web Transfer Family. Consultez [Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family](#).

Cross-origin politique de partage des ressources (CORS)

Vous devez configurer le partage de ressources entre origines (CORS) pour tous les buckets utilisés par votre application Web. Pour plus d'informations sur le CORS, consultez [Configurer le partage Cross-origin des ressources \(CORS\) pour votre bucket](#).

⚠ Important

Avant d'utiliser l'exemple de politique suivant, remplacez l'origine autorisée par votre point de terminaison d'accès. Dans le cas contraire, vos utilisateurs finaux recevront un message d'erreur lorsqu'ils tenteront d'accéder à un emplacement sur votre application Web.

Exemple de politique :

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
    ],
    "ExposeHeaders": [
      "last-modified",
      "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
  }
]
```

Restriction de l'accès à un point de terminaison d'un VPC spécifique

Voici un exemple de stratégie de compartiment Amazon S3 qui restreint l'accès à un compartiment spécifique, `amzn-s3-demo-bucket`, uniquement à partir du point de terminaison d'un VPC doté de l'ID `vpce-1a2b3c4d`. Si le point de terminaison spécifié n'est pas utilisé, la politique refuse tout accès au compartiment. La condition `aws:SourceVpce` spécifie le point de terminaison. La condition `aws:SourceVpce` ne requiert pas d'ARN pour la ressource du point de terminaison de VPC, uniquement l'ID du point de terminaison de VPC. Pour plus d'informations sur la mise à jour de votre politique de compartiment afin d'autoriser uniquement le trafic provenant de votre VPC, consultez la section [Contrôle de l'accès depuis les points de terminaison du VPC](#) à l'aide de politiques de compartiment. Pour plus d'informations sur l'utilisation de conditions dans une politique, consultez la section [Exemples de politiques de bucket utilisant des clés de condition](#). Pour appliquer cette politique, vous devez créer un point de terminaison [Amazon S3 VPC](#).

Important

Avant d'utiliser l'exemple de stratégie suivant, remplacez l'ID de point de terminaison du VPC par une valeur appropriée pour votre cas d'utilisation. Dans le cas contraire, vous ne parviendrez pas à accéder à votre compartiment.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

```
}
```

Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family

Après avoir créé une application Web Transfer Family, vous pouvez attribuer des utilisateurs et des groupes qui peuvent ensuite accéder à l'application Web. Vous pouvez soit récupérer les utilisateurs déjà créés et stockés dans IAM Identity Center, soit [ajouter directement de nouveaux utilisateurs](#) (si vous utilisez un annuaire IAM Identity Center comme fournisseur d'identité). Si vous ajoutez de nouveaux utilisateurs, ils sont également ajoutés à votre instance IAM Identity Center.

Notez ce qui suit :

- Vous ne pouvez ajouter de nouveaux utilisateurs que si vous utilisez le répertoire IAM Identity Center comme source d'identité et si vous disposez des autorisations appropriées. Si vous êtes membre d'une instance d'organisation, il se peut que vous ne disposiez pas des autorisations nécessaires pour ajouter des utilisateurs.

Note

Si vous n'attribuez pas d'utilisateurs ou de groupes à votre application, vos utilisateurs recevront un message d'erreur lorsqu'ils tenteront de se connecter à votre application Web.

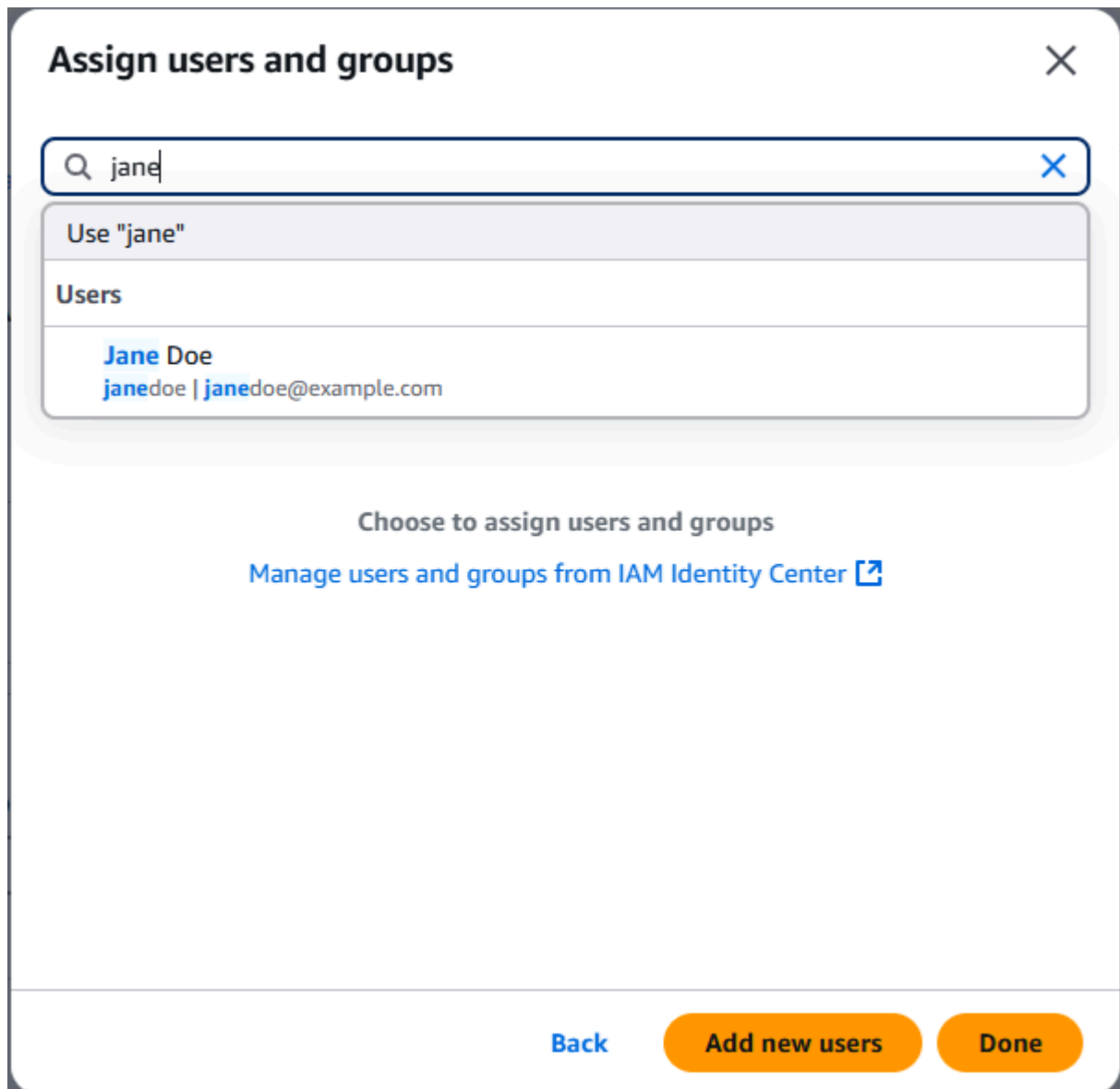
- Si vous créez un nouvel utilisateur, vous devez également créer une autorisation d'accès S3 pour cet utilisateur afin qu'il puisse accéder aux données de votre application Web.
- Une fois que vous avez créé un nouvel utilisateur, celui-ci reçoit un e-mail d'intégration d'IAM Identity Center contenant des instructions sur la marche à suivre.

Pour attribuer des utilisateurs à une application Web Transfer Family

1. Accédez à votre liste d'applications Web et choisissez celle que vous souhaitez modifier.
2. Choisissez Assign users and groups (Attribuer des utilisateurs et des groupes).

The screenshot shows the AWS IAM console interface for a web application named 'webapp-'. At the top, there are buttons for 'Assign users and groups' (orange), 'Clear customization', and 'Delete'. Below this is the 'Web app details' section, which includes an 'Access endpoint' (https://webapp-...transfer-webapp.us-east-2.on.aws), a 'Web app endpoint' (https://webapp-...-webapp.us-east-2.on.aws), and 'Web app units' (1). To the right, the 'Identity provider' is 'AWS IAM Identity Center', the 'IAM role' is a specific role, and the 'Instance ARN' is 'arn:aws:sso::instance/ssoins-...'. Below the details is a tabbed interface with 'Users' and 'Groups'. The 'Users' tab is active, showing 'Users (2)'. A search bar is present with the text 'Find resources'. Below the search bar is a table with columns: 'Display name', 'User ID', and 'Username'. Two users are listed in the table, each with a checkbox on the left and a link icon on the right.

3. Pour attribuer des utilisateurs que vous avez précédemment créés dans IAM Identity Center, sélectionnez Attribuer des utilisateurs et des groupes existants. Pour créer de nouveaux utilisateurs, passez directement à l'étape 4.
 - a. Un écran d'information apparaît. Choisissez Commencer pour continuer.
 - b. Recherchez l'utilisateur. Notez qu'aucun utilisateur n'apparaît tant que vous n'avez pas commencé à saisir vos critères de recherche. Vous devez effectuer la recherche par nom d'affichage, et non par nom d'utilisateur, s'il est différent. Seules les correspondances exactes sont renvoyées. Si vous ne trouvez pas votre utilisateur, accédez à la console de gestion IAM Identity Center, trouvez-le, puis copiez-collez son nom d'affichage ici.



- c. Choisissez les utilisateurs et les groupes à ajouter, puis choisissez Attribuer.
4. Pour créer un nouvel utilisateur, sélectionnez Ajouter et attribuez de nouveaux utilisateurs.
 - a. Un écran d'information apparaît. Choisissez Commencer pour continuer.
 - b. Choisissez Add new users (Ajouter de nouveaux utilisateurs).
 - c. Entrez les informations utilisateur suivantes dans la boîte de dialogue : nom d'utilisateur, prénom et adresse e-mail.

Add new users ✕

Information ✕
Newly-created users are enabled by default. To grant them access to Add User Widget, you must set their password in the IAM Identity Center console. [Manage user passwords in the IAM Identity Center console](#) 🔗

Username
A username is required for this person to sign in to the AWS access portal. You can't change the username later.

Maximum length of 128 characters. Can only contain alphanumeric characters or any of the following: `+ = , - @ _`

First name **Last name**

Email address **Confirm email address**

Display name
This is typically the full name of the user (first and last name) and appears in the users list.

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

- d. Choisissez Suivant, puis Ajouter pour ajouter l'utilisateur et fermer la boîte de dialogue, ou Ajouter un nouvel utilisateur pour créer un autre utilisateur.

Configurer le partage Cross-origin des ressources (CORS) pour votre bucket

Vous devez configurer le partage de ressources entre origines (CORS) pour tous les buckets utilisés par votre application Web. Une configuration CORS est un document qui définit des règles identifiant les origines auxquelles vous autoriserez l'accès à votre bucket. Pour plus d'informations sur CORS, voir [Configuration du partage de ressources entre origines \(CORS\)](#).

 Important

Si vous ne configurez pas CORS, vos utilisateurs finaux reçoivent un message d'erreur lorsqu'ils tentent d'accéder à un emplacement sur votre application Web.

Pour configurer le partage Cross-origin des ressources (CORS) pour votre compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez Buckets dans le panneau de navigation de gauche et recherchez votre compartiment dans la boîte de dialogue de recherche, puis choisissez l'onglet Autorisations.
3. Dans le partage de Cross-origin ressources (CORS), choisissez Modifier et collez le code suivant. *WebAppEndpoint* Remplacez-le par le point de terminaison d'accès réel de votre application Web. Il peut s'agir du point de terminaison d'accès public ou hébergé par un VPC créé lors de la création de l'application Web, ou d'un point de terminaison d'accès personnalisé, si vous en créez un. Veillez à ne pas saisir de barres obliques à la fin, car cela entraîne des erreurs lorsque les utilisateurs tentent de se connecter à votre application Web.
 - Exemple incorrect : `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
 - Exemples corrects :
 - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
 - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

Si vous réutilisez un bucket pour plusieurs applications Web, ajoutez leurs points de terminaison à la liste. `AllowedOrigins`

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
```

```
        "POST",
        "DELETE",
        "HEAD"
    ],
    "AllowedOrigins": [
        "https://WebAppEndpoint"
    ],
    "ExposeHeaders": [
        "last-modified",
        "content-length",
        "etag",
        "x-amz-version-id",
        "content-type",
        "x-amz-request-id",
        "x-amz-id-2",
        "date",
        "x-amz-cf-id",
        "x-amz-storage-class",
        "access-control-expose-headers"
    ],
    "MaxAgeSeconds": 3000
}
]
```

4. Choisissez Enregistrer les modifications pour mettre à jour le CORS.

Pour tester votre configuration CORS, voir [Tester CORS](#).

Configurer les subventions d'accès Amazon S3 pour les applications Web Transfer Family

Cette rubrique décrit comment ajouter une autorisation d'accès à l'aide d'Amazon S3 Access Grants. Cette autorisation d'accès définit l'accès à vos données directement aux utilisateurs et aux groupes de votre annuaire d'entreprise et fournit des informations d'identification temporaires « juste à temps », avec le moindre privilège, sur la base des autorisations accordées. Une autorisation individuelle dans une instance S3 Access Grants permet à un utilisateur ou à un groupe spécifique d'un annuaire d'entreprise d'accéder à un emplacement enregistré dans votre instance S3 Access Grants. Pour plus de détails, consultez les [concepts relatifs aux subventions d'accès S3](#) dans le guide de l'utilisateur Amazon S3.

 Note

Vous ne pouvez pas utiliser le répertoire IAM Identity Center avec S3 Access Grants autrement qu'avec les applications Web Transfer Family.

Vous devez spécifier une autorisation d'accès Amazon S3 pour la propagation de l'identité. Une autorisation d'accès Amazon S3 stocke les données auxquelles vos utilisateurs finaux doivent accéder. Lorsque vos utilisateurs finaux se connectent à votre application Web Transfer Family, S3 Access Grants transmet l'identité d'un utilisateur à l'application sécurisée. Cette section décrit comment ajouter et configurer une instance d'autorisation d'accès Amazon S3, puis une autorisation d'accès pour un compartiment Amazon S3.

 Note

Préparez l'[ARN et l'ID d'utilisateur ou de groupe de votre instance IAM Identity Center](#), car vous en aurez besoin pour terminer la configuration de votre autorisation d'accès.

Pour créer une subvention à l'aide d'Amazon S3 Access Grants

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/s3/>.
2. Créez un bucket ou notez un bucket existant à utiliser avec votre application Web. Pour plus d'informations sur la création de buckets, consultez le [guide de l'utilisateur Amazon S3](#).
3. Dans le volet de navigation de gauche, choisissez Access Grants.
4. Choisissez Create S3 Access Grants instance et fournissez les informations suivantes.
 - Sélectionnez Ajouter une instance IAM Identity Center dans **your-Region** laquelle se **your-Region** trouve votre Région AWS. Gardez cette case décochée si vous n'utilisez pas IAM Identity Center comme fournisseur d'identité.
 - Collez l'ARN de votre instance IAM Identity Center.

[Amazon S3](#) > [Access Grants](#) > Set up Access Grants Instance

- Step 1
☒ **Create S3 Access Grants instance**
- Step 2
☐ Register S3 Buckets or prefixes as locations
- Step 3
☐ Create grant
- Step 4
☐ Review and finish

Create S3 Access Grants instance [Info](#)

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

S3 Access Grants instance [Info](#)

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.

US East (Ohio) us-east-2

☒ Add IAM Identity Center instance in US East (Ohio) us-east-2 - *optional*

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

IAM Identity Center instance ARN

You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).

arn:aws:sso::instance/ssoins-

Format: arn:aws:sso::instance/<instanceidentifier>

Choisissez Next (Suivant) pour continuer.

- Enregistrez des compartiments ou des préfixes S3 en tant qu'emplacements. Nous vous recommandons d'enregistrer l'emplacement par défaut et de le mapper à un rôle IAM. `s3://` L'emplacement indiqué sur ce chemin par défaut couvre l'accès à tous vos compartiments Amazon S3 Région AWS de votre compte. Lorsque vous créez une autorisation d'accès, vous pouvez restreindre la portée à un compartiment, un préfixe ou un objet situé dans l'emplacement par défaut.

Saisissez les informations suivantes.

- Pour le champ d'application, recherchez un compartiment ou entrez le nom de votre compartiment, et éventuellement un préfixe.
- Pour le rôle IAM, choisissez Create new role pour que le service crée un rôle.

Vous pouvez également créer le rôle vous-même, comme décrit dans [Configuration des rôles IAM pour les applications Web Transfer Family](#), puis saisir son ARN ici.

Amazon S3 > Access Grants > US East (N. Virginia) us-east-1: default > Register location

Register location Info

Registering a location for S3 your S3 Access Grants instance assigns an IAM role the permission to get temporary credentials to access resources within the specified scope.

Location Info

Location scope Info

You can't edit the location scope after registering the location.

Scope

[View](#) [Browse S3](#)

Format for all buckets: s3://
 Format for bucket: s3://<bucket>
 Format for prefix: s3://<bucket>/<prefix-with-path>

Permissions

This IAM role allows S3 Access Grants to access your specified location scope.

ⓘ To ensure the role has proper permissions to access the location scope, consult the [list of permissions](#).

IAM role Info

This IAM role allows S3 Access Grants to access your specified location scope.

☒ Create new role
☐ Choose from existing IAM roles
☐ Enter IAM role ARN

[Cancel](#) [Register location](#)

Choisissez Next (Suivant) pour continuer.

6. Dans l'écran Créer une subvention, fournissez les informations suivantes.

- Pour les autorisations, sélectionnez Lire et écrire. Les autorisations d'accès peuvent être en lecture seule ou en lecture et écriture, mais l'écriture seule n'est pas prise en charge.
- Pour le type de bénéficiaire, choisissez Directory identity dans IAM Identity Center.
- Pour le type d'identité du répertoire, sélectionnez Utilisateur ou Groupe, selon le type que vous souhaitez enregistrer maintenant.
- Dans IAM Identity Center user/group ID, collez l'ID de votre utilisateur ou de votre groupe. Cet identifiant est disponible dans la console IAM Identity Center et dans votre application Web Transfer Family, dans le tableau des utilisateurs et des groupes.

Create Grant [Info](#)**Grant** [Info](#)

Grant a user or role a specific level of access to your S3 data.

Grant scope

The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

Location

s3://test

Location ID [Info](#)**IAM role** [Info](#)

[web-app-access-grants](#)

[Browse locations](#)

[Register location](#)

Subprefix - optional [Info](#)

Further scope the grant to a bucket, prefix, or an individual object.

*

Don't include any part of the grant already specified in the location.

Format for bucket: <bucket>/*

Format for prefix: <bucket>/<prefix-with-path>*

Format for object: <bucket>/<prefix-with-path>/<object>

Grant scope [Info](#)

s3://test/*

☐ The grant scope is an object

Permissions and access

Grant a user or role a specific level of access to your S3 data.

 The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

Permissions

☒ Read

☒ Write

Grantee type [Info](#)

☒ Directory identity from IAM Identity Center

☐ IAM principal

Directory identity type [Info](#)

☒ User

☐ Group

IAM Identity Center user ID [Info](#)

The user that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#)

Format: a1b2c3d4-5678-90ab-cdef-EXAMPLE1111

► **Application - optional**

Choisissez Suivant.

7. Vérifiez les paramètres à l'écran. Si tout est correct, choisissez Terminer pour créer l'autorisation d'accès. Vous pouvez également choisir Annuler ou Précédent pour apporter des modifications.

- Step 1
- Create S3 Access Grants instance
- Step 2
- Register S3 Buckets or prefixes as locations
- Step 3
- Create grant
- Step 4
- Review and finish

Review and finish

Step 1 - Create S3 Access Grants instance

S3 Access Grants instance

AWS Region

You can create one S3 Access Grants instance per AWS Region per account.
US East (Ohio) us-east-2

Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional

You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.
arn:aws:sso:::application/ssoinstance:/apl

Successfully created S3 Access Grants instance

Instance ARN: arn:aws:s3:us-east-2:::access-grants/default

You can grant other accounts access to this S3 Access Grants instance in the Resource Access Management console

Step 2 - Register S3 buckets or prefixes as locations

Location

Location scope

s3://

IAM role

web-app-beta-access-grants

Successfully registered location

Location ID:

Step 3 - Create grants

Grant

Grant a user or role a specific level of access to your S3 data.

Grant scope

s3:///*

IAM role

web-app-beta-access-grants

Location ID

Permissions and access

Access Type

READWRITE

Grantee type

Directory identity user

Grantee ID

Application - optional

Successfully created grant

Grant ARN: arn:aws:s3:us-east-2:::access-grants/default/grant/

Create another grant

Cancel

Previous

Finish

Configurer les autorisations d'accès Amazon S3

323

Amazon S3 > Access Grants > US East (Ohio) us-east-2: default

US East (Ohio) us-east-2: default

Share InstanceDelete Instance

S3 Access Grants provides scalable access control to data sets in your S3 buckets. To share an S3 Access Grants instance with external accounts by using the AWS Resource Access Manager console, choose Share instance. With S3 Access Grants, you can use identities from your corporate directory or from AWS Identity and Access Management (IAM) to control access. You can create one S3 Access Grants instance per AWS Region per account.

S3 Access Grants instance overview

Amazon Resource Name (ARN)
arn:aws:s3:us-east-2:account-id:access-grants/default

Creation date
October 25, 2024, 11:50:11 (UTC-04:00)

Account ID
account-id

IAM Identity Center

IAM Identity Center instance ARN
arn:aws:sso:us-east-2:account-id:application/ssoins-account-id/apl-account-id

DeregisterAdd

GrantsLocations

Grants (1)

DeleteCreate Grant

Find by grant scope or grantee

Grant scope	Grant ID	Permission	Grantee type	Grantee ID	Creation date	Location ID	Application ARN
s3://bucket-name/*	grant-id	Read, Write	Directory identity user	grantee-id	October 25, 2024, 11:57:30 (UTC-04:00)	location-id	ALL

La configuration de votre application Web est alors terminée. Les utilisateurs et les groupes que vous avez configurés peuvent accéder à l'application Web au point d'accès, se connecter et charger et télécharger des fichiers.

Mettez à jour votre point de terminaison d'accès avec une URL personnalisée

Le point de terminaison d'accès par défaut créé avec votre application Web contient des identifiants générés par le service. Pour offrir une expérience personnalisée, vous souhaitez peut-être fournir une URL personnalisée permettant à vos utilisateurs d'accéder à votre application Web Transfer Family. Cette rubrique décrit comment mettre à jour votre point de terminaison d'accès avec une URL personnalisée.

Note

Le point de terminaison d'accès ne peut pas être personnalisé pour les points de terminaison VPC. Pour ajouter une URL personnalisée, utilisez le point de terminaison public.

 Note

La procédure suivante repose sur l'utilisation du [modèle de CloudFormation pile](#) recommandé. Vous n'avez pas besoin d'utiliser le modèle : vous pouvez créer la distribution en utilisant directement la [CloudFront console](#).

Cependant, le modèle fourni simplifie le processus et permet d'éviter les erreurs de configuration. Si vous n'utilisez pas le CloudFormation modèle, veillez à suivre les consignes suivantes :

- La [politique de demande d'origine](#) doit transmettre les chaînes de requête et les cookies à l'origine, et non l'Host en-tête à l'origine.
- La [politique de cache](#) ne doit pas inclure l'Host en-tête dans la clé de cache.

Pour personnaliser l'URL de votre application Web

1. Créez une CloudFront distribution à l'aide du AWS CloudFormation modèle fourni par Transfer Family, [modèle de CloudFormation pile](#).
 - a. Ouvrez la CloudFormation console à l'adresse <https://console.aws.amazon.com/cloudformation>.
 - b. Choisissez Create stack et spécifiez ce qui suit.
 - Dans la section Prérequis - Préparer le modèle, choisissez Choisir un modèle existant.
 - Dans la section Spécifier un modèle, sélectionnez Charger un modèle de fichier.
 - Enregistrez le fichier du [modèle de CloudFormation pile](#), puis téléchargez-le ici.
 - c. Choisissez Next et fournissez les informations suivantes.
 - WebAppEndpoint: copiez la valeur depuis votre application Web
 - AccessEndpoint: indiquez le nom de domaine personnalisé que vous souhaitez utiliser
 - AcmCertificateArn: fournir l'ARN d'un SSL/TLS certificat public ou privé stocké dans AWS Certificate Manager
 - d. Terminez l' CloudFormation assistant jusqu'à ce que votre nouvelle pile soit créée.
2. Dans votre application Web, modifiez le point de terminaison Access en mettant à jour l'URL personnalisée en fonction de l'URL que vous souhaitez utiliser.

Edit web app details

Authentication access [Info](#)

Connect or create an Identity Center instance

Instance ARN

Select your instance ARN

Permission type [Info](#)☐ Create and use a new service role

Create and use an IAM role to allow the service to access the AWS resource it needs to create your application

☒ Use an existing role

Use an existing IAM role to allow the service to access the AWS resources it needs to create your application

By selecting use existing role, you need to manually create an IAM Role in order for the Transfer Family web application to access your AWS services data. Please select an existing IAM role below or [create a new role in IAM console](#)

Select an existing role

If your newly created role is not showing up in the dropdown list, please try the refresh button on the right

Find your IAM role

⚠ Make sure you have attached the trust policy and permission policy to the role you selected.[learn more about required policies](#)Access endpoint [Info](#)

Map your own fully qualified domain name to this web app so your end users can use your custom URL, not the service-provided URL to access your web app. Note- you can only complete this step in CloudFront after you have created the web app.

Custom URL

https://my-custom-url

[Create a new distribution](#)

3. Créez des enregistrements DNS pour acheminer le trafic de votre nom de domaine personnalisé vers la CloudFront distribution. Si vous utilisez Route 53 pour la zone, vous pouvez créer un enregistrement Alias ou CNAME pour le nom de CloudFront distribution (par exemple, xxxx.cloudfront.net). Pour plus d'informations sur l'utilisation d'Amazon Route 53 avec CloudFront, consultez [Configuration d'Amazon Route 53 pour acheminer le trafic vers une CloudFront distribution](#).
4. Mettez à jour votre politique de partage de ressources entre origines en remplaçant le point de terminaison d'accès par défaut par la ligne suivante dans le bloc de AllowedOrigins code :

```
"https://custom-url"
```

Vous devez effectuer cette modification pour chaque compartiment utilisé par votre application Web.

Après avoir effectué votre mise à jour, la AllowedOrigins section de votre politique CORS devrait ressembler à ce qui suit :

```
"AllowedOrigins": [
  "https://custom-url",
```

Vous n'avez besoin que d'une seule AllowedOrigins entrée pour chaque application Web Transfer Family.

Consultez la procédure de [configuration du partage Cross-origin des ressources \(CORS\) pour votre compartiment Amazon S3](#) pour plus de détails.

Vous pouvez désormais accéder à votre point de terminaison d'accès personnalisé et partager ce lien avec vos utilisateurs finaux.

CloudTrail enregistrement pour les applications Web Transfer Family

CloudTrail est un Service AWS qui crée un enregistrement des actions entreprises au sein de votre Compte AWS. Il surveille et enregistre en permanence les opérations d'API pour des activités telles que les connexions à la console, AWS Command Line Interface les commandes et SDK/API les opérations. 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 les applications Web Transfer Family, vous pouvez suivre à la fois les événements d'authentification et les opérations d'accès aux données effectuées par vos utilisateurs. Pour activer la journalisation complète, vous devez :

1. Configurez CloudTrail pour consigner les événements de gestion afin de suivre les activités d'authentification.
2. Activez les événements de données Amazon S3 pour suivre les opérations sur les fichiers effectuées via votre application Web.

Voir aussi

- [CloudTrail cas d'utilisation d'IAM Identity Center](#)
- [Comprendre les événements de connexion à IAM Identity Center](#)
- [CloudTrail Élément UserIdentity](#)
- [Activation de la journalisation des CloudTrail événements pour les compartiments et les objets S3](#)
- [CloudTrail Événements Amazon S3](#)

Activation des événements de données Amazon S3

Pour suivre les opérations de fichiers effectuées via les applications Web Transfer Family sur vos compartiments Amazon S3, vous devez activer les événements de données pour ces compartiments. Les événements de données fournissent une activité d'API au niveau de l'objet et sont particulièrement utiles pour suivre les chargements de fichiers, les téléchargements et les autres opérations effectuées par les utilisateurs d'applications Web.

Pour activer les événements de données Amazon S3 pour votre application Web Transfer Family :

1. Ouvrez la CloudTrail console à l'adresse <https://console.aws.amazon.com/cloudtrail/>.
2. Dans le volet de navigation, choisissez Sentiers, puis sélectionnez un parcours existant ou créez-en un nouveau.
3. Sous Sélecteurs d'événements avancés, choisissez Modifier.
4. Choisissez Ajouter un sélecteur d'événements avancé.
5. Pour le premier sélecteur de champs :
 - Régler le champ sur `eventCategory`
 - Définir l'opérateur sur `Equals`
 - Définissez la valeur sur `Data`
6. Choisissez Ajouter un champ et pour le second sélecteur de champ :
 - Régler le champ sur `resources.type`
 - Définir l'opérateur sur `Equals`
 - Définissez la valeur sur `AWS::S3::Object`
7. (Facultatif) Pour enregistrer les événements relatifs à des compartiments spécifiques uniquement, choisissez Ajouter un champ et ajoutez :
 - Régler le champ sur `resources.ARN`
 - Configurer l'opérateur pour qu'il commence par
 - Définissez la valeur sur `arn:aws:s3:::your-bucket-name/`
8. Sélectionnez Enregistrer les modifications.

Vous pouvez également utiliser l'ancienne configuration des événements de données :

1. Sous Événements liés aux données, sélectionnez Modifier.
2. Pour le type d'événement `Data`, sélectionnez le bucket S3 et les événements d'objet.

3. Choisissez les compartiments Amazon S3 pour lesquels enregistrer les événements de données. Vous pouvez sélectionner Tous les compartiments S3 actuels et futurs ou spécifier des compartiments individuels.
4. Choisissez de consigner les événements de lecture, d'écriture ou les deux.
5. Sélectionnez Enregistrer les modifications.

Après avoir activé les événements de données, vous pouvez accéder à ces journaux dans le compartiment Amazon S3 configuré pour CloudTrail. Les journaux contiennent des informations telles que l'utilisateur qui a effectué l'action, l'horodatage de l'action, l'objet spécifique concerné et le `onBehalfOf` champ permettant de suivre les `userId` actions effectuées via les applications Web Transfer Family.

Trouver et consulter vos journaux

Il existe plusieurs méthodes pour rechercher et consulter CloudTrail les journaux de votre application Web Transfer Family :

Utilisation de la CloudTrail console

Le moyen le plus rapide de consulter les événements récents :

1. Ouvrez la CloudTrail console à l'adresse <https://console.aws.amazon.com/cloudtrail/>.
2. Choisissez Historique des événements.
3. Filtrer les événements par :
 - Source de l'événement : `signin.amazonaws.com` pour les événements liés aux applications Web
 - Source de l'événement : `s3.amazonaws.com` pour les opérations sur les fichiers
4. Cliquez sur n'importe quel événement pour afficher des informations détaillées.

Accès aux journaux dans Amazon S3

Pour accéder à l'intégralité des fichiers journaux stockés dans Amazon S3 :

1. Identifiez le compartiment Amazon S3 de votre CloudTrail parcours :

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output table
```

2. Accédez aux fichiers journaux dans Amazon S3 :

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/
```

3. Téléchargez et recherchez dans les fichiers journaux l'identifiant de votre application Web :

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/DD/ . --recursive
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

Utilisation AWS CLI pour rechercher des événements

Recherchez des événements d'applications Web spécifiques à l'aide de AWS CLI :

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

Ou recherchez des événements d'authentification :

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "UserAuthentication" \
  --start-time $(date -d "1 day ago" +%s)000
```

Exemples de journaux d'authentification

CloudTrail enregistre les événements d'authentification pour les applications Web Transfer Family, ce qui peut vous aider à suivre les tentatives de connexion réussies et infructueuses. Ces journaux sont particulièrement utiles à des fins de surveillance de la sécurité et de conformité.

Rubriques

- [Exemple d'entrée de journal pour la vérification des informations d'identification](#)
- [Exemple d'entrée de journal pour l'authentification de connexion](#)
- [Exemple d'entrée de journal pour ListCallerAccessGrants](#)

- [Exemple d'entrée de journal pour un GetDataAccess événement](#)

Exemple d'entrée de journal pour la vérification des informations d'identification

L'exemple suivant montre une entrée de CloudTrail journal pour un événement de vérification des informations d'identification qui se produit pendant le processus d'authentification.

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"
  },
  "eventTime": "2025-08-08T15:29:30Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.224",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
    "CredentialType": "PASSWORD"
  },
  "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
  "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
  "readOnly": false,
  "eventType": "AWS ServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
```

```

    "CredentialVerification": "Success"
  },
  "eventCategory": "Management"
}

```

Cet événement fournit des informations supplémentaires sur l'étape de vérification des informations d'identification du processus d'authentification, en indiquant l'ID d'identification et l'ID du flux de travail d'authentification spécifiques utilisés.

Exemple d'entrée de journal pour l'authentification de connexion

L'exemple suivant montre une entrée de CloudTrail journal pour un événement d'authentification utilisateur réussi lors de la connexion à une application Web à l'aide d'IAM Identity Center.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "123456789012",
    "arn": "",
    "accountId": "123456789012",
    "accessKeyId": "",
    "userName": "demo-user-2",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/d-9a670c546e"
    },
    "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
  },
  "eventTime": "2025-08-07T14:09:07Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.14",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
    "LoginTo": "https://example.awsapps.com/start/",
    "CredentialType": "PASSWORD"
  }
}

```



```

    },
    "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",
    "eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
    "readOnly": false,
    "eventType": "AWS ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
      "UserAuthentication": "Success"
    },
    "eventCategory": "Management"
  }
}

```

Dans cet exemple, notez les champs importants suivants :

- `eventSource`: affiche « `signin.amazonaws.com` », indiquant qu'il s'agit d'un événement d'authentification IAM Identity Center.
- `userIdentity.onBehalfOf`: contient l'ID utilisateur et l'ARN du magasin d'identités de l'utilisateur de l'application Web.
- `additionalEventData.LoginTo`: indique l'URL de l'application IAM Identity Center à laquelle vous accédez.
- `additionalEventData.CredentialType`: indique la méthode d'authentification utilisée (MOT DE PASSE).
- `serviceEventDetails`: affiche le résultat de l'authentification (réussite).

Exemple d'entrée de journal pour ListCallerAccessGrants

L'exemple suivant montre une entrée de CloudTrail journal pour un `ListCallerAccessGrants` événement qui se produit lorsque l'application Web Transfer Family demande les autorisations d'accès disponibles pour un utilisateur.

```

{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:aws-transfer",
    "arn": "arn:aws:sts::123456789012:assumed-role/AWS
TransferWebAppIdentityBearer-us-east-2/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",

```

```

    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/service-role/AWS
TransferWebAppIdentityBearer-us-east-2",
        "accountId": "123456789012",
        "userName": "AWS TransferWebAppIdentityBearer-us-east-2"
      },
      "attributes": {
        "creationDate": "2025-08-08T15:29:34Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
    },
    "eventTime": "2025-08-08T15:29:35Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "ListCallerAccessGrants",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
      "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
      "allowedByApplication": "true",
      "maxResults": "100"
    },
    "responseElements": null,
    "additionalEventData": {
      "SignatureVersion": "SigV4",
      "CipherSuite": "TLS_AES_128_GCM_SHA256",
      "bytesTransferredIn": 0,
      "AuthenticationMethod": "AuthHeader",
      "x-amz-id-2": "1g34AaAELn/
fntxwriFVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
      "bytesTransferredOut": 462
    },
    "requestID": "48485MTZEDWT0ANT",
    "eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",

```

```
"readOnly": true,
"resources": [
  {
    "accountId": "123456789012",
    "type": "AWS:S3::AccessGrantsInstance",
    "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
  }
],
"eventType": "AWS ApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management"
}
```

Dans cet exemple, notez les champs importants suivants :

- `eventName`: indique qu'il s'agit d'un `ListCallerAccessGrants` événement qui interroge les autorisations d'accès S3 disponibles.
- `requestParameters.allowedByApplication`: indique que la requête est filtrée en fonction des autorisations autorisées par l'application.
- `requestParameters.maxResults`: indique le nombre maximum de subventions à renvoyer dans la réponse.
- `userIdentity.onBehalfOf`: lie la demande à l'utilisateur spécifique de l'application Web.

Cet événement permet de savoir quand l'application Web Transfer Family demande à quelles ressources S3 un utilisateur a accès, offrant ainsi une visibilité sur les opérations de découverte des autorisations d'accès.

Exemple d'entrée de journal pour un `GetDataAccess` événement

L'exemple suivant montre une entrée de CloudTrail journal pour un `GetDataAccess` événement qui se produit lorsque l'application Web Transfer Family demande des autorisations d'accès aux ressources S3 au nom d'un utilisateur.

```
{
  "eventVersion": "1.11",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROASEQRAEABP7ADWEZA5:aws-transfer",
```

```

    "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-
ap-southeast-1/aws-transfer",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROASEQRAEABP7ADWEZA5",
        "arn": "arn:aws:iam::123456789012:role/service-role/
AWSTransferWebAppIdentityBearer-ap-southeast-1",
        "accountId": "123456789012",
        "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
      },
      "attributes": {
        "creationDate": "2025-05-08T16:09:05Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "transfer.amazonaws.com",
    "onBehalfOf": {
      "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9667b0da7a",
      "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
    }
  },
  "eventTime": "2025-05-08T16:10:25Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetDataAccess",
  "awsRegion": "ap-southeast-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
    "durationSeconds": 900,
    "permission": "READWRITE",
    "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
  },
  "responseElements": null,
  "additionalEventData": {
    "AuthenticationMethod": "AuthHeader",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "SignatureVersion": "SigV4",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2244,

```

```

    "x-amz-id-2": "8ce8sZ0gNwsaj9w1mzagyA
+cs0NjYl8FgEw4FGpE8DARi90aNC0RfWlTYNE7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fM="
  },
  "requestID": "BXGSKKQXCWS5RAHB",
  "eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
  "readOnly": true,
  "resources": [
    {
      "type": "AWS:S3::AccessGrantsInstance",
      "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
      "accountId": "123456789012"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management"
}

```

Dans cet exemple, notez les champs importants suivants :

- `eventName`: indique qu'il s'agit d'un `GetDataAccess` événement qui se produit lorsque Transfer Family demande des autorisations d'accès aux ressources S3.
- `userIdentity.onBehalfOf`: contient l'ARN du magasin d'identités et l'ID utilisateur, reliant la demande d'accès à l'utilisateur spécifique de l'application Web.
- `requestParameters.target`: indique le modèle de chemin S3 pour lequel l'accès a été demandé.
- `requestParameters.permission`: indique le type d'accès demandé (READWRITE, READ ou WRITE).
- `requestParameters.durationSeconds`: indique la durée de validité de l'autorisation d'accès (généralement 900 seconds/15 minutes).
- `sourceIPAddress` et `userAgent` : Les deux affichent « `transfer.amazonaws.com` », indiquant qu'il s'agit d'une demande de service interne.

`GetDataAccess` les événements sont particulièrement utiles pour suivre le moment où les utilisateurs de l'application Web Transfer Family ont accès à des ressources S3 spécifiques, ce qui vous permet de surveiller les modèles d'accès et de garantir une autorisation appropriée.

Afficher les entrées du CloudTrail journal

Vous pouvez consulter et analyser les entrées du CloudTrail journal de votre application Web Transfer Family de plusieurs manières :

Utilisation de la CloudTrail console

La CloudTrail console fournit une interface conviviale permettant de visualiser et de filtrer les entrées du journal :

1. Ouvrez la CloudTrail console à l'adresse <https://console.aws.amazon.com/cloudtrail/>.
2. Dans le panneau de navigation, sélectionnez Historique des événements.
3. Utilisez les options de filtre pour affiner les événements :
 - Définissez la source de l'événement sur `transfer.amazonaws.com` pour afficher uniquement les événements Transfer Family.
 - Filtrez par nom d'événement pour voir des opérations spécifiques telles que `UserAuthentication`.
 - Utilisez la plage de temps pour vous concentrer sur les événements survenus au cours d'une période spécifique.
4. Cliquez sur n'importe quel événement pour voir ses informations détaillées.

Accès aux journaux dans Amazon S3

Si vous avez configuré un CloudTrail suivi pour envoyer des journaux vers un compartiment Amazon S3, vous pouvez accéder directement aux fichiers journaux bruts :

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Accédez au compartiment et au préfixe dans lesquels vos CloudTrail journaux sont stockés.
3. Les journaux sont organisés par année, mois, jour et région. Accédez au répertoire approprié.
4. Téléchargez et ouvrez les fichiers journaux, qui sont au format JSON.

Résolution des problèmes liés à vos applications Web

Note

Ces conseils de dépannage sont destinés à l'administrateur de l'application Web plutôt qu'à l'utilisateur final. Pour les utilisateurs finaux, si vous rencontrez des problèmes, contactez l'administrateur de votre application Web. Toutes les instances dans les paragraphes suivants font référence à l'administrateur de l'application Web.

Résoudre les erreurs réseau

Description

Votre utilisateur final voit une bannière réseau Erreur réseau lors du chargement du point de terminaison de l'application Web.

Cause

Les problèmes les plus courants sont les suivants :

- L'administrateur n'a pas désigné l'utilisateur qui tente de se connecter à la nouvelle application.
- L'administrateur n'a pas ajouté les actions nécessaires à vos rôles IAM.
- La liste des autorisations d'accès S3 attribuées à votre utilisateur s'affiche, mais CORS n'est pas configuré correctement pour votre ou vos compartiments Amazon S3.

Solution

- Dans IAM Identity Center, assurez-vous d'affecter l'utilisateur à l'application appropriée. Ou, si un groupe vous est attribué, assurez-vous que l'utilisateur qui tente de se connecter appartient au bon groupe. Ceci est décrit sous [Attribuer ou ajouter des utilisateurs ou des groupes à une application Web Transfer Family](#).
- Vérifiez si vos rôles contiennent les actions nécessaires dans la politique de confiance personnalisée pour sts:AssumeRole les deux sts:SetContext actions. Ceci est décrit sous [Configuration des rôles IAM pour les applications Web Transfer Family](#).
- Vérifiez la politique CORS pour tous les buckets utilisés par votre application Web. Ceci est décrit dans [Configurer le partage Cross-origin des ressources \(CORS\) pour votre compartiment Amazon S3](#).

Résoudre les problèmes liés à l'absence d'affichage du bucket configuré

Description

Tout semble être correctement configuré, mais le compartiment Amazon S3 n'apparaît pas dans l'application Web.

Cause

L'une des causes possibles est que le compartiment Amazon S3 ne se trouve pas dans le même compte que l'application Web.

Solution

Assurez-vous que le compartiment Amazon S3 se trouve dans le même compte que l'application Web. Cross-account buckets ne sont actuellement pas pris en charge.

Résoudre les erreurs d'URL personnalisées

Description

Lorsque votre utilisateur final se connecte à l'application Web, il reçoit le message d'erreur Échec de l'autorisation : code d'autorisation manquant.

Cause

Si vous avez utilisé CloudFront directement, plutôt que le CloudFormation modèle fourni, vous avez probablement mal configuré la politique de demande d'origine afin de ne pas transmettre les chaînes de requête.

Solution

Mettez à jour votre politique de demande d'origine pour transférer les chaînes de requête et les cookies à l'origine.

Description

Lorsque votre utilisateur final tente d'accéder à une application Web Transfer Family, il reçoit une réponse 404.

Cause

Si vous avez utilisé CloudFront directement, plutôt que le CloudFormation modèle fourni, vous avez probablement mal configuré la politique de cache pour inclure l'Hosten-tête dans la clé de cache ou mal configuré la politique de demande d'origine pour transférer l'Hosten-tête.

Solution

- Assurez-vous que votre politique de cache n'inclut pas l'Hosten-tête dans la clé de cache
- Assurez-vous que votre politique de demande d'origine ne transmet pas l'Hosten-tête.

Résoudre les erreurs diverses

Description

Votre utilisateur final ne peut pas se connecter, ne peut consulter aucun compartiment ou fichier, ou vous recevez un autre message d'erreur.

Cause

L'une des causes possibles est que l'ARN de l'instance IAM Identity Center ne correspond pas à la valeur de l'ARN de vos autorisations ou de l'ARN de l'instance IAM Identity Center de votre application Web.

Solution

Vérifiez les éléments suivants pour voir s'ils correspondent.

- Dans IAM Identity Center, accédez à Paramètres et consultez l'ARN de l'instance.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

- Dans Amazon S3, accédez à Access Grants et consultez l'ARN de votre instance IAM Identity Center.

```
arn:aws:sso:::account-id:application/ssoins-instance-identifier/apl-1234567890abcdef0
```

- Dans Transfer Family, accédez à la page de détails de votre application Web et consultez son ARN d'instance.

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

La *instance-identifier* valeur doit être la même à ces trois endroits.

Des compartiments S3 dupliqués apparaissent dans l'application Web

Description

Les utilisateurs voient le même bucket S3 répertorié plusieurs fois dans l'interface de l'application Web Transfer Family.

Cause

Cela se produit lorsqu'un utilisateur fait partie de plusieurs groupes Active Directory qui ont des autorisations dupliquées pour le même compartiment S3. L'application Web répertorie toutes les autorisations de haut niveau associées à l'utilisateur (UID ou GID), que l'utilisateur dispose ou non de plusieurs autorisations attribuées au même emplacement de compartiment.

Solution

Pour résoudre ce problème, les administrateurs doivent dédupliquer les autorisations afin que chaque utilisateur ne dispose que d'une seule autorisation pour chaque emplacement S3. Passez en revue la configuration de vos autorisations d'accès S3 et consolidez les autorisations dupliquées pour le même compartiment dans différents groupes Active Directory.

Instructions destinées à l'utilisateur final pour les applications Web Transfer Family

Note

Dans cette rubrique, les informations sont destinées aux utilisateurs finaux qui interagissent avec l'application Web. Dans cette rubrique, toutes les instances où vous vous trouvez font référence à des utilisateurs finaux.

Cette rubrique décrit comment accéder à une application AWS Transfer Family Web que vous êtes autorisé à utiliser et comment vous pouvez interagir avec elle.

Quotas d'applications Web

Notez les limites suivantes lorsque vous utilisez des applications Web.

- Nombre maximum de résultats de recherche par requête : 10 000
- Les compartiments Amazon S3 utilisés par l'application Web Transfer Family doivent se trouver dans le même compte que l'application Web elle-même. Cross-account les buckets ne sont actuellement pas pris en charge.
- Étendue de recherche maximale par requête : 10 000 fichiers recherchés
- Taille de téléchargement maximale par fichier : 160 Go (149 GiB)
- Taille maximale du fichier à copier : 5,36 Go (5 GiB)
- Les noms de dossiers commençant ou se terminant par des points (.) ne sont pas pris en charge

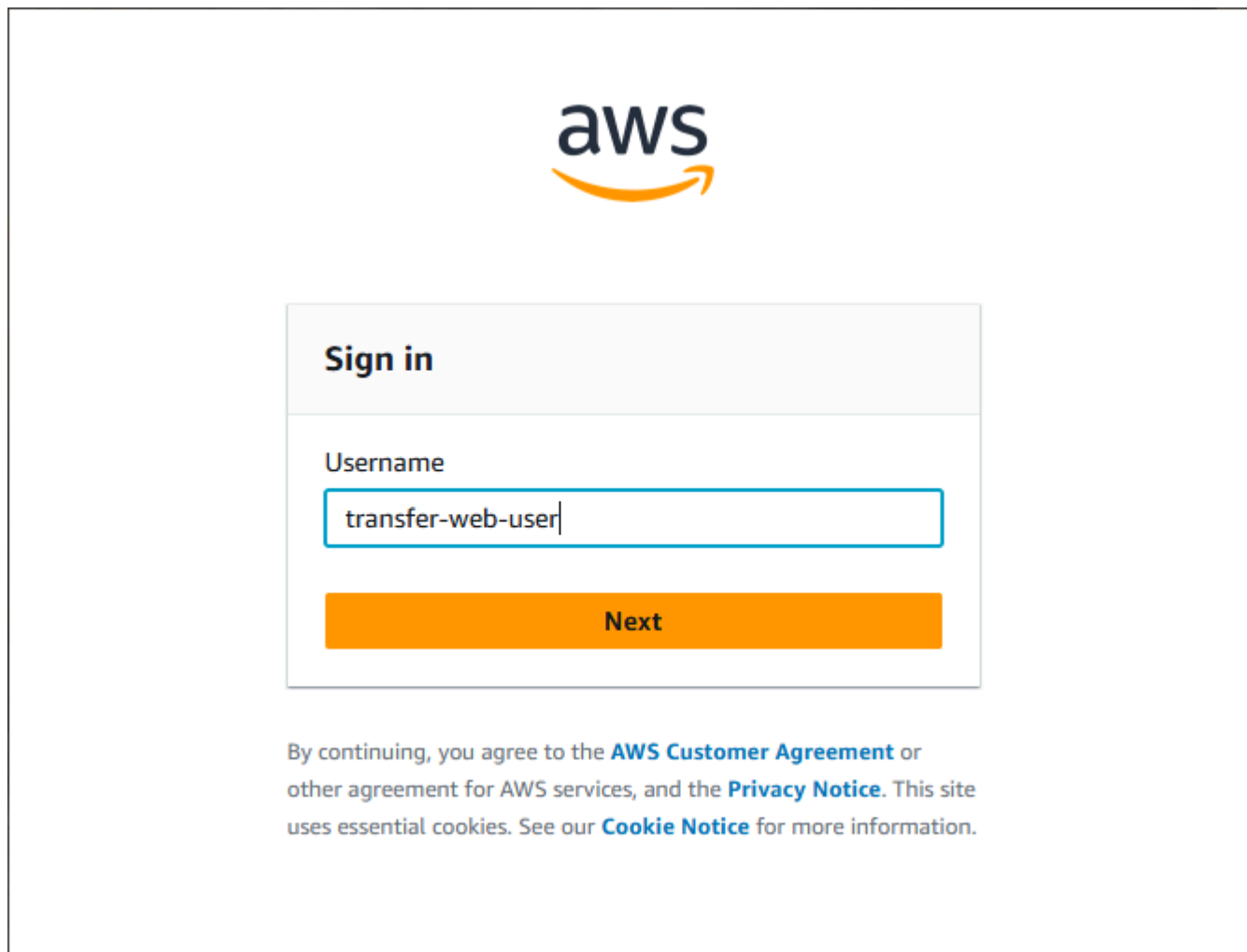
Expérience utilisateur pour les utilisateurs d'IAM Identity Center

Cette section décrit l'expérience utilisateur si votre organisation a utilisé IAM Identity Center pour configurer ses utilisateurs.

Pour accéder à une application Web Transfer Family

1. Vous devriez recevoir un e-mail de no-reply@login.awsapps.com intitulé « Invitation à participer » AWS IAM Identity Center. Acceptez l'invitation à activer votre compte utilisateur.
2. Dans le message, choisissez l'URL sous l'URL de votre portail AWS d'accès.

Cela vous amène à l'écran de AWS connexion.



aws

Sign in

Username

transfer-web-user

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

3. Entrez vos informations d'identification et choisissez Se connecter.

Cela vous amène au Portail d'accès AWS, qui affiche la liste de vos applications disponibles.

4. Choisissez l'application pour votre application Web Transfer Family.

Expérience utilisateur pour les utilisateurs de fournisseurs d'identité tiers

Si votre organisation n'a pas configuré ses utilisateurs, votre expérience d'intégration dépendra de l'application de fournisseur d'identité utilisée pour configurer ses utilisateurs finaux. AWS IAM Identity Center Une fois que vous vous êtes authentifié et connecté, l'interface de votre application Web est identique à celle décrite dans la section suivante.

 Note

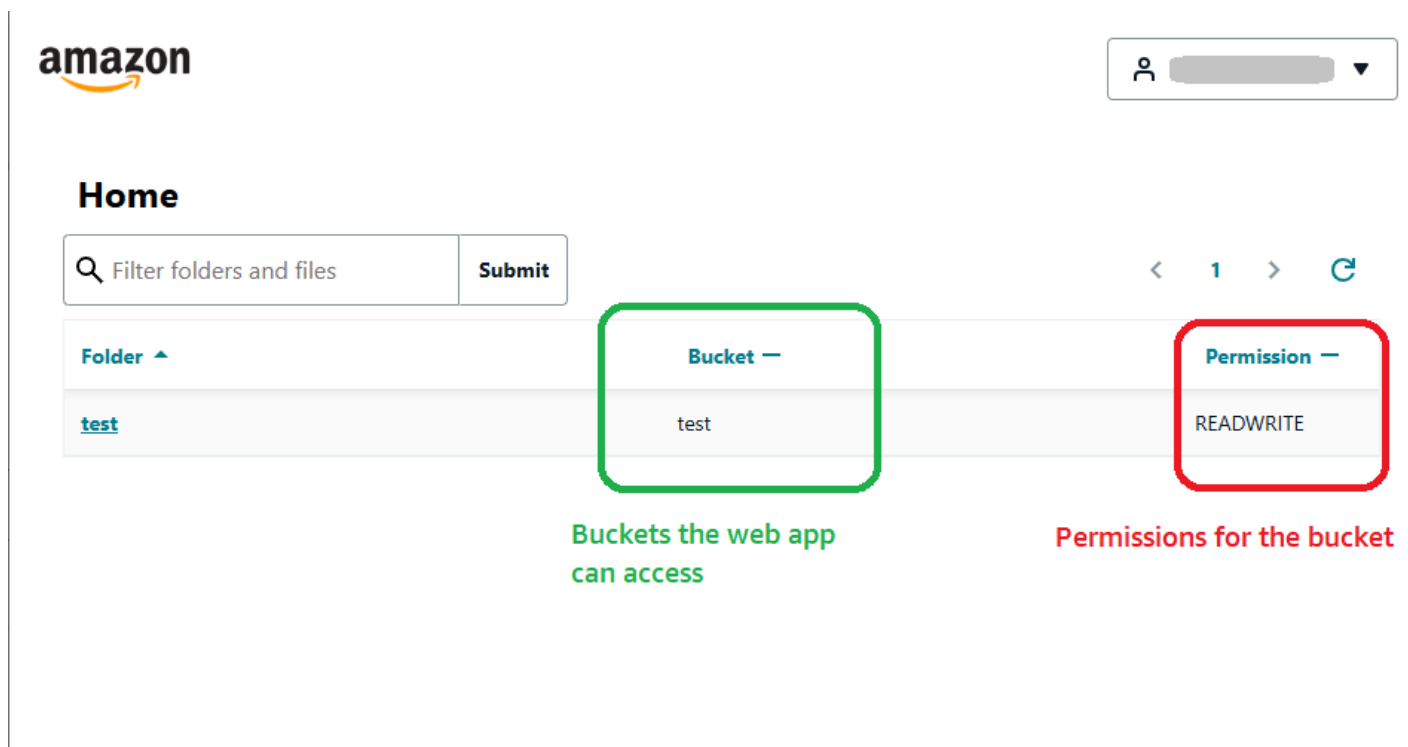
Si un utilisateur appartient à plusieurs groupes Active Directory dotés d'autorisations pour le même compartiment Amazon S3, le compartiment apparaît plusieurs fois dans l'interface de l'application Web. Cela se produit parce que l'application Web répertorie toutes les autorisations de haut niveau associées à l'UID ou au GID de l'utilisateur, y compris les autorisations dupliquées pour le même compartiment. Pour éviter les doublons dans les listes, les administrateurs peuvent regrouper plusieurs autorisations afin que chaque utilisateur ne dispose que d'une seule autorisation par site Amazon S3.

Interface utilisateur final de Transfer Family

Après vous être authentifié et connecté, vous pouvez interagir avec l'application Web.

Il existe quatre points de vue principaux.

- Page d'accueil : Votre page d'accueil répertorie les emplacements S3 auxquels vous pouvez accéder, ainsi que les autorisations pour chacun d'entre eux. Un emplacement S3 est un compartiment ou un préfixe S3, que vous pouvez définir à l'aide de S3 Access Grants. Il s'agit de la vue initiale pour les utilisateurs qui montre les ressources S3 de niveau racine auxquelles vos utilisateurs finaux ont accès et les autorisations pour chaque emplacement S3.



- Détails de l'emplacement : cette vue permet aux utilisateurs de parcourir les fichiers et les dossiers dans S3, et de charger ou de télécharger des fichiers.
- Action de localisation : une fois que vous avez choisi une action (telle que Télécharger), une autre vue de l'emplacement du fichier s'ouvre.
- Ellipses verticales : l'icône représentant des points de suspension verticaux ouvre le menu Actions.

Actions disponibles

La plupart des actions sont disponibles dans le menu Actions. Pour l'autre action principale, le téléchargement de fichiers, vous utilisez l'icône de téléchargement après avoir sélectionné un fichier (actuellement, vous ne pouvez télécharger qu'un seul fichier à la fois).

Transfer Web App

Scott

Home / test2 / Testing-01

Testing-01/

☐ Include subfolders

< 1 > ↺ ⋮

☐	Name ▲	Type —	Last Modified —	Size —	
☐	 scott-small.png	png	10/30/2024, 2:28:31 PM	375.4 kB	
☐	 Scott-02.jpg	jpg	10/30/2024, 2:28:30 PM	196.6 kB	
☐	 Scott-badge.jpg	jpg	10/30/2024, 2:28:31 PM	1.3 MB	

Download icon

À partir d'un dossier, utilisez le menu Actions pour effectuer l'une des tâches suivantes :

- Copiez un ou plusieurs fichiers vers un autre emplacement.
- Créez un dossier.
- Supprimez un ou plusieurs fichiers.
- Téléchargez un ou plusieurs fichiers.
- Téléchargez un dossier entier (y compris les sous-dossiers, le cas échéant).
- Sélectionnez un dossier et naviguez jusqu'à celui-ci. Vous pouvez ensuite effectuer n'importe laquelle des actions répertoriées précédemment.
- Trier par page.
- Filtrez par nom de fichier ou de dossier par dossier et sous-dossiers.

amazon

Home / test

test

🔍 Search current folder

Submit

☐ Include subfolders

< 1 > ↺ ⋮

Name ▲	Type —	Last Modified —
📁 My First Folder/	Folder	
📁 My Second Folder/	Folder	
📁 Testing-01/	Folder	
📁 Testing-02/	Folder	

📄 Copy files

📁 Create folder

🗑 Delete files

📁 Upload files

📁 Upload folder

AWS Transfer Family Connecteurs SFTP

Un connecteur AWS Transfer Family SFTP établit une connexion avec un serveur SFTP distant pour transférer des fichiers entre le stockage Amazon et un serveur distant, en utilisant le protocole SFTP. Vous pouvez envoyer des fichiers depuis Amazon S3 vers un serveur SFTP externe appartenant à un partenaire, récupérer des fichiers depuis le serveur SFTP d'un partenaire vers Amazon S3 ou répertorier, supprimer, renommer ou déplacer des fichiers sur le serveur distant. Les connecteurs SFTP prennent en charge deux types de sortie : les services gérés (à l'aide d'une infrastructure AWS gérée) et les VPC (routage via votre VPC à l'aide d'Amazon VPC Lattice). À l'aide des connecteurs SFTP, vous pouvez créer des flux de travail de transfert de fichiers automatisés et pilotés par des événements. AWS

Consultez la [AWS Transfer Family section Connecteurs SFTP](#) pour une brève présentation des connecteurs SFTP Transfer Family.

Rubriques

- [Création de connecteurs SFTP](#)
- [Connectivité VPC pour connecteurs SFTP](#)
- [Utilisation de connecteurs SFTP](#)
- [Surveillance des connecteurs SFTP](#)
- [Gestion des connecteurs SFTP](#)
- [Dimensionnement et quotas pour les connecteurs SFTP](#)
- [Architectures de référence utilisant des connecteurs SFTP](#)

Création de connecteurs SFTP

Cette rubrique explique comment créer des connecteurs SFTP. Chaque connecteur permet de se connecter à un serveur SFTP distant. Vous devez effectuer les tâches de haut niveau suivantes pour configurer un connecteur SFTP.

Note

Pour les VPC-based connecteurs qui acheminent le trafic via votre cloud privé virtuel, consultez [Création d'un connecteur SFTP avec sortie VPC-based](#).

1. Stockez les informations d'authentification du connecteur dans AWS Secrets Manager.
2. Créez le connecteur en spécifiant l'ARN secret, l'URL du serveur distant ou l'ARN de configuration des ressources, la politique de sécurité contenant les algorithmes qui seront pris en charge par le connecteur et d'autres paramètres de configuration.
3. Après avoir créé le connecteur, vous pouvez le tester pour vous assurer qu'il peut établir des connexions avec le serveur SFTP distant.

Choix du type de sortie du connecteur SFTP

Lorsque vous créez un connecteur SFTP, vous choisissez le type de sortie entre « Service géré » et « VPC Lattice ».

- **Service géré (par défaut) :** le connecteur utilise des passerelles NAT et des adresses IP détenues par AWS Transfer Family pour acheminer les connexions via l'Internet public. Le service fournit 3 adresses IP statiques pour vos connecteurs qui doivent être répertoriées sur les serveurs distants pour établir des connexions.
- **Réseau VPC :** le connecteur achemine le trafic via votre environnement VPC à l'aide d'Amazon VPC Lattice. Utilisez la connectivité VPC pour les connecteurs SFTP dans les scénarios suivants :
 - **Serveurs SFTP privés :** connectez-vous à des serveurs SFTP uniquement accessibles depuis votre VPC
 - **On-premises connectivité :** Connectez-vous à des serveurs SFTP locaux via AWS Direct Connect ou des connexions AWS Virtual Private Network
 - **Adresses IP personnalisées :** présentez vos propres passerelles NAT et adresses IP élastiques au serveur distant
 - **Contrôles de sécurité centralisés :** acheminez les transferts de fichiers via les ingress/egress contrôles centraux de votre entreprise

La matrice suivante vous aide à choisir le type de connecteur adapté à vos cas d'utilisation.

Matrice de type sortie du connecteur SFTP

Capacité	Type de sortie = Service géré	Type de sortie = réseau VPC
Connectivité aux serveurs SFTP hébergés publiquement (accessibles par Internet)	Pris en charge	Supporté ¹

Capacité	Type de sortie = Service géré	Type de sortie = réseau VPC
Connectivité aux serveurs SFTP hébergés en privé (sur site)	Non pris en charge	Soutenu ⁽²⁾
Connectivité aux serveurs SFTP hébergés en privé (In-VPC)	Non pris en charge	Pris en charge
Adresses IP statiques présentées au serveur SFTP distant	Pris en charge via les adresses IP statiques fournies par le service	Pris en charge via les adresses IP statiques appartenant aux clients
Bande passante disponible	50 Mbits/s par compte	Bande passante plus élevée, telle que disponible auprès de Resource Gateway et de NAT Gateway appartenant au client
Acheminement du trafic vers Internet via des passerelles NAT et des pare-feux réseau appartenant au client	Non pris en charge. Les passerelles NAT sont détenues et gérées par le service Transfer Family.	Pris en charge

¹ Avec Type de sortie = VPC Lattice, la connectivité aux serveurs hébergés publiquement est prise en charge à l'aide de l'infrastructure de sortie (passerelles NAT) configurée dans vos VPC de sortie.

² Avec Type de sortie = VPC Lattice, la connectivité aux serveurs hébergés en privé est prise en charge via les réseaux existants de votre VPC, tels que le VPN. AWS Direct Connect

Choix du mode d'adressage IP

Lorsque vous créez un connecteur SFTP avec sortie gérée par service, vous pouvez choisir entre deux modes d'adressage IP :

- IPv4 uniquement (par défaut) : le connecteur utilise des adresses IPv4 exclusivement pour se connecter au serveur SFTP distant. Il s'agit du mode par défaut lors de la création de connecteurs via la console, la AWS CLI ou l'API.

- **Dual-stack:** le connecteur prend en charge les adresses IPv6 et IPv4. En mode double pile, le connecteur préfère IPv6 lorsque la résolution DNS renvoie des résultats IPv6, et utilise IPv4 lorsque seuls les résultats DNS IPv4 sont renvoyés.

Note

Le mode d'adressage IP s'applique uniquement aux connecteurs dotés d'un type de sortie géré par le service. Les connecteurs qui utilisent la sortie VPC Lattice ne prennent pas en charge ce paramètre.

Rubriques

- [Stockez les informations d'authentification pour les connecteurs SFTP dans Secrets Manager](#)
- [Création d'un connecteur SFTP avec sortie gérée par service](#)
- [Création d'un connecteur SFTP avec sortie VPC-based](#)
- [Tester un connecteur SFTP](#)

Stockez les informations d'authentification pour les connecteurs SFTP dans Secrets Manager

Vous pouvez utiliser Secrets Manager pour stocker les informations d'identification utilisateur de vos connecteurs SFTP. 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 en savoir plus, consultez [Quotas pour les connecteurs SFTP](#).

Note

Lorsque vous stockez des secrets dans Secrets Manager, des frais Compte AWS vous sont facturés. Pour plus d'informations sur la tarification, consultez la section [AWS Secrets Manager Tarification](#).

Pour stocker les informations d'identification de l'utilisateur dans Secrets Manager pour un connecteur SFTP

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 panneau 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. Fournissez les key/value informations relatives à votre secret : vous devez fournir le nom d'utilisateur, ainsi qu'une clé privée ou un mot de passe.
 - a. Dans la section des Key/value paires, choisissez l'onglet Key/value.
 - Clé — Entrée **Username**.
 - valeur — Entrez le nom de l'utilisateur autorisé à se connecter au serveur du partenaire.
 - b. Si vous souhaitez fournir une paire de clés, choisissez Ajouter une ligne, puis dans la section Key/value paires, sélectionnez l'onglet Key/value.
 - Clé — Entrée **PrivateKey**.
 - valeur : collez votre clé privée.

Conseil : Les données de clé privée que vous entrez doivent correspondre à la clé publique enregistrée pour cet utilisateur sur le serveur SFTP distant.

 Note

Il n'est pas possible d'utiliser une clé privée protégée par un mot de passe pour l'authentification avec un connecteur SFTP. AWS Transfer Family

Pour plus de détails sur la génération d'une paire de public/private clés, consultez [Création de clés SSH sous macOS, Linux ou Unix](#).

- c. Si vous souhaitez fournir un mot de passe, choisissez Ajouter une ligne, puis dans la section des Key/value paires, sélectionnez l'onglet Key/value.
- Clé — Entrée **Password**.

- valeur — Entrez le mot de passe de l'utilisateur.
6. Choisissez Suivant.
 7. 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**.
 8. Choisissez Next, puis acceptez les valeurs par défaut sur la page Configurer la rotation. Ensuite, sélectionnez Suivant.
 9. Sur la page Révision, choisissez Store pour créer et stocker le secret.

Création d'un connecteur SFTP avec sortie gérée par service

Cette procédure explique comment créer des connecteurs SFTP à l'aide de la AWS Transfer Family console ou AWS CLI.

Console

Pour créer un connecteur SFTP

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 SFTP Connectors, puis Create SFTP connector.
3. Dans la section Configuration du connecteur, pour le type de sortie, choisissez Service géré. Cette option utilise une infrastructure de sortie AWS Transfer Family gérée. Le service Transfer Family fournit et gère des adresses IP statiques pour chaque connecteur SFTP.
4. Dans la section Configuration du connecteur, fournissez les informations suivantes :

Connector configuration

Egress type [Info](#)
Choose your SFTP connector's egress type: either directly over public internet, or via your VPC environment

☒ **Service managed**
Connect to public endpoints over the internet. The connector will present service-provided static IP addresses to remote server.

☐ **VPC Lattice**
Connect to public or private endpoints through your VPC. The connector will present elastic IP address from your VPC's CIDR range to remote server.

URL
Enter the URL of remote server to which you need to connect using the SFTP connector

sftp://sftp.example.com

URL of the remote (target) SFTP server

Access role [Info](#)
IAM Role for Amazon S3 access and AWS Secrets Manager access

Choose an IAM role

Logging role - optional [Info](#)
IAM role for the connector to push events to your CloudWatch logs

Choose a logging role

- Pour l'URL, entrez l'URL d'un serveur SFTP distant. Cette URL doit être formatée comme `suitsftp://partner-SFTP-server-url`, par exemples `ftp://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 Gestion des identités et des accès AWS (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 l'ARN du secret. L'ARN contient le nom secret, mais y ajoute six caractères alphanumériques aléatoires. L'ARN d'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](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
      "Sid": "GetConnectorSecretValue",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ]
    }
  ]
}
```



```

    ],
    "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333: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 rôle IAM pour plusieurs utilisateurs et plusieurs 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 informations d'identification SFTP 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](#).

5. Terminez la configuration du connecteur :

- (Facultatif) Pour le rôle de journalisation, choisissez le rôle IAM que le connecteur doit utiliser pour transférer des événements vers vos CloudWatch journaux. L'exemple de politique suivant répertorie les autorisations nécessaires pour consigner des événements pour les connecteurs SFTP.

```

{
  "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/*"
  }
]
}

```

6. Dans la section Configuration SFTP, fournissez les informations suivantes :

SFTP configuration [Info](#)

Connector credentials [Info](#)
 Select a secret from AWS Secrets Manager containing the username and SSH private key, or username and password, to be used to connect to the remote server

aws/transfer/sftp-connector1  [Store a new secret](#) 

Trusted host keys - optional [Info](#)
 Enter the public portion of the host key(s) that is used to identify the remote server you need to connect to. You can enter the trusted host key(s) now, or add them after creating the connector by using the host key information returned by the TestConnection action.

 Connections to the remote server are established only if it's SSH fingerprint matches one of the provided trusted host key(s).

ssh-rsa AAAAE... [Remove](#)

[Add trusted host key](#)

Maximum concurrent connections [Info](#)
 Select the maximum number of concurrent connections that your connector can create to the remote server

5 ▼

- Pour les informations d'identification du connecteur, dans la liste déroulante, choisissez le nom d'un secret AWS Secrets Manager contenant la clé privée ou le mot de passe de l'utilisateur SFTP. Vous devez créer un secret et le stocker d'une manière spécifique. Pour en savoir plus, consultez [Stockez les informations d'authentification pour les connecteurs SFTP dans Secrets Manager](#).
- (Facultatif) Vous avez la possibilité de créer votre connecteur tout en laissant le `TrustedHostKeys` paramètre vide. Toutefois, votre connecteur ne sera pas en mesure de transférer des fichiers avec le serveur distant tant que vous n'aurez pas fourni ce paramètre dans la configuration de votre connecteur. Vous pouvez saisir la ou les clés d'hôte fiables au moment de créer votre connecteur, ou mettre à jour votre connecteur ultérieurement en utilisant les informations de clé d'hôte renvoyées par l'action de la `TestConnection` console ou la commande d'API. En d'autres termes, pour la zone de texte Clés d'hôte fiables, vous pouvez effectuer l'une des opérations suivantes :

- Fournissez la ou les clés d'hôte fiables au moment de créer votre connecteur. 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 serveur SFTP 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, consultez [SFTPConnectorConfig](#).
- Laissez la zone de texte Trusted Host Key (s) vide lors de la création de votre connecteur et mettez à jour votre connecteur ultérieurement avec ces informations. Si vous ne disposez pas des informations relatives à la clé de l'hôte au moment de créer votre connecteur, vous pouvez laisser ce paramètre vide pour le moment et poursuivre la création de votre connecteur. Une fois le connecteur créé, utilisez l'identifiant du nouveau connecteur pour exécuter la `TestConnection` commande, soit dans la page détaillée du connecteur, AWS CLI soit à partir de celle-ci. En cas de succès, `TestConnection` renverra les informations de clé d'hôte nécessaires. Vous pouvez ensuite modifier votre connecteur à l'aide de la console (ou en exécutant la `UpdateConnector` AWS CLI commande) et ajouter les informations de clé d'hôte renvoyées lors de l'exécution `TestConnection`.

 Important

Si vous récupérez la clé d'hôte du serveur distant en exécutant `TestConnection`, assurez-vous d'effectuer une validation hors bande sur la clé renvoyée.

Vous devez accepter la nouvelle clé comme étant fiable ou vérifier l'empreinte digitale présentée à l'aide d'une empreinte connue que vous avez reçue du propriétaire du serveur SFTP distant auquel vous vous connectez.

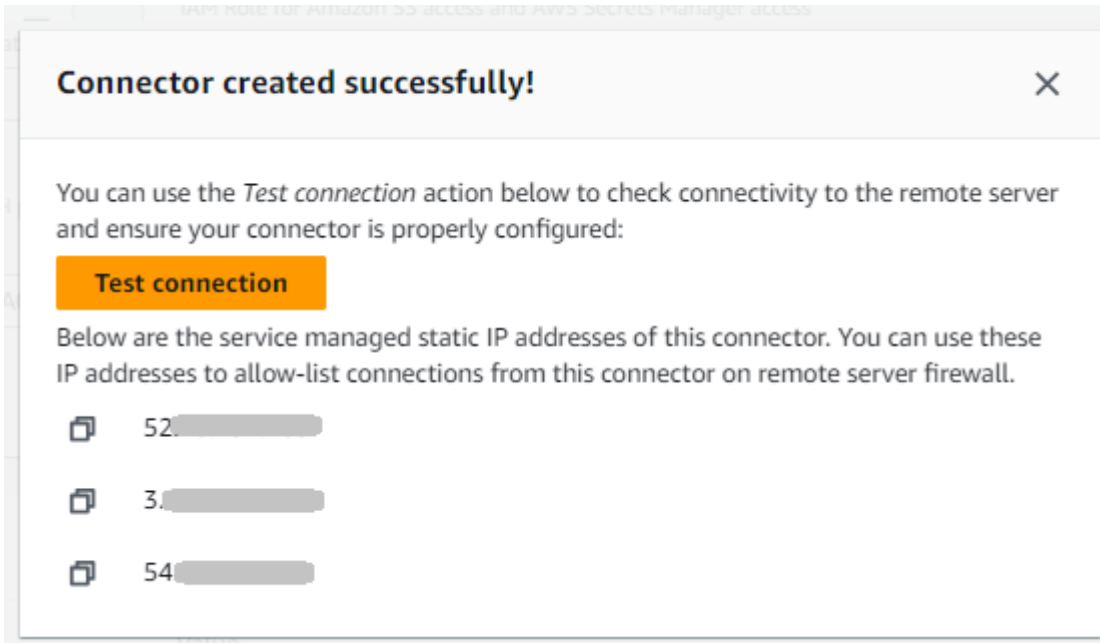
- (Facultatif) Pour Maximum de connexions simultanées, dans la liste déroulante, choisissez le nombre de connexions simultanées que votre connecteur crée avec le serveur distant. La sélection par défaut sur la console est 5.

Ce paramètre indique le nombre de connexions actives que votre connecteur peut établir avec le serveur distant en même temps. La création de connexions simultanées peut améliorer les performances du connecteur en permettant des opérations parallèles.

7. Dans la section Options de l'algorithme cryptographique, choisissez une politique de sécurité dans la liste déroulante du champ Stratégie de sécurité. La politique de sécurité vous permet de sélectionner les algorithmes cryptographiques pris en charge par votre

connecteur. Pour plus de détails sur les politiques de sécurité et les algorithmes disponibles, consultez [Politiques de sécurité pour AWS Transfer Family Connecteurs SFTP](#).

8. (Facultatif) Dans la section Balises, pour Clé et Valeur, entrez une ou plusieurs balises sous forme de paires clé-valeur.
9. Après avoir confirmé tous vos paramètres, choisissez **Create SFTP connector** (Créer un connecteur SFTP) pour créer le connecteur SFTP. 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 connecteur SFTP ajouté à la liste. Pour consulter les détails de vos connecteurs, consultez [Afficher les détails du connecteur SFTP](#).

CLI

Vous utilisez la [create-connector](#) commande pour créer un connecteur. Pour utiliser cette commande afin de créer un connecteur SFTP, vous devez fournir les informations suivantes.

- URL d'un serveur SFTP distant. Cette URL doit être formatée comme `sftp://partner-SFTP-server-url`, par exemple `sftp://AnyCompany.com`.
- Le rôle d'accès. Choisissez le nom de ressource Amazon (ARN) du rôle Gestion des identités et des accès AWS (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 l'`secretsmanager:GetSecretValue` accès au secret.

 Note

Dans la politique, vous devez spécifier l'ARN du secret. L'ARN contient le nom secret, mais y ajoute six caractères alphanumériques aléatoires. L'ARN d'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](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowListingOfUserFolder",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    },
    {
      "Sid": "HomeDirObjectAccess",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
  },
  {
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-west-2:111122223333: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 rôle IAM pour plusieurs utilisateurs et plusieurs 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 informations d'identification SFTP 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 rôle IAM que le connecteur doit utiliser pour transférer des événements vers vos CloudWatch journaux. L'exemple de politique suivant répertorie les autorisations nécessaires pour consigner des événements pour les connecteurs SFTP.

```

{
  "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/*"
    }
}

```

- Fournissez les informations de configuration SFTP suivantes.
 - L'ARN d'un secret AWS Secrets Manager contenant la clé privée ou le mot de passe de l'utilisateur SFTP.
 - 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 informations SFTP 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": [
        "ssh-rsa AAAAbbbb...EEEE="
    ]
}

```

- Spécifiez une politique de sécurité pour votre connecteur, en saisissant le nom de la politique de sécurité.

Note

Il `SecretId` peut s'agir de l'ARN complet 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 \
--security-policy-name security-policy-name \
--maximum-concurrent-connections integer-from-1-to-5
```

Lorsque vous décrivez un connecteur de type sortie VPC, la réponse inclut les nouveaux champs :

```
{
  "Connector": {
    "AccessRole": "arn:aws:iam::123456789012:role/connector-role",
    "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/
c-1234567890abcdef0",
    "ConnectorId": "c-1234567890abcdef0",
    "Status": "ACTIVE",
    "EgressConfig": {
      "VpcLattice": {
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-12345678",
        "PortNumber": 22
      }
    },
    "EgressType": "VPC",
    "ServiceManagedEgressIpAddresses": null,
    "SftpConfig": {
      "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
      "UserSecretId": "aws/transfer/connector-secret"
    },
    "Url": "sftp://my.sftp.server.com:22"
  }
}
```

Notez que cela ServiceManagedEgressIpAddresses est nul pour les connecteurs de type sortie VPC, car le trafic passe par votre VPC plutôt que par l'infrastructure gérée. AWS

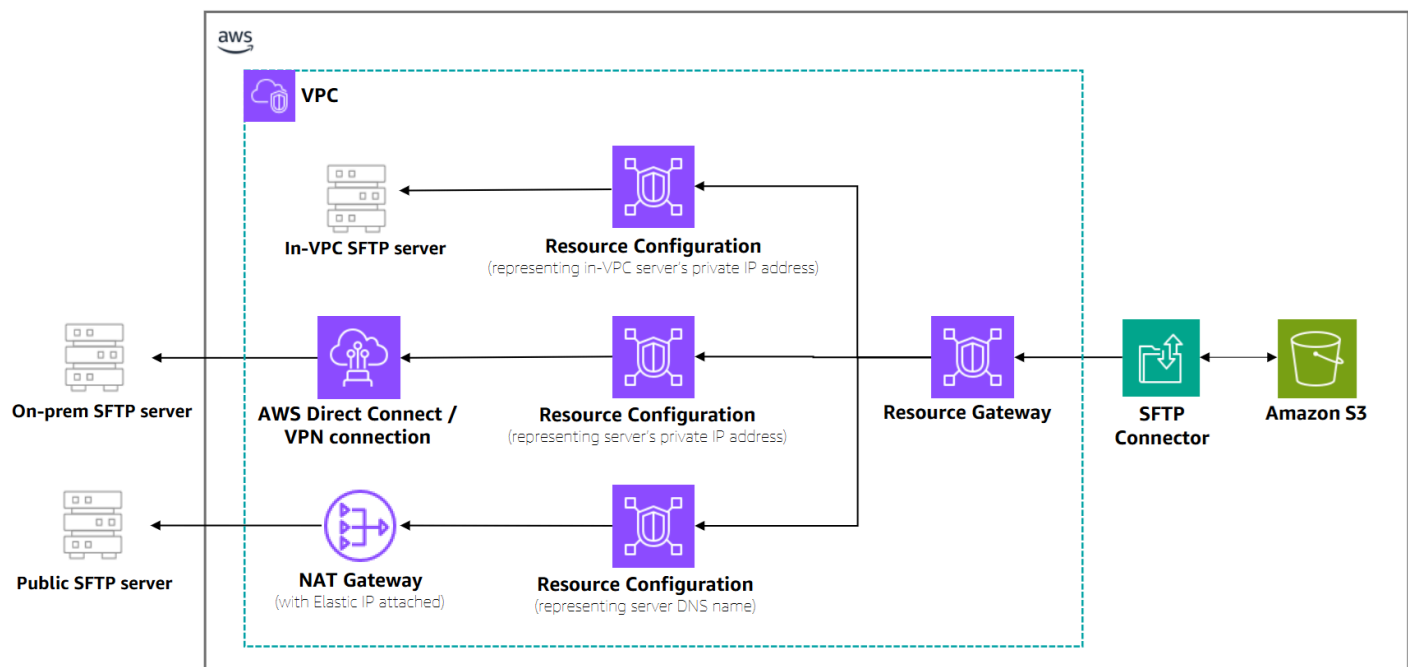
Création d'un connecteur SFTP avec sortie VPC-based

Cette rubrique fournit des instructions détaillées pour créer des connecteurs SFTP avec une connectivité VPC. LATTICE-enabled Les connecteurs VPC_ utilisent Amazon VPC Lattice pour acheminer le trafic via votre cloud privé virtuel, en permettant des connexions sécurisées vers des points de terminaison privés ou en utilisant vos propres passerelles NAT pour l'accès à Internet.

Quand utiliser la connectivité VPC

Utilisez la connectivité VPC pour les connecteurs SFTP dans les scénarios suivants :

- **Serveurs SFTP privés** : connectez-vous à des serveurs SFTP uniquement accessibles depuis votre VPC.
- **On-premises connectivité** : connectez-vous aux serveurs SFTP locaux via Direct AWS Connect ou des connexions AWS Site-to-Site VPN.
- **Adresses IP personnalisées** : utilisez vos propres passerelles NAT et adresses IP élastiques, y compris les scénarios BYOIP.
- **Contrôles de sécurité centralisés** : acheminez les transferts de fichiers via les ingress/egress contrôles centraux de votre entreprise.



Prérequis pour les connecteurs VPC_ SFTP LATTICE-enabled

Avant de créer un connecteur VPC_ LATTICE-enabled SFTP, vous devez remplir les conditions préalables suivantes :

Comment fonctionne VPC-based la connectivité

VPC Lattice vous permet de partager en toute sécurité des ressources VPC avec d'autres services. AWS AWS Transfer Family utilise un réseau de service pour simplifier le processus de partage des ressources. Les composants clés sont les suivants :

- Passerelle de ressources : sert de point d'accès à votre VPC. Vous le créez dans votre VPC avec un minimum de deux zones de disponibilité.
- Configuration des ressources : contient l'adresse IP privée ou le nom DNS public du serveur SFTP auquel vous souhaitez vous connecter.

Lorsque vous créez un LATTICE-enabled connecteur VPC_, il AWS Transfer Family utilise la session d'accès direct (FAS) pour obtenir temporairement vos informations d'identification et associer votre configuration de ressources à notre réseau de services.

Étapes de configuration requises

1. Infrastructure VPC : assurez-vous de disposer d'un VPC correctement configuré avec les sous-réseaux, les tables de routage et les groupes de sécurité nécessaires pour répondre aux exigences de connectivité de votre serveur SFTP.
2. Passerelle de ressources : créez une passerelle de ressources dans votre VPC à l'aide de la commande VPC Lattice. `create-resource-gateway` La passerelle de ressources doit être associée à des sous-réseaux dans au moins deux zones de disponibilité. Pour plus d'informations, consultez [Resource Gateways](#) dans le guide de l'utilisateur Amazon VPC Lattice.
3. Configuration des ressources : créez une configuration des ressources qui représente le serveur SFTP cible à l'aide de la commande VPC `create-resource-configuration` Lattice. Vous pouvez spécifier soit :
 - Une adresse IP privée pour les points de terminaison privés
 - Un nom DNS public pour les points de terminaison publics (les adresses IP ne sont pas prises en charge pour les points de terminaison publics)

4. Informations d'authentification : stockez les informations d'identification de l'utilisateur SFTP AWS Secrets Manager comme décrit dans [Stockez les informations d'authentification pour les connecteurs SFTP dans Secrets Manager](#).

 Important

La passerelle de ressources et la configuration des ressources doivent être créées dans le même AWS compte. Lorsque vous créez une configuration de ressources, vous devez d'abord disposer d'une passerelle de ressources.

Pour plus d'informations sur les configurations des ressources VPC, consultez la section Configurations [des ressources dans le guide](#) de l'utilisateur Amazon VPC Lattice.

 Note

La connectivité VPC pour les connecteurs SFTP est disponible là où les ressources Régions AWS Amazon VPC Lattice sont disponibles. Pour plus d'informations, consultez les FAQ sur les [treillis VPC](#). La prise en charge des zones de disponibilité varie selon les régions, et les passerelles de ressources nécessitent un minimum de deux zones de disponibilité.

Création d'un connecteur VPC_ SFTP LATTICE-enabled

Une fois les conditions requises remplies, vous pouvez créer un connecteur SFTP avec connectivité VPC à l'aide de la console de AWS gestion AWS CLI ou des SDK. AWS

Console

Pour créer un connecteur VPC_ SFTP LATTICE-enabled

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 SFTP Connectors, puis Create SFTP connector.
3. Dans la section Configuration du connecteur, pour Type de sortie, choisissez VPC Lattice.

Cette option achemine le trafic via votre VPC à l'aide d'Amazon VPC Lattice pour l'accès aux ressources entre VPC. Vous pouvez utiliser cette option pour vous connecter à des points de terminaison de serveurs hébergés en privé, acheminer le trafic via les contrôles de sécurité de votre VPC ou utiliser vos propres passerelles NAT et adresses IP élastiques. L'adresse du serveur SFTP distant est représentée sous forme de configuration de ressources dans votre VPC. Pour plus d'informations sur les configurations des ressources, consultez la section [Configurations des ressources pour les ressources VPC](#) dans le guide de l'utilisateur Amazon VPC Lattice.

4. Terminez la configuration du connecteur :

- Pour le rôle Access, choisissez le nom de ressource Amazon (ARN) du rôle Gestion des identités et des accès AWS (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 l'ARN du secret. L'ARN contient le nom secret, mais y ajoute six caractères alphanumériques aléatoires. L'ARN d'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](#).

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

```

        "s3:ListBucket",
        "s3:GetBucketLocation"
    ],
    "Effect": "Allow",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
},
{
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
},
{
    "Sid": "GetConnectorSecretValue",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-  
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
}
]
}

```

Note

Pour le rôle d'accès, l'exemple accorde l'accès à un secret unique. Vous pouvez toutefois utiliser un caractère générique, ce qui peut vous faire économiser du travail si vous souhaitez réutiliser le même rôle IAM pour plusieurs utilisateurs et plusieurs 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 informations d'identification SFTP 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](#).

- Pour l'ARN de configuration des ressources, entrez l'ARN de la configuration des ressources en treillis VPC qui pointe vers votre serveur SFTP :

```
arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678
```

- (Facultatif) Pour le rôle de journalisation, choisissez le rôle IAM que le connecteur doit utiliser pour transférer des événements vers vos CloudWatch journaux.

```
{
  "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/*"
    }
  ]
}
```

5. Dans la section Configuration SFTP, fournissez les informations suivantes :

- Pour les informations d'identification du connecteur, choisissez le nom d'un secret AWS Secrets Manager contenant la clé privée ou le mot de passe de l'utilisateur SFTP.

- Pour les clés d'hôte fiables, collez la partie publique de la clé d'hôte utilisée pour identifier le serveur externe, ou laissez le champ vide pour le configurer ultérieurement à l'aide de la `TestConnection` commande.

Comme cette clé d'hôte est destinée à un connecteur `VPC_LATTICE`, supprimez le nom d'hôte dans la clé

- (Facultatif) Pour Nombre maximal de connexions simultanées, choisissez le nombre de connexions simultanées que votre connecteur crée avec le serveur distant (la valeur par défaut est 5).
6. Dans la section Options de l'algorithme cryptographique, choisissez une politique de sécurité dans la liste déroulante.
 7. (Facultatif) Dans la section Balises, ajoutez des balises sous forme de paires clé-valeur.
 8. Choisissez `Create SFTP connector` pour créer le connecteur `VPC_LATTICE-enabled SFTP`.

Le connecteur sera créé avec l'état `PENDING` pendant le provisionnement de l'association de ressources, ce qui prend généralement plusieurs minutes. Une fois que l'état passe à `ACTIVE`, le connecteur est prêt à être utilisé.

CLI

Utilisez la commande suivante pour créer un connecteur `VPC_LATTICE-enabled SFTP` :

```
aws transfer create-connector \
  --url "sftp://my.sftp.server.com:22" \
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
  --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \
  --security-policy-name TransferSecurityPolicy-2024-01
```

Le paramètre clé de la connectivité VPC est `--egress-config` le suivant : il spécifie l'ARN de configuration des ressources qui définit la cible de votre serveur SFTP.

Surveillance de l'état du connecteur VPC

Les `LATTICE-enabled` connecteurs `VPC_` ont un processus de configuration asynchrone. Après la création, surveillez l'état du connecteur :

- **EN ATTENTE** : Le connecteur est en cours de provisionnement. Le provisionnement du réseau de services est en cours, ce qui prend généralement plusieurs minutes.
- **ACTIF** : Le connecteur est prêt à être utilisé et permet de transférer des fichiers.
- **ERREUR** : Le connecteur n'a pas pu être configuré. Consultez les détails de l'erreur pour obtenir des informations de dépannage.

Vérifiez l'état du connecteur à l'aide de la `describe-connector` commande :

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Pendant l'état **PENDING**, l'`test-connectionAPI` renvoie le message « Connecteur non disponible » jusqu'à ce que le provisionnement soit terminé.

Limites et considérations

- **Points de terminaison publics** : lorsque vous vous connectez à des points de terminaison publics via VPC, vous devez fournir un nom DNS dans la configuration des ressources. Les adresses IP publiques ne sont pas prises en charge.
- **Disponibilité régionale** : la connectivité VPC est disponible dans certains pays. Régions AWS Cross-region le partage de ressources n'est pas pris en charge.
- **Exigences relatives aux zones de disponibilité** : les passerelles de ressources doivent être associées à des sous-réseaux dans au moins deux zones de disponibilité. Les zones de disponibilité ne sont pas toutes compatibles avec le VPC Lattice dans toutes les régions.
- **Limites de connexion** : 350 connexions maximum par ressource avec un délai d'inactivité de 350 secondes pour les connexions TCP.

Considérations de coût

Il n'y a pas de frais supplémentaires autres AWS Transfer Family que les frais de service réguliers. Toutefois, les clients peuvent être soumis à des frais supplémentaires de la part d'Amazon VPC Lattice associés au partage de leurs ressources Amazon Virtual Private Cloud, ainsi qu'à des frais de passerelle NAT s'ils utilisent leurs propres passerelles NAT pour accéder à Internet.

Pour obtenir AWS Transfer Family des informations complètes sur les prix, consultez la [page AWS Transfer Family des tarifs](#).

Exemples de connectivité VPC pour les connecteurs SFTP

Cette section fournit des exemples de création de connecteurs SFTP avec connectivité VPC pour différents scénarios. Avant d'utiliser ces exemples, assurez-vous d'avoir terminé la configuration de l'infrastructure VPC comme décrit dans la documentation de connectivité VPC.

Exemple : connexion à un point de terminaison privé

Cet exemple montre comment créer un connecteur SFTP qui se connecte à un serveur SFTP privé accessible uniquement depuis votre VPC.

Conditions préalables

1. Créez une passerelle de ressources dans votre VPC :

```
aws vpc-lattice create-resource-gateway \  
  --name my-private-server-gateway \  
  --vpc-identifiant vpc-1234567890abcdef0 \  
  --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. Créez une configuration de ressources pour votre serveur SFTP privé :

```
aws vpc-lattice create-resource-configuration \  
  --name my-private-server-config \  
  --resource-gateway-identifiant rgw-1234567890abcdef0 \  
  --resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \  
  --port-ranges 22
```

Créez le connecteur VPC_ LATTICE-enabled

1. Créez le connecteur SFTP avec connectivité VPC :

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \  
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-  
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. Surveillez l'état du connecteur jusqu'à ce qu'il devienne ACTIVE :

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Le serveur SFTP distant verra les connexions provenant de l'adresse IP de Resource Gateway dans la plage d'adresses CIDR de votre VPC.

Exemple : point de terminaison public via VPC

Cet exemple montre comment acheminer les connexions vers un serveur SFTP public via votre VPC afin de tirer parti des contrôles de sécurité centralisés et d'utiliser vos propres adresses IP de passerelle NAT.

Conditions préalables

1. Créez une passerelle de ressources dans votre VPC (identique à l'exemple d'un point de terminaison privé).
2. Créez une configuration de ressource pour le serveur SFTP public à l'aide de son nom DNS :

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="sftp.example.com"} \  
  --port-ranges 22
```

Note

Pour les points de terminaison publics, vous devez utiliser un nom DNS et non une adresse IP.

Création du connecteur

- Créez le connecteur SFTP :

```
aws transfer create-connector \  
  --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \  
  --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-  
rsa AAAAB3NzaC..." \
```

```
--egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

Le trafic circulera du connecteur vers votre passerelle de ressources, puis via votre passerelle NAT pour atteindre le serveur SFTP public. Le serveur distant verra l'adresse IP élastique de votre passerelle NAT comme source.

Exemple : point de terminaison Cross-account privé

Cet exemple montre comment se connecter à un serveur SFTP privé sur un autre AWS compte en utilisant le partage de ressources.

 Note

Si le partage de ressources inter-VPC est déjà activé via d'autres mécanismes, par exemple AWS Transit Gateway, vous n'avez pas besoin de configurer le partage de ressources décrit ici. Les mécanismes de routage existants, tels que les tables de routage Transit Gateway, sont automatiquement utilisés par les connecteurs SFTP. Il vous suffit de créer une configuration de ressources dans le compte sur lequel vous créez le connecteur SFTP.

Compte A (fournisseur de ressources) - Partagez la configuration des ressources

1. Créez une passerelle de ressources et une configuration de ressources dans le compte A (comme dans les exemples précédents).
2. Partagez la configuration des ressources avec le compte B à l'aide de AWS Resource Access Manager :

```
aws ram create-resource-share \  
  --name cross-account-sftp-share \  
  --resource-arns arn:aws:vpc-lattice:us-east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \  
  --principals 222222222222
```

Compte B (consommateur de ressources) - Acceptez et utilisez le partage

1. Acceptez l'invitation au partage de ressources :

```
aws ram accept-resource-share-invitation \
  --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/invitation-id
```

2. Créez le connecteur SFTP dans le compte B :

```
aws transfer create-connector \
  --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \
  --sftp-config UserSecretId=cross-account-server-
credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
  --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

Le connecteur du compte B peut désormais accéder au serveur SFTP privé du compte A via la configuration des ressources partagées.

Scénarios courants de résolution des problèmes

Voici des solutions aux problèmes courants rencontrés lors de la création de connecteurs VPC_LATTICE-enabled :

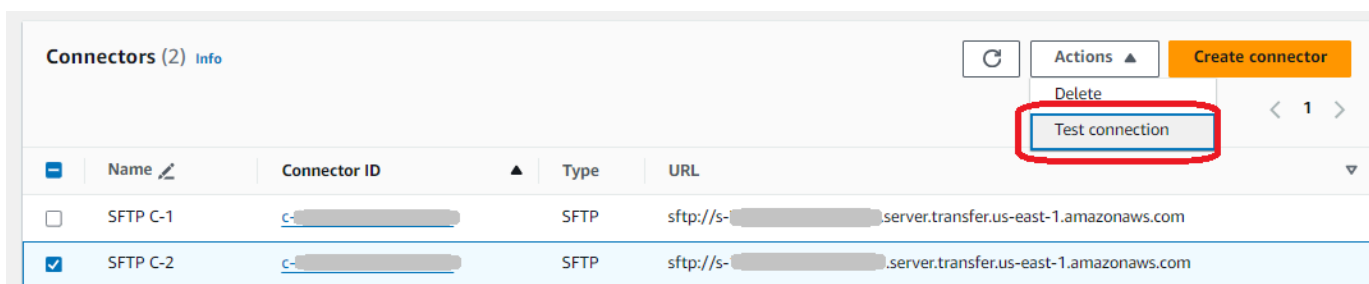
- **Connecteur bloqué avec le statut EN ATTENTE** : vérifiez que votre passerelle de ressources est ACTIVE et possède des sous-réseaux dans les zones de disponibilité prises en charge. Si le connecteur est toujours bloqué avec le statut EN ATTENTE, appelez en UpdateConnector utilisant les mêmes paramètres de configuration que ceux que vous avez utilisés initialement. Cela déclenche un nouvel événement de statut susceptible de résoudre le problème.
- **Délais de connexion** : vérifiez que les règles du groupe de sécurité autorisent le trafic sur le port 22 et que le routage de votre VPC est correct.
- **Problèmes de résolution DNS** : pour les points de terminaison publics, assurez-vous que votre VPC dispose d'une connectivité Internet via une passerelle NAT ou une passerelle Internet.
- **Cross-account accès refusé** : vérifiez que le partage de ressources est accepté et que l'ARN de configuration des ressources est correct. Si la politique d'autorisation appropriée est attachée à la configuration des ressources lorsque le compte d'origine crée le partage de ressources, les autorisations suivantes sont requises : vpc-lattice:AssociateViaAWSService, vpc-lattice:AssociateViaAWSService-EventsAndStates, vpc-lattice:CreateServiceNetworkResourceAssociation, vpc-lattice:GetResourceConfiguration.

Tester un connecteur SFTP

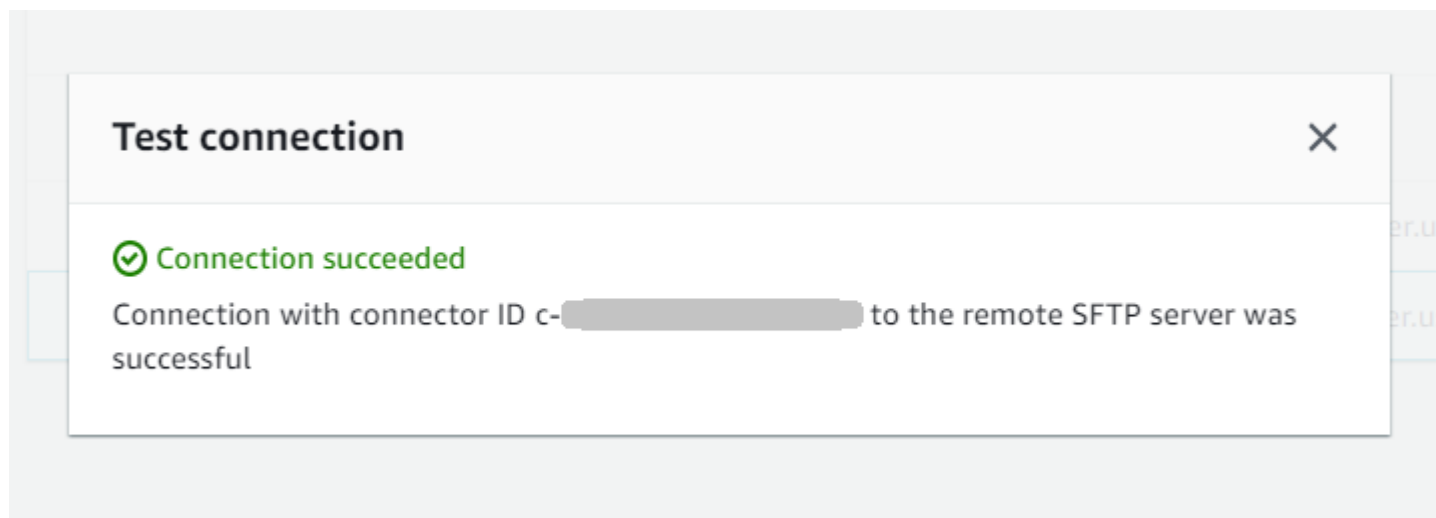
Après avoir créé un connecteur SFTP, nous vous recommandons de le tester avant de tenter de transférer des fichiers à l'aide de votre nouveau connecteur.

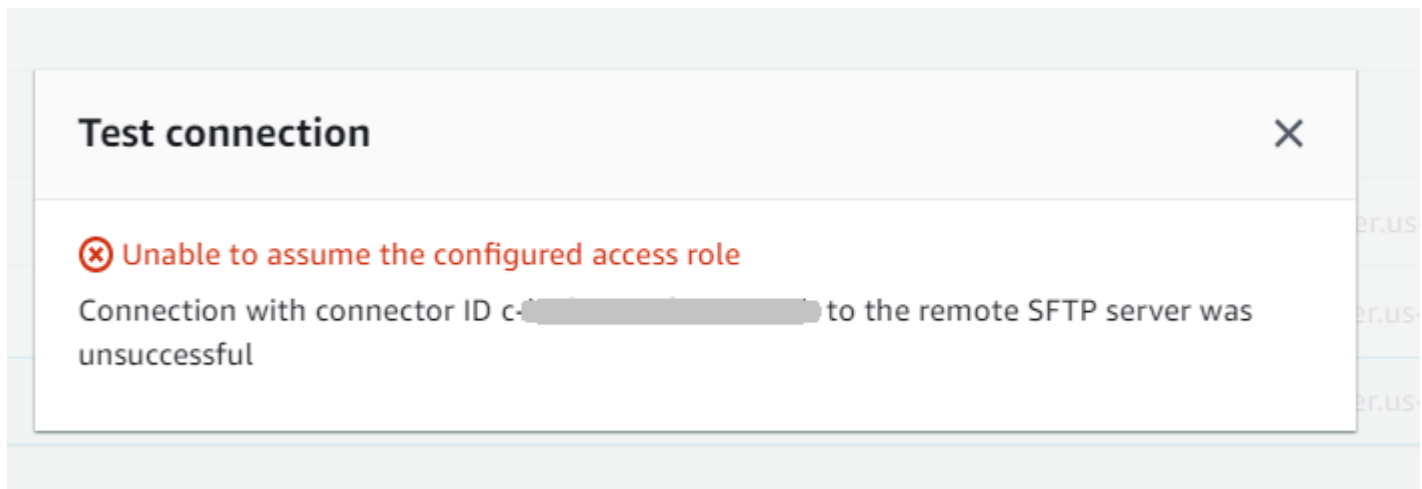
Pour tester un connecteur SFTP

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 SFTP 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 utiliser l'API afin de tester votre connecteur, consultez la documentation de l'[TestConnection](#) API.

Connectivité VPC pour connecteurs SFTP

AWS Transfer Family Les connecteurs SFTP prennent en charge la connectivité aux serveurs SFTP distants via vos environnements VPC à l'aide d'Amazon VPC Lattice. Cela vous permet de vous connecter à des serveurs SFTP hébergés en privé ou d'acheminer le trafic Internet via les contrôles de sécurité de votre VPC, et d'utiliser vos propres passerelles NAT et adresses IP élastiques.

Types de sorties

Les connecteurs SFTP peuvent utiliser l'un des deux types de sortie suivants :

- Service géré (par défaut) : le connecteur utilise des passerelles NAT et des adresses IP détenues par AWS Transfer Family pour acheminer les connexions via l'Internet public.
- VPC_LATTICE : Le connecteur achemine le trafic via votre environnement VPC à l'aide de Resource Access. Cross-VPC

Quand utiliser la connectivité VPC

Utilisez la connectivité VPC pour les connecteurs SFTP dans les scénarios suivants :

- Serveurs SFTP privés : connectez-vous à des serveurs SFTP uniquement accessibles depuis votre VPC.
- On-premises connectivité : connectez-vous aux serveurs SFTP locaux via Direct AWS Connect ou des connexions AWS Site-to-Site VPN.
- Adresses IP personnalisées : utilisez vos propres passerelles NAT et adresses IP élastiques, y compris les scénarios BYOIP.
- Contrôles de sécurité centralisés : acheminez les transferts de fichiers par le biais des ingress/egress contrôles centraux de votre entreprise.

Exigences

Avant de créer un connecteur VPC_ LATTICE-enabled SFTP, vous devez :

- VPC et infrastructure associée (sous-réseaux, tables de routage, groupes de sécurité)
- Passerelle de ressources dans votre VPC (au moins deux zones de disponibilité)
- Configuration des ressources spécifiant le serveur SFTP cible

Pour des instructions de configuration détaillées, voir [Création d'un connecteur VPC_ SFTP LATTICE-enabled](#). Et, pour des exemples, voir [Exemples de connectivité VPC pour les connecteurs SFTP](#).

Utilisation de connecteurs SFTP

Cette rubrique décrit comment effectuer les opérations sur les fichiers prises en charge à l'aide de votre connecteur SFTP. Vous pouvez également trouver des exemples de commandes pour effectuer ces opérations en sélectionnant les détails de votre connecteur sur la AWS Transfer Family console à l'adresse <https://console.aws.amazon.com/transfer/>.

Après avoir créé un connecteur SFTP, vous pouvez l'utiliser pour effectuer les opérations de fichier suivantes sur le serveur SFTP distant auquel il est associé.

- Envoyez des fichiers depuis Amazon S3 vers le serveur SFTP distant.
- Récupérez des fichiers depuis le serveur SFTP distant vers Amazon S3.
- Répertoirez les fichiers et les sous-dossiers d'un répertoire sur le serveur SFTP distant.
- Supprimez, renommez ou déplacez des fichiers et des répertoires sur le serveur SFTP distant.

Pour plus de détails sur la création de connecteurs, voir [Création de connecteurs SFTP](#).

Rubriques

- [Transférer des fichiers](#)
- [Lister le contenu d'un répertoire distant](#)
- [Déplacer, renommer ou supprimer des fichiers ou des répertoires sur le serveur distant](#)

Transférer des fichiers

Rubriques

- [Envoyer et récupérer des fichiers à l'aide d'un connecteur SFTP](#)

Envoyer et récupérer des fichiers à l'aide d'un connecteur SFTP

Pour envoyer et récupérer des fichiers à l'aide d'un connecteur SFTP, vous devez utiliser l'opération [StartFileTransfer](#) API et spécifier les paramètres suivants, selon que vous envoyez des fichiers (transferts sortants) ou que vous recevez des fichiers (transferts entrants). Notez que chaque `StartFileTransfer` demande peut contenir 10 chemins distincts.

Note

Par défaut, les connecteurs SFTP traitent un fichier à la fois, transférant les fichiers de manière séquentielle. Vous pouvez accélérer les performances de transfert en demandant à vos connecteurs de créer des sessions simultanées avec des serveurs distants qui prennent en charge les sessions simultanées du même utilisateur et traitent jusqu'à 5 fichiers en parallèle.

Pour activer les connexions simultanées pour n'importe quel connecteur, vous pouvez modifier le paramètre `Nombre maximal de connexions simultanées` lors de la création ou de la mise à jour d'un connecteur. Pour en savoir plus, consultez [Création d'un connecteur SFTP avec sortie gérée par service](#).

- Transferts sortants
 - `send-file-paths` contient de un à dix chemins de fichiers sources, pour les fichiers à transférer vers le serveur SFTP du partenaire.
 - `remote-directory-path` est le chemin distant vers lequel envoyer un fichier sur le serveur SFTP 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 serveur SFTP 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 `/amzn-s3-demo-source-bucket/file1.txt` et `/amzn-s3-demo-source-bucket/file2.txt` situés dans le stockage Amazon S3 vers le `/tmp` répertoire du serveur SFTP de votre partenaire. Pour utiliser cet exemple de commande, remplacez le `amzn-s3-demo-source-bucket` par votre propre bucket.

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
  --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

Pour récupérer des fichiers, vous devez spécifier les `local-directory-path` paramètres `retrieve-file-paths` et. L'exemple suivant extrait les fichiers `/my/remote/file1.txt` et les place `/my/remote/file2.txt` sur le serveur SFTP du partenaire dans l'emplacement Amazon S3 `/amzn-s3-demo-bucket/`. `prefix` Pour utiliser cet exemple de commande, remplacez `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 /amzn-s3-demo-bucket/prefix --connector-id
c-2222BBBB3333CCCC4 --region us-east-2
```

Les exemples précédents spécifient des chemins absolus sur le serveur SFTP. Vous pouvez également utiliser des chemins relatifs, c'est-à-dire des chemins relatifs au répertoire personnel de l'utilisateur SFTP. Par exemple, si l'utilisateur SFTP est `marymajor` et que son répertoire personnel sur le serveur SFTP est `/users/marymajor/`, la commande suivante envoie à `/amzn-s3-demo-source-bucket/file1.txt` `/users/marymajor/test-connectors/file1.txt`

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt \
```

```
--remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --  
region us-east-2
```

Lister le contenu d'un répertoire distant

Avant de récupérer des fichiers depuis un serveur SFTP distant, vous pouvez récupérer le contenu d'un répertoire sur le serveur SFTP distant. Pour ce faire, vous devez utiliser l'opération [StartDirectoryListing](#) API.

L'exemple suivant répertorie le contenu du home dossier sur le serveur SFTP distant, qui est spécifié dans la configuration du connecteur. Les résultats sont placés dans l'emplacement `/amzn-s3-demo-bucket/connector-files` Amazon S3 et dans un fichier nommé `c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json`.

```
aws transfer start-directory-listing \  
  --connector-id c-AAAA1111BBBB2222C \  
  --output-directory-path /amzn-s3-demo-bucket/example/connector-files \  
  --remote-directory-path /home
```

Cette AWS CLI commande renvoie un numéro de liste et le nom du fichier contenant les résultats.

```
{  
  "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",  
  "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"  
}
```

Note

La convention de dénomination du fichier de sortie est `connector-ID-listing-ID.json`.

Le fichier JSON contient les informations suivantes :

- `filePath`: le chemin complet d'un fichier distant, relatif au répertoire de la demande de listage pour votre connecteur SFTP sur le serveur distant.
- `modifiedTimestamp`: la dernière fois que le fichier a été modifié, en secondes, au format UTC (Coordinated Universal Time). Ce champ est facultatif. Si les attributs du fichier distant ne contiennent pas d'horodatage, celui-ci est omis de la liste des fichiers.

- **size**: la taille du fichier, en octets. Ce champ est facultatif. Si les attributs du fichier distant ne contiennent pas de taille de fichier, celui-ci est omis de la liste des fichiers.
- **path**: le chemin complet d'un répertoire distant, relatif au répertoire de la demande de listage pour votre connecteur SFTP sur le serveur distant.
- **truncated**: un drapeau indiquant si la sortie de la liste contient tous les éléments contenus dans le répertoire distant ou non. Si votre valeur en **truncated** sortie est vraie, vous pouvez augmenter la valeur fournie dans l'attribut **max-items** d'entrée facultatif pour pouvoir répertorier davantage d'éléments (jusqu'à la taille de liste maximale autorisée de 200 000 éléments).

Voici un exemple du contenu du fichier de sortie (c-

AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json), où le répertoire distant contient deux fichiers et deux sous-répertoires (chemins).

```
{
  "files": [
    {
      "filePath": "/home/what.txt",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 2323
    },
    {
      "filePath": "/home/how.pgp",
      "modifiedTimestamp": "2024-01-30T20:34:54Z",
      "size" : 4691
    }
  ],
  "paths": [
    {
      "path": "/home/magic"
    },
    {
      "path": "/home/aws"
    }
  ],
  "truncated": "false"
}
```

Déplacer, renommer ou supprimer des fichiers ou des répertoires sur le serveur distant

Rubriques

- [Déplacer ou renommer des fichiers ou des répertoires sur le serveur SFTP distant](#)
- [Supprimer des fichiers ou des répertoires sur le serveur SFTP distant](#)

Déplacer ou renommer des fichiers ou des répertoires sur le serveur SFTP distant

Vous pouvez utiliser un connecteur SFTP pour déplacer ou renommer des fichiers et des répertoires sur un serveur SFTP distant. Notez que le serveur distant doit prendre en charge ces opérations pour un traitement réussi à l'aide de connecteurs.

Certains cas d'utilisation courants sont les suivants.

- Un serveur distant génère ou reçoit un nouveau fichier toutes les heures, avec le même nom de fichier mais un horodatage différent. Pour maintenir le dossier principal à jour (afin qu'il ne contienne que le dernier fichier), vous pouvez utiliser un connecteur pour déplacer les anciens fichiers vers un dossier archivé.
- Vous utilisez un connecteur pour répertorier tous les fichiers d'un répertoire distant, puis vous transférez tous les fichiers vers votre stockage local. Vous pouvez ensuite utiliser un connecteur pour déplacer les fichiers vers un dossier archivé sur le serveur distant.

Vous devez utiliser un `StartRemoteMove` appel pour chaque fichier ou répertoire que vous souhaitez traiter, car la commande prend un seul fichier ou répertoire source et de destination comme arguments. Cependant, vous pouvez améliorer les performances en demandant à vos connecteurs de créer des sessions simultanées avec des serveurs distants qui prennent en charge les sessions simultanées du même utilisateur et `move/rename` jusqu'à 5 fichiers en parallèle.

L'exemple suivant déplace un fichier sur le serveur SFTP distant de `/source/folder/sourceFile` vers `/destination/targetFile` et renvoie un identifiant unique pour l'opération.

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \  
  --source-path /source/folder/sourceFile --target-path /destination/targetFile
```

 Note

Pour les move/rename opérations, Transfer Family utilise la SFTP `SSH_FXP_RENAME` commande standard pour effectuer l' move/rename opération.

Supprimer des fichiers ou des répertoires sur le serveur SFTP distant

Vous pouvez utiliser un connecteur SFTP pour supprimer des fichiers ou des répertoires sur un serveur SFTP distant. Notez que le serveur distant doit prendre en charge ces opérations pour un traitement réussi à l'aide de connecteurs.

 Note

Les opérations de suppression pour les répertoires distants ne sont prises en charge que pour les répertoires vides.

Certains cas d'utilisation courants sont les suivants.

- Vous utilisez un connecteur pour récupérer un fichier depuis un serveur SFTP distant, le stocker dans votre compartiment Amazon S3, puis le chiffrer. Enfin, vous pouvez utiliser un connecteur pour supprimer le fichier non chiffré sur le serveur distant.
- Vous utilisez un connecteur pour répertorier tous les fichiers d'un répertoire distant, puis vous transférez tous les fichiers vers votre stockage local. Vous pouvez ensuite utiliser un connecteur pour supprimer tous les fichiers que vous avez transférés. Vous pouvez également supprimer le répertoire distant si vous le souhaitez.

Vous devez utiliser un `StartRemoteDelete` appel pour chaque fichier ou répertoire que vous souhaitez supprimer, car la commande prend un seul fichier ou répertoire comme argument. Cependant, vous pouvez améliorer les performances en demandant à vos connecteurs de créer des sessions simultanées avec des serveurs distants qui prennent en charge les sessions simultanées du même utilisateur, et en supprimant jusqu'à 5 files/directories en parallèle.

L'exemple suivant supprime un fichier sur le serveur SFTP distant dans le chemin `/delete/folder/deleteFile` et renvoie un identifiant unique pour l'opération.

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \
```

```
--delete-path /delete/folder/deleteFile
```

Note

Pour l'opération de suppression, Transfer Family utilise la `SSH_FXP_REMOVE` commande standard pour supprimer un fichier et `SSH_FXP_RMDIR` un répertoire.

Surveillance des connecteurs SFTP

Vous pouvez surveiller l'état des opérations de votre connecteur en utilisant l'une des méthodes suivantes. Choisissez l'approche qui répond à vos besoins.

Utilisez l'API du connecteur pour connaître l'état des demandes de transfert de fichiers

Pour suivre la progression d'une opération de transfert de fichiers, vous utilisez l'opération [ListFileTransferResults](#) API, qui renvoie des mises à jour en temps réel et des informations détaillées sur le statut de chaque fichier transféré dans le cadre d'une opération de transfert de fichiers spécifique. Vous spécifiez le transfert de fichier en fournissant son identifiant de connecteur et son identifiant de transfert. L'exemple suivant renvoie une liste de fichiers pour l'ID du connecteur `a-11112222333344444` et l'ID de transfert `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.

```
aws transfer list-file-transfer-results --connector-id a-11112222333344444 --transfer-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Note

Les résultats du transfert de fichiers sont disponibles jusqu'à 7 jours après l'appel de l'opération `ListFileTransferResults` API.

Vous pouvez également consulter les journaux et les événements relatifs à vos demandes de transfert de fichiers utilisant des connecteurs SFTP. EventBridge Les événements Amazon pour Transfer Family sont décrits dans [Événements relatifs au connecteur SFTP](#). Pour savoir comment consulter les entrées du CloudWatch journal Transfer Family, consultez [Afficher les flux de log de Transfer Family](#).

Afficher les événements relatifs au connecteur SFTP sur Amazon EventBridge

Pour chaque opération effectuée par les connecteurs SFTP, Transfer Family génère et envoie automatiquement des événements au bus d'événements par défaut de votre EventBridge compte Amazon. Les événements contiennent des métadonnées détaillées sur l'opération, y compris son état. Vous pouvez vous abonner à ces événements dans EventBridge, appliquer des filtres sur des critères d'événements spécifiques tels que l'état de l'opération, et déclencher automatiquement des actions en aval en fonction de l'état. Pour plus de détails sur les événements générés par les opérations du connecteur SFTP, consultez [Événements relatifs au connecteur SFTP](#).

Afficher les journaux du connecteur SFTP sur Amazon CloudWatch

Toutes les opérations du connecteur SFTP génèrent des connexions détaillées. CloudWatch Par exemple, les entrées de journal générées par les connecteurs SFTP, voir [Exemples d'entrées de journal pour les connecteurs SFTP](#).

Surveillance des connecteurs de type sortie VPC

Les connecteurs de type sortie VPC offrent des fonctionnalités de surveillance et des considérations supplémentaires au-delà des connecteurs de gestion de services standard :

Surveillance de l'état du connecteur

Les connecteurs VPC_LATTICE incluent des informations supplémentaires pour vous aider à surveiller le provisionnement et l'état opérationnel :

- EgressType champ : S'affiche VPC pour les connecteurs de type sortie VPC_LATTICE
- EgressConfig champ : contient l'ARN de configuration des ressources et les informations de port

Surveillez l'état du connecteur à l'aide de `describe-connector` l'API :

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

Surveillance des coûts du réseau VPC

Les connecteurs de type sortie VPC entraînent des frais supplémentaires liés au réseau VPC que vous devez surveiller :

- Frais du fournisseur de ressources : 0\$ vous sont facturés. 006/GB pour le traitement des données en tant que fournisseur de ressources (facturé directement par VPC Lattice)
- Frais de consommation de ressources : AWS Transfer Family absorbe les 0\$. 01/GB coûts de consommation des ressources (1 premier PB)
- Frais de passerelle NAT : pour les points de terminaison publics accessibles via VPC, des frais supplémentaires de passerelle NAT et de transfert de données peuvent s'appliquer
- Frais de Transfer Family : 0\$ standard. 40/GB les frais de traitement des données s'appliquent toujours

Surveillez l'utilisation et les coûts du VPC Lattice via la console AWS Cost and Billing, en filtrant par le service VPC Lattice.

Surveillance réseau pour connecteurs VPC

Surveillez l'activité et les performances du réseau pour les connecteurs de type sortie VPC :

- Journaux de flux VPC : activez les journaux de flux VPC pour surveiller les modèles de trafic réseau entre les passerelles de ressources et les serveurs SFTP
- Journaux d'accès VPC Lattice : VPC Lattice fournit des journaux d'accès indiquant les adresses source/destination IP, le calendrier des connexions et les volumes de transfert de données
- Surveillance des groupes de sécurité : surveillez les règles des groupes de sécurité et les modèles de trafic pour garantir des contrôles d'accès au réseau appropriés
- Surveillance de la résolution DNS : surveillez les temps de résolution DNS et les défaillances des points de terminaison du réseau de service

Exemple d'entrée dans le journal d'accès au réseau VPC :

```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/
sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-12345678",
  "protocol": "tcp",
  "sourceIpPort": "10.0.1.100:33760",
  "destinationIpPort": "10.0.2.200:22",
```



```
"gatewayIpPort": "10.0.1.150:1769",  
"resourceIpPort": "10.0.2.200:22"  
}
```

Résolution des problèmes grâce à la surveillance

Utilisez les données de surveillance pour résoudre les problèmes courants liés aux connecteurs VPC :

- **État EN ATTENTE** : surveillez la progression de la résolution DNS et attendez le statut ACTIF avant de tenter de transférer
- **Délais de connexion** : vérifiez les journaux de flux VPC et les règles des groupes de sécurité pour détecter le trafic bloqué sur le port 22
- **Défaillances de transfert** : consultez CloudWatch les journaux pour les messages d'erreur détaillés et les journaux d'accès VPC Lattice pour les problèmes au niveau du réseau
- **Problèmes de performances** : surveillez les journaux d'accès au réseau VPC pour connaître le calendrier de connexion et les indicateurs de débit

Gestion des connecteurs SFTP

Cette rubrique explique comment afficher et mettre à jour les connecteurs SFTP.

Note

Chaque connecteur reçoit automatiquement des adresses IP statiques qui restent inchangées pendant toute la durée de vie du connecteur. Cela vous permet de vous connecter à des serveurs SFTP distants qui n'acceptent que les connexions entrantes provenant d'adresses IP connues. Vos connecteurs se voient attribuer un ensemble d'adresses IP statiques partagées par tous les connecteurs utilisant le même protocole (SFTP ou AS2) dans votre compte AWS. Ces adresses ne sont pas exclusivement dédiées à votre compte.

Si vous avez besoin d'adresses IP dédiées et prévisibles, configurez vos connecteurs avec une VPC-based sortie. Pour de plus amples informations, veuillez consulter [the section called "Création d'un connecteur SFTP avec sortie VPC-based"](#).

Mettre à jour les connecteurs SFTP

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
```

Mise à jour des paramètres de connectivité VPC

Vous pouvez mettre à jour les paramètres de connectivité VPC pour les connecteurs existants, notamment en basculant entre le type de sortie géré par le service et le type de sortie VPC ou en modifiant l'ARN de configuration des ressources.

Pour passer d'un connecteur géré par des services à une sortie VPC, procédez comme suit :

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-type VPC \
  --egress-config ResourceConfigurationArn=resource-configuration-arn
```

Pour mettre à jour l'ARN de configuration des ressources pour un connecteur VPC_ LATTICE-enabled :

```
aws transfer update-connector \
  --connector-id connector-id \
  --egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

Note

Lors de la mise à jour des paramètres de connectivité VPC, l'état du connecteur passe au PENDING cours du processus de reconfiguration. Surveillez l'état du connecteur à l'aide de la `describe-connector` commande.

Afficher les détails du connecteur SFTP

Vous trouverez la liste des détails et des propriétés d'un connecteur SFTP 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 connecteur SFTP en choisissant Modifier sur la page de détails du connecteur.

Surveillance de l'état du connecteur VPC

Les LATTICE-enabled connecteurs VPC_ incluent des informations d'état supplémentaires pour vous aider à surveiller le processus de provisionnement :

- État : PENDING ÉmissionsACTIVE, ou ERRORRED
- EgressType: Émissions VPC ou SERVICE_MANAGED
- EgressConfig: contient l'ARN de configuration des ressources pour les connecteurs VPC
- Erreur : fournit des informations d'erreur détaillées si le connecteur est en ERRORRED état

Pour les connecteurs VPC, le ServiceManagedEgressIpAddresses champ sera nul car le trafic utilise plutôt vos adresses IP VPC.

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](#) la référence de l'API.

Dimensionnement et quotas pour les connecteurs SFTP

Rubriques

- [Quotas pour les connecteurs SFTP](#)
- [Dimensionnement de vos connecteurs SFTP](#)

Quotas pour les connecteurs SFTP

Les quotas suivants sont en place pour les connecteurs SFTP.

Note

D'autres quotas de service pour les connecteurs SFTP sont répertoriés dans les [AWS Transfer Family points de terminaison et les quotas](#) dans le. Référence générale d'Amazon Web Services

Quotas de connecteurs SFTP

Nom	Par défaut	Ajustable
Nombre maximal de transactions de connexion de test par seconde (TPS)	1 demande par seconde, par compte	Non
Taille de file d'attente maximale pour les transferts de fichiers en attente	1 000	Non
Taille maximale du fichier	150 Gibiots (GiB)	Non
Durée de transfert maximale par fichier	12 heures	Non

Nom	Par défaut	Ajustable
Temps d'attente maximal pour les demandes par fichier	12 heures	Non
Bande passante maximale pour les connecteurs par compte (les connecteurs SFTP et AS2 contribuent à cette valeur)	50 Mbits/s	Non
Nombre maximum d'éléments pour les opérations de listage dans les annuaires	200 000	Non

Note

Par défaut, les connecteurs SFTP traitent un fichier à la fois, transférant les fichiers de manière séquentielle. Vous pouvez accélérer les performances de transfert en demandant à vos connecteurs de créer des sessions simultanées avec des serveurs distants qui prennent en charge les sessions simultanées du même utilisateur et traitent jusqu'à 5 fichiers en parallèle.

Pour activer les connexions simultanées pour n'importe quel connecteur, vous pouvez modifier le paramètre Nombre maximal de connexions simultanées lors de la création ou de la mise à jour d'un connecteur. Pour en savoir plus, consultez [Création d'un connecteur SFTP avec sortie gérée par service](#).

Pour stocker les informations d'identification des connecteurs SFTP, 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

Dimensionnement de vos connecteurs SFTP

Cette section décrit les considérations relatives à la manière de dimensionner les charges de travail de votre connecteur AWS Transfer Family SFTP. Vous devez tenir compte des trois quotas suivants qui s'appliquent lorsque vous souhaitez dimensionner vos charges de travail à l'aide de connecteurs SFTP.

- Taille maximale de la file d'attente. Cela fait référence au nombre maximum d'opérations en attente dans la file d'attente d'un connecteur qui ont été demandées. Une opération en attente fait référence à toute demande de transfert soumise précédemment qui n'est pas encore terminée, que ce soit avec succès ou sans succès.

La profondeur de file d'attente maximale pour les demandes en attente est actuellement fixée à 1 000 par connecteur (comme défini dans les [quotas de AWS Transfer Family service](#)). Vos charges de travail peuvent dépasser cette limite de service lorsque vous demandez des milliers d'opérations de transfert sur une courte durée, et vous recevrez un message `ThrottlingException` avec le message « Dépassement du nombre maximum de demandes en attente ». Si vos charges de travail sont soumises à ce quota, contactez l'équipe du service Transfer Family AWS Support ou l'équipe chargée de votre compte pour discuter de vos besoins en matière d'évolutivité.

Vous pouvez également effectuer l'une ou l'autre des actions suivantes, ou les deux.

- Répartissez vos volumes de fichiers sur plusieurs connecteurs.
- Demandez à vos connecteurs de créer des sessions simultanées avec le serveur distant pour traiter en parallèle plusieurs demandes provenant de la file d'attente.
- Le nombre de sessions simultanées. Par défaut, un connecteur SFTP transfère un fichier à la fois, en transférant les fichiers de manière séquentielle depuis sa file d'attente.

Vous avez la possibilité d'accélérer les performances de transfert en faisant en sorte que vos connecteurs transfèrent plusieurs fichiers en parallèle. Vous pouvez créer des sessions simultanées avec des serveurs distants qui prennent en charge les sessions simultanées du même utilisateur et traitent jusqu'à 5 fichiers en parallèle. Lorsque vous créez un connecteur SFTP, choisissez une valeur maximale de 5 pour le paramètre Nombre maximal de connexions simultanées lorsque vous créez ou mettez à jour le connecteur. Pour en savoir plus, consultez [Création d'un connecteur SFTP avec sortie gérée par service](#).

- Le taux de **StartFileTransfer** demandes. Vous pouvez demander jusqu'à 100 chemins de fichiers par seconde pour le transfert avec chaque connecteur SFTP. Les chemins de fichiers

demandés sont ajoutés à la file d'attente de vos connecteurs pour être traités. Vous pouvez utiliser la `StartFileTransfer` commande de manière récursive pour demander jusqu'à 100 chemins de fichiers par seconde et par connecteur, quel que soit le nombre de fichiers fourni dans une `StartFileTransfer` commande individuelle.

Architectures de référence utilisant des connecteurs SFTP

Cette section répertorie les documents de référence disponibles pour configurer des flux de transfert de fichiers automatisés à l'aide de connecteurs SFTP. Vous pouvez concevoir vos propres architectures pilotées par les événements en utilisant les événements du connecteur SFTP dans Amazon EventBridge, pour orchestrer votre action de transfert de fichiers et les actions de pré-traitement et de post-traitement dans AWS.

Billets de blogs

Le billet de blog suivant fournit une architecture de référence pour créer un flux de travail MFT à l'aide de connecteurs SFTP, y compris le chiffrement de fichiers à l'aide de PGP avant de les envoyer à un serveur SFTP distant à l'aide de connecteurs SFTP : [Architecture de transferts de fichiers gérés sécurisés et conformes avec AWS Transfer Family les connecteurs SFTP et le chiffrement PGP](#).

Ateliers

- L'atelier suivant propose des ateliers pratiques sur la configuration des connecteurs SFTP et l'utilisation de vos connecteurs pour envoyer ou récupérer des fichiers depuis des serveurs SFTP distants : [Transfer Family - SFTP workshop](#).
- [L'atelier suivant propose des ateliers pratiques pour créer des flux de travail entièrement automatisés et pilotés par des événements impliquant le transfert de fichiers vers ou depuis des serveurs SFTP externes vers Amazon S3, ainsi que le prétraitement et le post-traitement courants de ces fichiers : atelier MFT. Event-driven](#)

Cette vidéo présente un aperçu de cet atelier.

Des solutions

AWS Transfer Family propose les solutions suivantes :

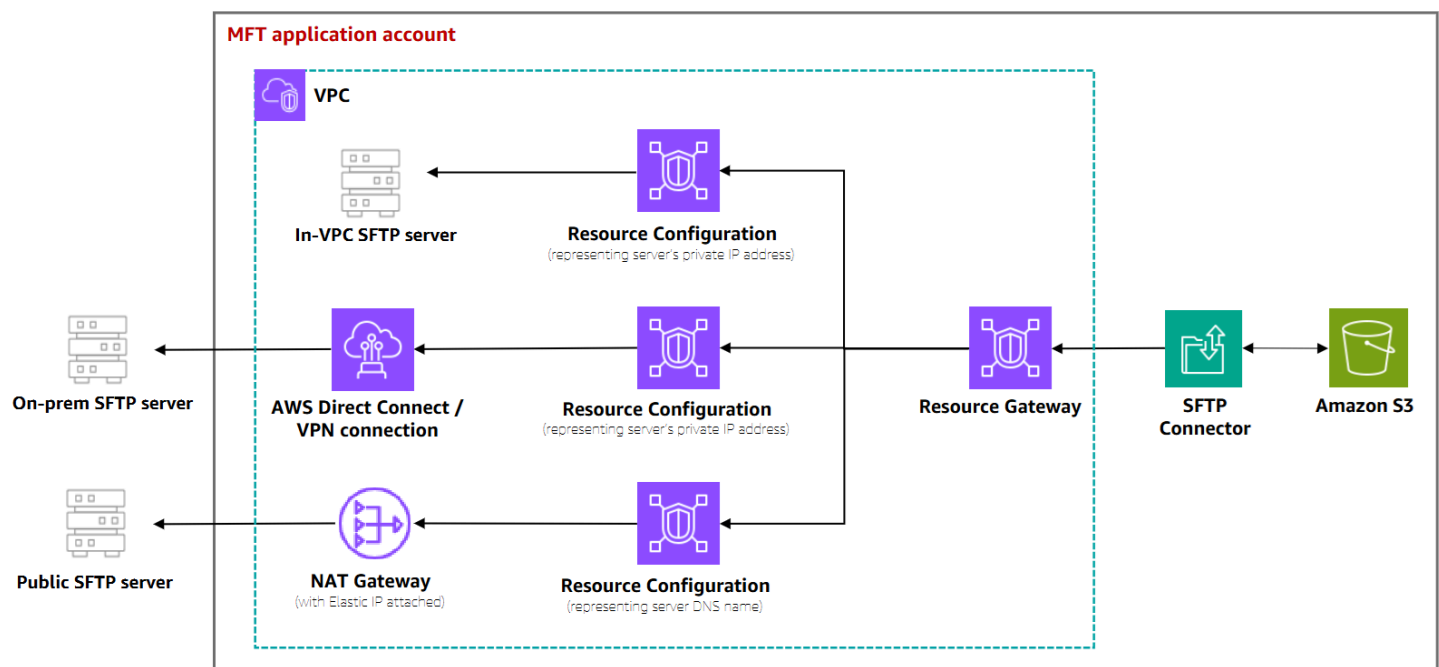
- La [solution de synchronisation des transferts de fichiers](#) fournit une architecture de référence pour automatiser le processus de synchronisation des répertoires SFTP distants, y compris des structures de dossiers complètes, avec vos compartiments Amazon S3 locaux à l'aide d'un connecteur SFTP. Il orchestre le processus de listage des répertoires distants, de détection des modifications et de transfert de fichiers nouveaux ou modifiés.
- [Serverlessland - Transfert de fichiers sélectif entre un serveur SFTP distant et S3 ; l'utilisation AWS Transfer Family](#) fournit un exemple de modèle pour répertorier les fichiers stockés sur des emplacements SFTP distants et transférer des fichiers sélectifs vers Amazon S3.

Architectures de référence VPC

Les architectures de référence suivantes présentent des modèles courants de déploiement de connecteurs LATTICE-enabled VPC_SFTP. Ces exemples vous aident à comprendre où les ressources VPC Lattice doivent être créées dans votre architecture globale. AWS

Compte unique avec infrastructure de sortie partagée

Dans cette architecture, l'infrastructure de sortie (passerelle NAT, tunnel VPN ou Direct Connect) est configurée dans un VPC au sein du même compte que vos connecteurs SFTP. Tous les connecteurs peuvent partager la même passerelle de ressources et la même passerelle NAT.

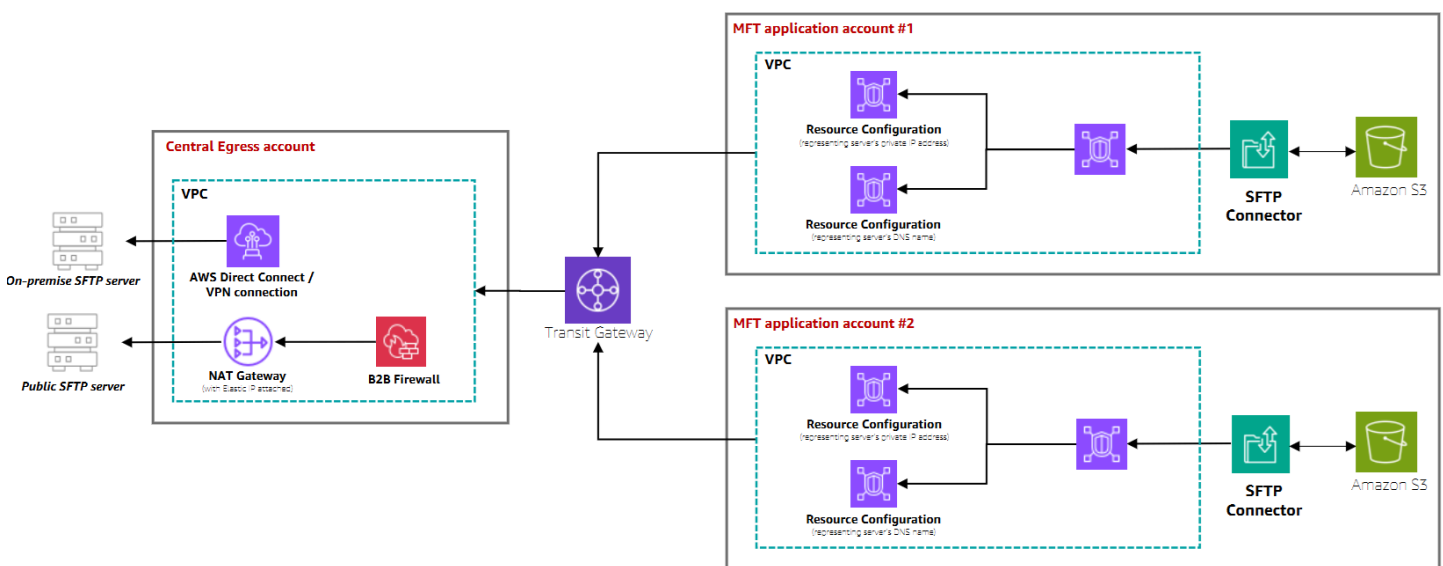


Ce modèle est idéal lorsque :

- Tous les connecteurs SFTP sont gérés en un seul Compte AWS
- L'infrastructure de sortie est configurée dans un VPC au sein du même compte que vos connecteurs SFTP

Cross-account avec une infrastructure de sortie centralisée

Dans cette architecture, l'infrastructure de sortie (passerelle NAT, tunnel VPN, Direct Connect ou pare-feux B2B) est configurée dans un compte de sortie central géré par l'équipe réseau. Les connecteurs SFTP sont créés dans le compte d'application MFT géré par l'équipe d'administration MFT. Cross-account le réseau est établi à l'aide de Transit Gateway pour respecter les règles de réseau existantes.



Ce modèle est idéal lorsque :

- L'infrastructure réseau est gérée par une équipe distincte dans un compte dédié
- Vous avez des itinéraires existants (tels que AWS Transit Gateway) entre le compte où les connecteurs SFTP sont créés et le compte où l'infrastructure de sortie est configurée. Les connecteurs SFTP pourront tirer parti de vos itinéraires existants reliant les deux comptes.
- Des contrôles de sécurité centralisés et des pare-feux B2B sont nécessaires
- Vous devez maintenir la séparation des tâches entre les équipes de mise en réseau et d'application

AWS Transfer Family pour AS2

La déclaration d'applicabilité 2 (AS2) est une spécification de RFC-defined transmission de fichiers qui inclut de solides mécanismes de protection et de vérification des messages. La protection d'une charge utile AS2 en transit utilise la syntaxe des messages cryptographiques (CMS) associée au chiffrement et aux signatures numériques pour assurer la protection des données et l'authentification des pairs. Une charge utile de réponse MDN (Message Disposition Notice) signée permet de vérifier (non répudiation) qu'un message a été reçu et correctement déchiffré.

Le protocole AS2 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. AWS Transfer Family Les terminaux AS2 sont [certifiés Drummond](#), ce qui permet aux clients de secteurs tels que le commerce de détail, les sciences de la vie, la fabrication, les services financiers et les services publics d'effectuer des transactions en toute sécurité avec leurs partenaires commerciaux.

Lorsque vous utilisez AS2 avec Transfer Family, les données traitées sont accessibles de manière native dans les formats suivants : AWS

- Traitement, analyse et apprentissage automatique
- Intégration aux systèmes de planification des ressources d'entreprise (ERP)
- Intégration aux systèmes de gestion de la relation client (CRM)

Pour échanger des fichiers avec un partenaire disposant d'un AS2-enabled serveur, vous devez :

- Génération d'une paire de clés publique-privée pour le chiffrement
- Générez une paire de clés publique-privée pour la signature
- Échangez les clés publiques avec votre partenaire

Important

Les points de terminaison du serveur HTTPS AS2 ne sont actuellement pas pris en charge. Vous êtes responsable de la résiliation du protocole TLS.

Transfer Family propose un atelier auquel vous pouvez participer, au cours duquel vous pouvez configurer un point de terminaison Transfer Family avec AS2 activé et un connecteur Transfer Family AS2. Vous pouvez consulter les détails de cet atelier [ici](#).

Pour obtenir des instructions détaillées sur la configuration d'AS2 dans Transfer Family, consultez ce qui suit :

1. [Importer des certificats AS2](#)
2. [Création de profils AS2](#)
3. [Création d'un serveur AS2](#)
4. [Création d'un accord AS2](#)
5. [Configuration des connecteurs AS2](#)

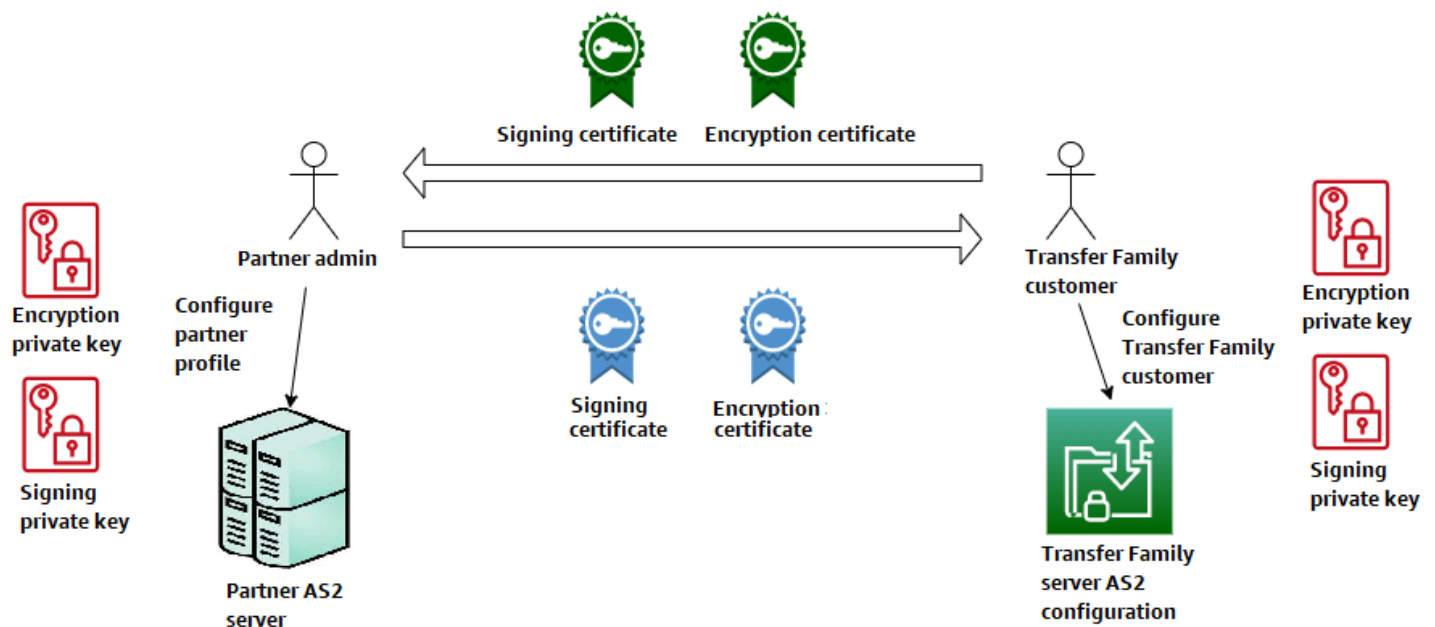
Pour un exemple complet, voir [Configuration d'une configuration AS2](#).

 Note

Pour montrer la prise en charge des modèles AS2 Terraform, ajoutez une réaction positive (#) à la demande de fonctionnalité des modèles Transfer [Family Terraform](#). Vous pouvez également ajouter un commentaire décrivant votre cas d'utilisation.

Cas d'utilisation de l'AS2

Si vous êtes un AWS Transfer Family client qui souhaite échanger des fichiers avec un partenaire disposant d'un AS2-enabled serveur, 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 de MDN dans le tableau suivant supposent des MDN signés.

Cas d'utilisation de l'AS2

Inbound-only cas d'utilisation

- Transférez des messages AS2 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 utilisant le protocole AS2.
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 des messages AS2 cryptés 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 des messages AS2 cryptés d'un partenaire commercial vers un serveur Transfer Family et ajoutez la signature et l'envoi d'une réponse MDN.

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 MDN signée.

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.

Outbound-only cas d'utilisation

- Transférez des messages AS2 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 serveur AS2, vous créez un connecteur. Dans ce cas, vous importez la clé publique de votre partenaire commercial dans son profil.

- Transférez des messages AS2 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 des messages AS2 cryptés d'un serveur Transfer Family vers un partenaire commercial, ajoutez une signature et envoyez une réponse MDN.

Vous n'effectuez toujours que des transferts sortants, mais désormais, en plus d'envoyer des charges utiles signées, vous souhaitez recevoir une réponse MDN signée de la part 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 des messages AS2 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 utilisant le protocole AS2.
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 des messages AS2 cryptés 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 des messages AS2 cryptés dans les deux sens entre un serveur Transfer Family et un partenaire commercial, ajoutez une signature et envoyez une réponse MDN.

Vous souhaitez désormais échanger des charges utiles signées, et vous et votre partenaire commercial souhaitez obtenir des réponses MDN.

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.

Modèles AS2 CloudFormation

Cette rubrique fournit des informations sur les AWS CloudFormation modèles que vous pouvez utiliser pour déployer rapidement des serveurs AS2 et des configurations pour AWS Transfer Family lesquels. Ces modèles automatisent le processus de configuration et vous aident à mettre en œuvre les meilleures pratiques pour les transferts de fichiers AS2.

- Le modèle AS2 de base est décrit dans [Utilisez un modèle pour créer un stack Transfer Family AS2 de démonstration](#)
- Le modèle AS2 pour personnaliser les en-têtes HTTP est décrit dans. [Personnalisation des en-têtes HTTP pour les messages AS2](#)

Personnalisation des modèles AS2

Vous pouvez personnaliser les modèles fournis pour répondre à vos besoins spécifiques :

1. Téléchargez le modèle à partir de l'URL S3.
2. Modifiez le code YAML pour ajuster des configurations telles que :
 - Paramètres de sécurité et configurations de certificats
 - Architecture réseau et paramètres VPC
 - Options de stockage et gestion des fichiers
 - Préférences de surveillance et de notification
3. Téléchargez votre modèle modifié dans votre propre compartiment S3.
4. Déployez le modèle personnalisé à l'aide de CloudFormation la console ou AWS CLI.

Important

Lorsque vous personnalisez des modèles, veillez à maintenir les dépendances entre les ressources et à suivre les meilleures pratiques en matière de sécurité.

Test de votre déploiement AS2

Après avoir déployé un serveur AS2 à l'aide d'un modèle, vous pouvez tester la configuration :

1. Vérifiez les sorties de la CloudFormation pile pour obtenir des exemples de commandes et des informations sur les points de terminaison.
2. Utilisez le AWS CLI pour envoyer un fichier de test :

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt
aws transfer start-file-transfer --connector-id your-connector-id --send-file-
paths /your-bucket-name/test.txt
```

3. Vérifiez la livraison des fichiers dans le compartiment S3 de destination.
4. Vérifiez les CloudWatch journaux pour vérifier la réussite du traitement et les réponses MDN.

Pour des tests plus complets, pensez à utiliser des clients AS2 tiers pour envoyer des fichiers à votre serveur Transfer Family AS2.

Bonnes pratiques pour le déploiement de modèles AS2

Suivez ces bonnes pratiques lorsque vous utilisez des CloudFormation modèles AS2 :

Sécurité

Utilisez des certificats fiables et alternez-les régulièrement.

Mettez en œuvre des politiques IAM fondées sur le principe du moindre privilège.

Limitez l'accès au réseau à l'aide de groupes de sécurité.

Fiabilité

Déployez sur plusieurs zones de disponibilité.

Mettez en place une surveillance et des alertes en cas d'échec des transferts.

Configurez des tentatives automatisées en cas d'échec des transferts.

Performance

Choisissez les types d'instances appropriés pour votre volume de transfert.

Mettez en œuvre des politiques de cycle de vie S3 pour une gestion efficace des fichiers.

Surveillez et optimisez les configurations réseau.

Optimisation des coûts

Utilisez l'auto-scaling pour les charges de travail variables.

Implémentez les classes de stockage S3 pour les anciens fichiers.

Surveillez et ajustez les ressources en fonction de l'utilisation réelle.

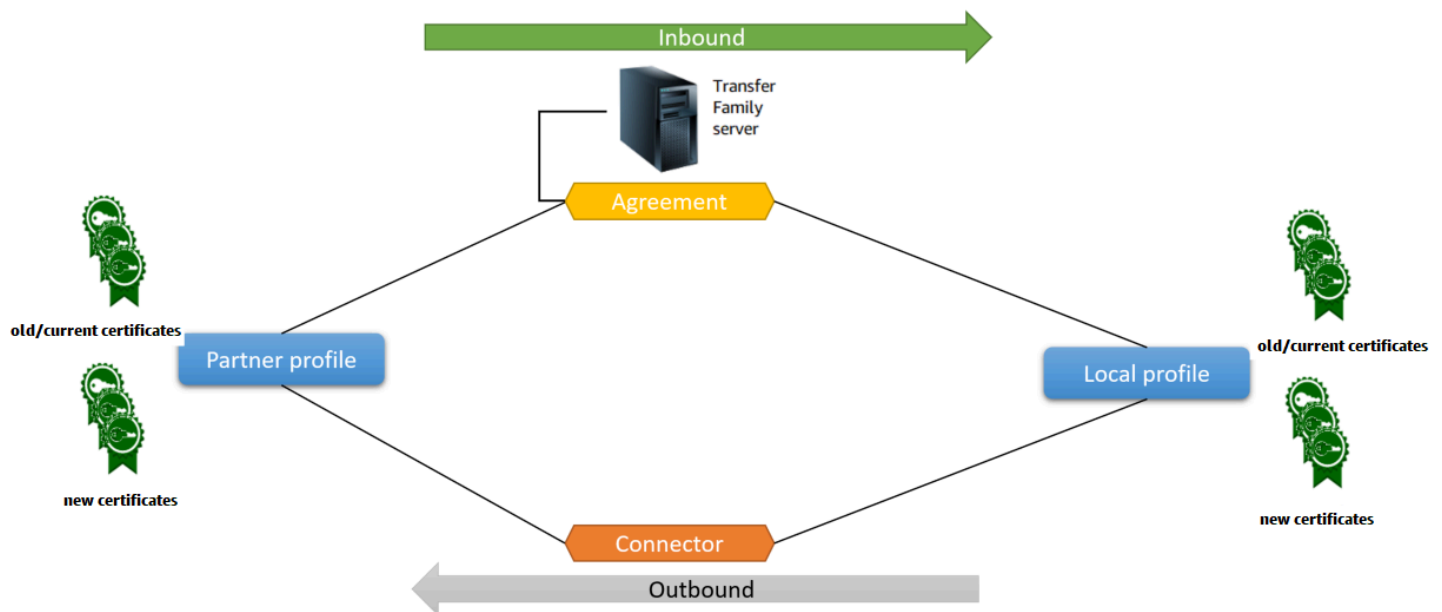
Configuration d'AS2

Pour créer un AS2-enabled serveur, vous devez également spécifier les composants suivants :

- **Accords** — Les accords bilatéraux entre 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 du serveur, du profil local, du profil du partenaire et du certificat. Transfer Family AS2-inbound traite les accords d'utilisation.
- **Certificats** — Les certificats à clé publique (X.509) sont utilisés dans les communications AS2 pour le chiffrement et la vérification des messages. Les certificats sont également utilisés pour les points de terminaison des connecteurs.
- **Profil locaux et profil de partenaires** — Un profil local définit l'organisation ou le « groupe » local (AS2-enabled Transfer Family server). 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 AS2-enabled serveurs, 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 non AWS serveur du client.

Le schéma suivant montre la relation entre les objets AS2 impliqués dans les processus entrants et sortants.



Pour un exemple de configuration AS2 de bout en bout, voir. [Configuration d'une configuration AS2](#)

Rubriques

- [Configurations AS2](#)
- [Quotas et limites AS2](#)
- [Caractéristiques et capacités de l'AS2](#)

Configurations AS2

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.

Signature, chiffrement, compression, MDN

Pour les transferts entrants et sortants, les éléments suivants sont obligatoires ou facultatifs :

- Chiffrement — Obligatoire (pour le transport HTTP, qui est la seule méthode de transport actuellement prise en charge). Les messages non chiffrés ne sont acceptés que s'ils sont transférés par un TLS-terminating proxy tel qu'un Application Load Balancer (ALB) et que X-Forwarded-Proto: https l'en-tête est présent.
- Signature — Facultatif

- Compression — Facultative (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
- 3DES (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 réponses MDN, certains types sont pris en charge, comme suit :

- Transferts entrants : synchrones et asynchrones
- Transferts sortants : synchrones et asynchrones
- Protocole de transfert de courrier simple (SMTP) (e-mail MDN) — Non pris en charge

Transports

- Transferts entrants : le protocole HTTP est le seul transport actuellement pris en charge, et vous devez le spécifier explicitement.

Note

Si vous devez utiliser le protocole HTTPS pour les transferts entrants, vous pouvez mettre fin au protocole TLS sur un Application Load Balancer ou un Network Load Balancer. Ceci est décrit sous [Recevoir des messages AS2 via HTTPS](#).

- Transferts sortants : si vous fournissez une URL HTTP, vous devez également spécifier un algorithme de chiffrement. Si vous fournissez une URL HTTPS, vous avez la possibilité de spécifier NONE pour votre algorithme de chiffrement.

Quotas et limites AS2

Cette section traite des quotas et des limites pour AS2.

Rubriques

- [Quotas AS2](#)
- [Quotas pour le traitement des secrets](#)
- [Limitations connues](#)

Quotas AS2

Les quotas suivants sont en place pour les transferts de fichiers AS2. Pour demander l'augmentation d'un quota ajustable, consultez les [Service AWS quotas](#) dans le Références générales AWS.

Quotas AS2

Nom	Par défaut	Ajustable
Nombre maximum de fichiers par demande sortante	10	Non
Nombre maximum de demandes sortantes par seconde	100	Non

Nom	Par défaut	Ajustable
Nombre maximum de demandes entrantes par seconde	100	Non
Bande passante sortante maximale par compte (les requêtes SFTP et AS2 sortantes contribuent toutes deux à cette valeur)	50 Mo par seconde	Non

Quotas pour le traitement des secrets

AWS Transfer Family passe des appels au AWS Secrets Manager nom des clients AS2 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 compte Compte AWS.

Pour `Secrets ManagerGetSecretValue`, le quota applicable est le taux combiné de demandes d'`GetSecretValue` API `DescribeSecret` et le taux, comme décrit dans la section [AWS Secrets Manager Quotas](#).

Secrets Manager **GetSecretValue**

Nom	Value	Description
Taux combiné de demandes d' <code>GetSecretValue</code> API <code>DescribeSecret</code> et de demandes d'API	Chaque Région prise en charge : 10 000 par seconde	Le nombre maximum de transactions par seconde pour <code>DescribeSecret</code> les opérations <code>GetSecretValue</code> d'API combinées.

Pour AWS KMS, les quotas suivants s'appliquent à Decrypt. Pour plus de détails, voir [Quotas de demande pour chaque opération AWS KMS d'API](#)

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 du type de AWS KMS clé utilisé dans la demande. Région AWS 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

- Server-side Le protocole TCP keep-alive 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 en-têtes AS2 valides.
- [Le serveur qui reçoit les messages de AWS Transfer Family for AS2 doit prendre en charge l'attribut de protection de l'algorithme CMS \(Cryptographic Message Syntax\) pour valider les signatures des messages, tel que défini dans la RFC 6211.](#) Cet attribut n'est pas pris en charge dans certains anciens produits IBM Sterling.
- Les identifiants de message dupliqués donnent lieu à un message processed/Warning: document dupliqué.
- La longueur de clé pour les certificats AS2 doit être d'au moins 2 048 bits et d'au plus 4 096 bits.
- Lorsque vous envoyez des messages AS2 ou des mDNS asynchrones au point de terminaison HTTPS d'un partenaire commercial, les messages ou mDNS doivent utiliser un certificat SSL valide signé par une autorité de certification (CA) reconnue publiquement. Self-signed les certificats sont actuellement pris en charge uniquement pour les transferts sortants.
- 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 serveurs](#)).
- Les pièces jointes multiples et les messages d'échange de certificats (CEM) de la version 1.2 d'AS2 ne sont actuellement pas pris en charge.
- L'authentification de base est actuellement prise en charge uniquement pour les messages sortants.
- Vous pouvez associer un flux de traitement de fichiers à un serveur Transfer Family qui utilise le protocole AS2. Toutefois, les messages AS2 n'exécutent pas les flux de travail attachés au serveur.

Caractéristiques et capacités de l'AS2

Les tableaux suivants répertorient les fonctionnalités et capacités disponibles pour les ressources Transfer Family qui utilisent AS2.

Caractéristiques de l'AS2

Transfer Family propose les fonctionnalités suivantes pour AS2.

Fonctionnalité	Soutenu par AWS Transfer Family
Certification Drummond	Oui
AWS CloudFormation soutien	Oui
CloudWatchMétriques Amazon	Oui
SHA-2 algorithmes cryptographiques	Oui
Support pour Amazon S3	Oui
Prise en charge d'Amazon EFS	Non
Messages planifiés	Oui ¹
AWS Transfer Family Flux de travail gérés	Non
Messagerie d'échange de certificats (CEM)	Non
TLS mutuel (mTLS)	Non
Support pour les certificats auto-signés	Oui

1. Messages planifiés sortants disponibles via les [AWS Lambda fonctions de planification à l'aide d'Amazon EventBridge](#)

Capacités d'envoi et de réception AS2

Le tableau suivant fournit une liste des fonctionnalités d'envoi et de réception AWS Transfer Family AS2.

Capacité	Entrant : réception avec le serveur	Sortant : envoi avec connecteur
Transport crypté TLS (HTTPS)	Oui ¹	Oui

Capacité	Entrant : réception avec le serveur	Sortant : envoi avec connecteur
Non-TLS Transport (HTTP)	Oui	Oui ²
MDN synchrone	Oui	Oui
Compression des messages	Oui	Oui
MDN asynchrone	Oui	Oui
Adresse IP statique	Oui	Oui
Apportez votre propre adresse IP	Oui	Non
Pièces jointes multiples	Non	Non
Authentification de base	Non	Oui
Redémarrage AS2	Non applicable	Non
Fiabilité AS2	Non	Non
Objet personnalisé par message	Non applicable	Non

1. Transport crypté TLS entrant disponible avec Network Load Balancer (NLB) ou Application Load Balancer (ALB)

2. Transport sortant non TLS disponible uniquement lorsque le chiffrement est activé

Gérer les certificats AS2

Cette rubrique explique comment importer et gérer des certificats AS2. L'importation de certificats est la première étape du processus AS2 pour Transfer Family.

1. Importer des certificats
2. [Création de profils AS2](#)
3. [Création d'un serveur AS2](#)

4. [Création d'un accord AS2](#)

5. [Configuration des connecteurs AS2](#)

Importer des certificats AS2

Le processus Transfer Family AS2 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 clé pour les certificats AS2 doit être d'au moins 2 048 bits et d'au plus 4 096 bits.

Les points suivants détaillent la manière dont les certificats AS2 sont utilisés au cours du processus.

- AS2 entrant
 - 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.
- AS2 sortant
 - 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.
 - Si vous utilisez le protocole HTTPS, vous pouvez importer un certificat TLS (Transport Layer Security) auto-signé.

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 2 : Importer des certificats en tant que ressources de certificats Transfer Family”](#).

Pour spécifier un AS2-enabled certificat

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 AS2 Trading Partners, sélectionnez Certificates.
3. Sélectionnez Importer un certificat.
4. Dans la section Configuration du certificat, pour 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 Utilisation du certificat, choisissez l'objectif de ce certificat. Il peut être utilisé pour le chiffrement, la signature ou les deux.

Conseil : Si vous choisissez Encryption and signing for the use, 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.

6. Dans la section Contenu du certificat, fournissez un certificat public d'un partenaire commercial ou les clés publiques et privées d'un certificat local.

Renseignez la section Contenu du certificat avec les informations appropriées.

- Si vous choisissez Self-signed un certificat, vous ne fournissez pas la chaîne de certificats.
 - Collez le texte du certificat et sa chaîne dans le champ Certificat et chaîne de certificats.
 - S'il s'agit d'un certificat local, collez sa clé privée.
7. Choisissez Importer le certificat pour terminer le processus et enregistrer les détails du certificat importé.

Note

Les certificats TLS ne peuvent être importés qu'en tant que certificats publics d'un partenaire. Si vous sélectionnez le certificat public d'un partenaire, puis que vous sélectionnez Transport Layer Security (TLS) pour l'utilisation, vous recevez un avertissement. En outre, les certificats

TLS doivent être auto-signés (c'est-à-dire que vous devez sélectionner Certificat autosigné pour importer un certificat TLS).

Rotation des certificats AS2

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 chiffrement (obligatoire). Vous pouvez spécifier un seul certificat pour les deux objectifs, si vous le souhaitez.

La rotation des certificats est le processus de remplacement d'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.

X.509 les certificats ont `Not Before` et `Not After` leurs dates. Toutefois, il est possible que ces paramètres ne fournissent pas un contrôle suffisant aux administrateurs. Transfer Family fournit `Active Date` des `Inactive Date` paramètres permettant de contrôler quel certificat est utilisé pour les charges utiles sortantes et lequel est accepté pour les charges utiles entrantes.

Surveillance de l'expiration des certificats

Transfer Family publie une CloudWatch métrique Amazon `DaysUntilExpiry` après avoir importé un certificat. La métrique émet le nombre de jours entre la date actuelle et la date spécifiée `InactiveDate` sur le certificat. La métrique se trouve sous l'espace de `Transfer AWS` noms dans le tableau de bord des CloudWatch métriques.

Cette métrique comportera toujours une dimension métrique pour `CertificatId` et inclura éventuellement une dimension de description si le client l'indique sur le certificat. Pour plus d'informations sur les dimensions CloudWatch métriques, consultez la section [Dimension](#) dans la référence de l'CloudWatch API.

Note

L'importation d'un certificat peut prendre jusqu'à une journée complète pour que Transfer Family émette cette métrique sur le compte client.

Vous pouvez utiliser cette métrique pour créer des CloudWatch alarmes qui vous avertissent lorsque les certificats approchent de l'expiration.

La sélection des certificats sortants utilise la valeur maximale antérieure à la date du transfert en tant qu'`Inactive Date`. Les processus entrants acceptent les certificats compris entre `Active Date` et `Inactive Date`. `Not Before` et `Not After`

Exemple de rotation de certificats

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 profils AS2

Cette rubrique explique comment créer des profils à utiliser dans le processus AS2. Un profil local définit l'organisation ou le « groupe » local (AS2-enabled Transfer Family server). De même, un profil de partenaire définit l'organisation partenaire distante, externe à Transfer Family.

1. [Importer des certificats AS2](#)
2. Création de profils AS2
3. [Création d'un serveur AS2](#)
4. [Création d'un accord AS2](#)
5. [Configuration des connecteurs AS2](#)

Utilisez cette procédure pour créer des profils locaux et partenaires. Cette procédure explique comment créer des profils AS2 à l'aide de la console Transfer Family. Si vous souhaitez utiliser le à la AWS CLI place, consultez [the section called “Étape 3 : Créez des profils pour vous et votre partenaire commercial”](#).

Pour créer un profil AS2

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 AS2 Trading Partners, choisissez Profiles, puis Create profile.
3. Dans la section Configuration du profil, entrez l'ID AS2 du profil. Cette valeur est utilisée pour les en-têtes HTTP spécifiques au protocole AS2 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.

Conseil : 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 [Importer des certificats AS2](#).

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.

Création d'un serveur AS2

Cette rubrique fournit des instructions pour créer un serveur AS2-enabled Transfer Family, à l'aide de la console ou d'un CloudFormation modèle. Pour un exemple de configuration AS2 de bout en bout, voir. [Configuration d'une configuration AS2](#) Après avoir créé un serveur AS2, vous pouvez ajouter un accord au serveur.

1. [Importer des certificats AS2](#)
2. [Création de profils AS2](#)
3. Création d'un serveur AS2
4. [Création d'un accord AS2](#)
5. [Configuration des connecteurs AS2](#)

Rubriques

- [Création d'un serveur AS2 à l'aide de la console Transfer Family](#)
- [Utilisez un modèle pour créer un stack Transfer Family AS2 de démonstration](#)
- [Création d'un accord AS2](#)

Création d'un serveur AS2 à l'aide de la console Transfer Family

Cette procédure explique comment créer un AS2-enabled serveur à l'aide de la console Transfer Family. Si vous souhaitez utiliser le à la AWS CLI place, consultez [the section called “Étape 4 : Création d'un serveur Transfer Family utilisant le protocole AS2”](#).

 Note

Vous pouvez associer un flux de traitement de fichiers à un serveur Transfer Family qui utilise le protocole AS2. Toutefois, les messages AS2 n'exécutent pas les flux de travail attachés au serveur.

Pour créer un AS2-enabled 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 Create server.
3. Sur la page Choisir des protocoles, sélectionnez AS2 (Déclaration d'applicabilité 2), puis cliquez sur Suivant.
4. Sur la page Choisir un fournisseur d'identité, sélectionnez Suivant.

 Note

Pour AS2, vous ne pouvez pas choisir de fournisseur d'identité car l'authentification de base n'est pas prise en charge par le protocole AS2. Au lieu de cela, vous contrôlez l'accès par le biais de groupes de sécurité du cloud privé virtuel (VPC).

5. 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 VPC-hosted terminal, 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 protocole AS2. Pour rendre votre point de terminaison VPC 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 VPC et vos VPC-connected environnements, tels qu'un centre de données sur site ou un VPN. Direct Connect
- Accès à Internet : choisissez cette option pour fournir un accès via Internet et depuis votre VPC et vos VPC-connected environnements, tels qu'un centre de données sur site ou un VPN. Direct Connect

Si vous choisissez Internet Facing, indiquez vos adresses IP élastiques lorsque vous y êtes invité.

- c. Pour le VPC, choisissez un VPC existant ou choisissez Create VPC pour créer un nouveau VPC.
- d. Pour FIPS Enabled, laissez la case FIPS Enabled Endpoint cochée.

 Note

FIPS-enabled les points de terminaison ne sont pas pris en charge par le protocole AS2.

- 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 plus de l'AS2, tous les paramètres de détail supplémentaires s'appliquent. Toutefois, pour le protocole AS2, 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 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.

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 stack Transfer Family AS2 de démonstration

Nous fournissons un CloudFormation modèle autonome pour créer rapidement un serveur AS2-enabled Transfer Family. Le modèle configure le serveur avec un point de terminaison Amazon VPC public, des certificats, des profils locaux et partenaires, un accord et un connecteur.

Le modèle de serveur AS2 de base crée les ressources suivantes :

- Un serveur AS2-enabled Transfer Family avec un point de terminaison VPC
- Profils AS2 locaux et partenaires avec certificats
- Un accord entre les profils
- Un compartiment Amazon S3 pour le stockage de fichiers
- Rôles et politiques IAM requis
- CloudWatch configuration de journalisation

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 serveur AS2 de production, vous pouvez utiliser Secrets Manager pour gérer et faire régulièrement pivoter 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 code YAML 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 serveur AS2-enabled Transfer Family à partir d'un CloudFormation modèle

1. Ouvrez la 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, choisissez Choisir un modèle existant.
5. Copiez ce lien, le [modèle de démonstration AS2](#), et collez-le dans le champ URL d'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'ID AS2 local et l'ID AS2 du partenaire, ou acceptez les valeurs par défaut, et, `local` respectivement. `partner`
 - Sous Réseau, entrez une valeur pour l'adresse IP CIDR d'entrée du groupe de sécurité, ou acceptez la valeur par défaut. `0.0.0.0/0`

 Note

Cette valeur, au format CIDR, indique quelles adresses IP sont autorisées pour le trafic entrant sur le serveur AS2. 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-amzn-s3-demo-bucket`.

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 cela CloudFormation peut créer des ressources Gestion des identités et des accès AWS (IAM).

Une fois la pile créée, vous pouvez envoyer un message de test AS2 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, accédez à l'onglet Sorties de votre pile et copiez le `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 amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

 Note

Votre version de cette commande contient les valeurs réelles des *TransferConnectorId* ressources *amzn-s3-demo-bucket* 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 amzn-s3-demo-bucket --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 /amzn-s3-demo-bucket/test.txt
```

Après avoir exécuté la commande, vous pouvez accéder à votre compartiment Amazon S3 (*amzn-s3-demo-bucket*) et en consulter le contenu. Si la commande aboutit, vous devriez voir apparaître les objets suivants dans votre compartiment :

- *processed/*— Ce dossier contient un fichier JSON qui décrit le fichier transféré et la réponse MDN.
- *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'identifiant AS2 du partenaire), qui contient lui-même *failed/processed/*, et des *processing/* dossiers. Le */server-id/from-partner/processed/* dossier contient une copie du fichier texte transféré, ainsi que les fichiers JSON et MDN correspondants.
- *test.txt*— Cet objet est le fichier (vide) qui a été transféré.

Création d'un accord AS2

Les accords sont associés aux serveurs Transfer Family. Ils fournissent des informations détaillées aux partenaires commerciaux qui utilisent le protocole AS2 pour échanger des messages ou des fichiers à l'aide de Transfer Family, pour les transferts entrants, c'est-à-dire l'envoi de fichiers AS2 depuis une source externe appartenant au partenaire vers un serveur Transfer Family.

Cette procédure explique comment créer des accords AS2 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 utilisant le protocole AS2.

Sinon, tant que vous disposez d'au moins un serveur Transfer Family qui utilise le protocole AS2, sélectionnez Agreements pour recevoir des messages dans le menu AS2 Trading Partners. Ensuite, dans l'écran Créer un accord, sélectionnez le serveur AS2 auquel vous souhaitez associer cet accord.

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 de la communication, choisissez un profil local et un profil partenaire. Choisissez également d'appliquer ou non la signature des messages.
 - Par défaut, Enforce la signature des messages est activée, ce qui signifie que Transfer Family rejette les messages non signés de votre partenaire commercial concernant cet accord.
 - Désactivez ce paramètre pour autoriser Transfer Family à accepter les messages non signés de votre partenaire commercial dans le cadre de cet accord.
 - c. Dans la section Configuration du répertoire de la boîte de réception, fournissez les informations suivantes.
 - Déterminez s'il faut sélectionner Spécifier des répertoires distincts pour stocker vos messages AS2, vos fichiers MDN et vos fichiers d'état JSON.
 - Si vous sélectionnez cette option, vous spécifiez des emplacements distincts pour les fichiers de charge utile, les fichiers ayant échoué, les fichiers MDN, les fichiers d'état et les fichiers temporaires.
 - Si vous désactivez cette option, tous les fichiers AS2 sont placés dans l'emplacement que vous spécifiez pour votre répertoire de base.
 - Pour le compartiment S3, choisissez un compartiment Amazon S3.

- Dans Préfixe, vous pouvez saisir un préfixe (dossier) à utiliser pour stocker les fichiers dans le compartiment.

Par exemple, si vous entrez **amzn-s3-demo-bucket** votre bucket et **incoming** votre préfixe, vos fichiers AS2 sont enregistrés dans le **/amzn-s3-demo-bucket/incoming** dossier.

- Pour le rôle AWS IAM, choisissez un rôle qui peut accéder au compartiment que vous avez spécifié.
 - Pour Conserver le nom de fichier, indiquez si vous souhaitez conserver les noms de fichiers d'origine pour les charges utiles des messages AS2 entrants.
 - Si vous sélectionnez ce paramètre, le nom de fichier fourni par votre partenaire commercial est conservé lors de son enregistrement dans Amazon S3.
 - Si vous désactivez ce paramètre, lorsque Transfer Family enregistre le fichier, le nom du fichier est ajusté, comme décrit dans [Noms et emplacements des fichiers](#).
- 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.

Configuration des connecteurs AS2

L'objectif d'un connecteur est d'établir une relation entre les partenaires commerciaux pour les transferts sortants, en envoyant des fichiers AS2 d'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. Chaque serveur AS2 se voit attribuer trois adresses IP statiques. Les connecteurs AS2 utilisent ces adresses IP pour envoyer des mDNS asynchrones à vos partenaires commerciaux via AS2.

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 message AS2 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.

1. [Importer des certificats AS2](#)
2. [Création de profils AS2](#)
3. [Création d'un serveur AS2](#)
4. [Création d'un accord AS2](#)
5. Création d'un connecteur AS2

Création d'un connecteur AS2

Cette procédure explique comment créer des connecteurs AS2 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 connecteur AS2

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 Connecteurs pour envoyer des messages, dans le menu AS2 Trading Partners, puis sélectionnez Créer un connecteur AS2.
3. Dans la section Configuration du connecteur, spécifiez les informations suivantes :
 - URL — Entrez l'URL pour les connexions sortantes.
 - Mode d'adressage IP — Choisissez IPv4 uniquement (par défaut) pour utiliser exclusivement les adresses IPv4 ou Dual-stack pour prendre en charge à la fois IPv6 et IPv4. En mode double pile, le connecteur préfère IPv6 lorsque la résolution DNS renvoie des résultats IPv6, et utilise IPv4 lorsque seuls les résultats DNS IPv4 sont renvoyés.
 - Rôle d'accès : choisissez le nom de ressource Amazon (ARN) du rôle Gestion des identités et des accès AWS (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](#).

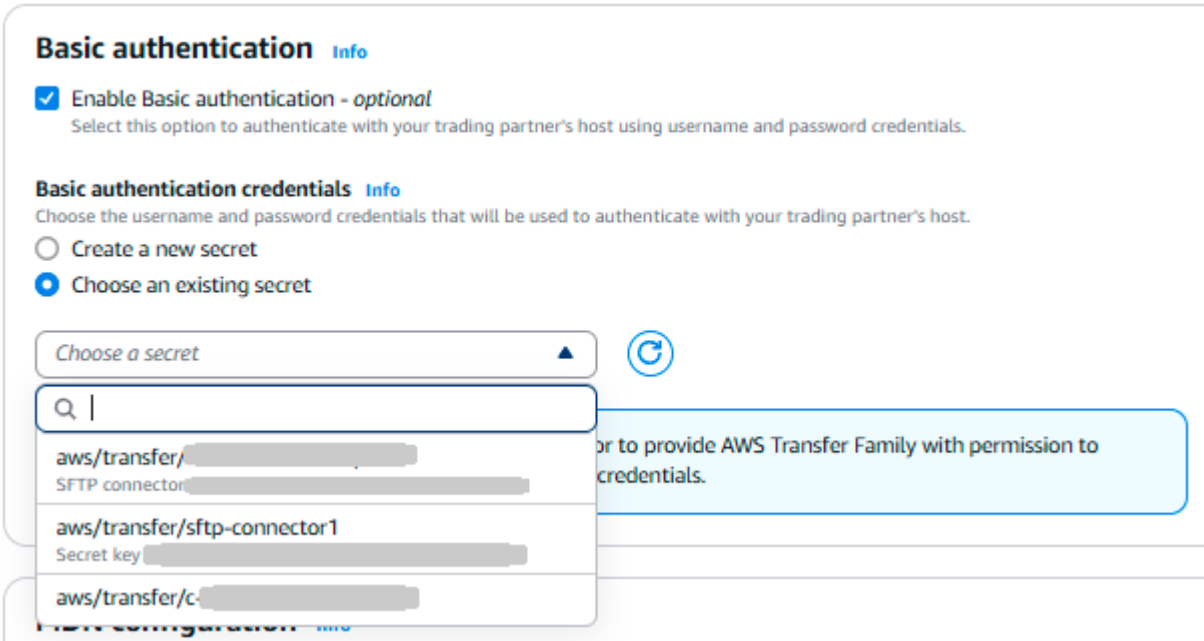
- Rôle de journalisation (facultatif) — Choisissez le rôle IAM que le connecteur doit utiliser pour transférer des événements vers vos CloudWatch journaux.
4. Dans la section de configuration AS2, choisissez les profils local et partenaire, les algorithmes de chiffrement et de signature, et indiquez si vous souhaitez compresser les informations transférées. Notez ce qui suit :
- Le Content-Type paramètre Preserve S3 est activé par défaut.

Lorsque Content-Type cette option est définie, Transfer Family utilise l'Amazon S3 associé aux objets dans S3 au lieu de faire mapper le type de contenu en fonction de l'extension de fichier. Désactivez ce paramètre si vous souhaitez que le service mappe le type de contenu de vos messages AS2 en fonction de l'extension de fichier, plutôt que d'utiliser le type de contenu de l'objet S3.

- 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'en-tête `subject` HTTP dans les messages AS2 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 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.

- 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 connecteurs AS2](#).



6. Dans la section de configuration MDN, spécifiez les informations suivantes :
- Demander un MDN — Vous avez la possibilité de demander à votre partenaire commercial de vous envoyer un MDN une fois qu'il aura bien reçu votre message via AS2.

MDN signé — Vous avez la possibilité d'exiger que le MDN soit signé. Cette option n'est disponible que si vous avez sélectionné Request MDN.
7. Après avoir confirmé tous vos paramètres, choisissez Create AS2 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 du connecteur AS2](#).

Algorithmes du connecteur AS2

Lorsque vous créez un connecteur AS2, les algorithmes de sécurité suivants sont attachés au connecteur.

Type	Algorithm
Chiffre TLS	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

Type	Algorithm
	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

Authentification de base pour les connecteurs AS2

Lorsque vous créez ou mettez à jour un serveur Transfer Family qui utilise le protocole AS2, 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 le protocole 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.

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 connecteurs AS2](#).

Activer l'authentification de base pour les connecteurs AS2

Lorsque vous activez l'authentification de base pour les connecteurs AS2, 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

[i](#) Update the [access role associated with your connector](#) [🔗](#) to provide AWS Transfer Family with permission to read the secret containing your Basic authentication credentials.

[i](#) 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 d'y trouver 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](#).

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

Choose a secret

aws/transfer/...
SFTP connector...

aws/transfer/sftp-connector1
Secret key ...

aws/transfer/c...

You must provide AWS Transfer Family with permission to use the secret.

Créez un secret dans AWS Secrets Manager

La procédure suivante explique comment créer un secret approprié à utiliser avec votre connecteur AS2.

Note

L'authentification de base n'est disponible que si vous utilisez le protocole HTTPS.

Pour stocker les informations d'identification de l'utilisateur dans Secrets Manager pour l'authentification AS2 Basic

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 panneau 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 des Key/value paires, choisissez l'Key/valueonglet.
 - 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 des Key/value paires, sélectionnez l'onglet Key/value.

Choisissez Ajouter une ligne, puis dans la section des Key/value paires, sélectionnez l'onglet Key/value.

- 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 des Key/value paires, sélectionnez l'onglet Key/value.
- Clé — Entrée **PrivateKey**.
 - valeur — Entrez une clé privée pour l'utilisateur. Cette valeur doit être stockée au format OpenSSH 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 connecteurs AS2](#)). À l'étape où vous activez l'authentification de base, choisissez le secret dans la liste déroulante des secrets disponibles.

Afficher les détails du connecteur AS2

Vous trouverez la liste des détails et des propriétés d'un AWS Transfer Family connecteur AS2 dans la AWS Transfer Family console. Les propriétés d'un connecteur AS2 incluent son URL, ses rôles, ses profils, ses mDNS, ses balises et ses mesures 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 connecteur AS2 sur la page de détails du connecteur en choisissant Modifier.

C-

Delete

Connector configuration

Info

Edit

Name

my-as2-connector

Access role

URL

<https://www.example.com>

Logging role

[AWSTransferLoggingAccess](#)

Communication settings

Info

AS2-From header

AS2-To header

AS2 configuration

Info

Edit

Local profile

Compression

Enabled

Encryption algorithm

AES128_CBC

Partner profile

Message Subject

View

Signing algorithm

SHA384

Preserve S3 Content-Type

Enabled

MDN configuration

Info

Edit

Request MDN

Enabled

Signed MDN

Default to message signing algorithm: SHA384

Synchronization

Enabled

Basic authentication [Info](#)[Edit](#)**Basic authentication**
✔ Enabled**Secret**
aws/transfer/c- [redacted] [Copy](#)**Egress IP details** [Info](#)

Service managed static IP addresses of this connector

[Copy](#) 23.23.130.9[Copy](#) 44.196.109.11[Copy](#) 3.219.16.7**Tags (1)**[Manage tags](#)

Use tags to organize, search, and filter your Connectors. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Connector.

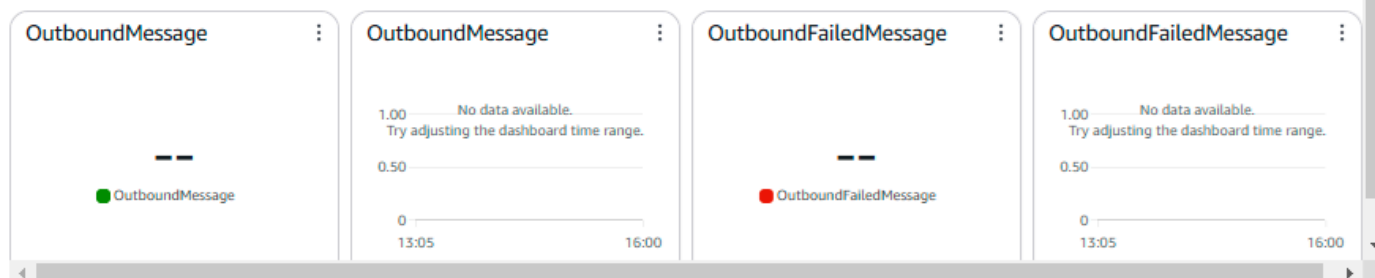
< 1 >

Key	Value
Name	my-as2-connector

AS2 Monitoring

3h 1d 1w

UTC timezone

**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](#) la référence de l'API.

Envoyer et recevoir des messages AS2

Cette section décrit les processus d'envoi et de réception de messages AS2. Il fournit également des détails sur les noms de fichiers et les emplacements associés aux messages AS2.

Le tableau suivant répertorie les algorithmes de chiffrement disponibles pour les messages AS2 et indique dans quels cas vous pouvez les utiliser.

Algorithme de chiffrement	HTTP	HTTPS	Remarques
AES128_CBC	Oui	Oui	
AES192_CBC	Oui	Oui	
AES256_CBC	Oui	Oui	
DES_EDE3_CBC	Oui	Oui	N'utilisez cet algorithme que si vous devez prendre en charge un ancien client qui en a besoin, car il s'agit d'un algorithme de chiffrement faible.
NONE	Non	Oui	Si vous envoyez des messages à un serveur Transfer Family, vous ne pouvez sélectionner que NONE si vous utilisez un Application Load Balancer (ALB).

Rubriques

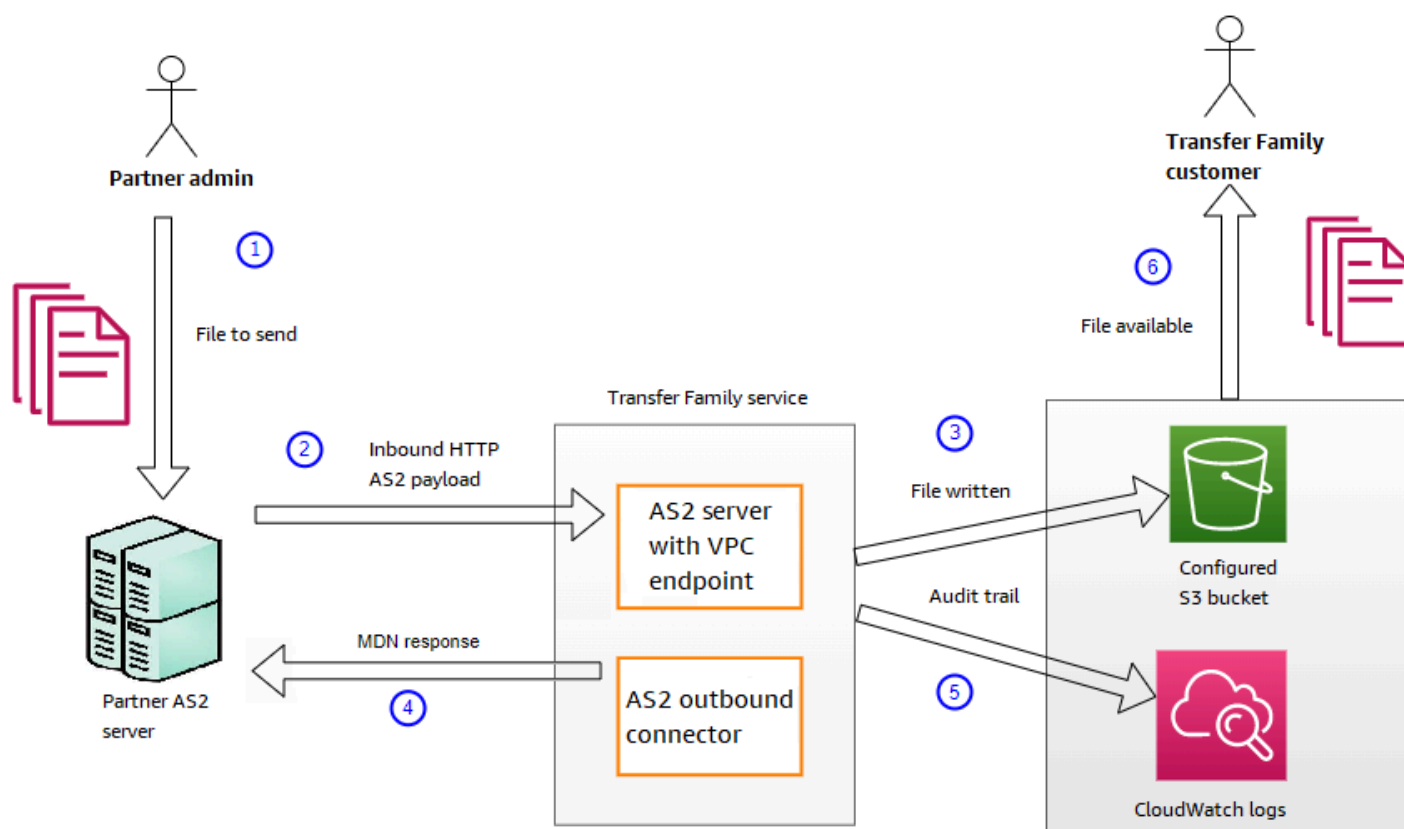
- [Processus de réception des messages AS2](#)
- [Envoi et réception de messages AS2 via HTTPS](#)

- [Transfert de fichiers à l'aide d'un connecteur AS2](#)
- [Noms et emplacements des fichiers](#)
- [Codes d'état](#)
- [Exemples de fichiers JSON](#)

Processus de réception des messages AS2

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 processus administratif ou automatisé lance un transfert de fichiers AS2 sur le serveur AS2 distant du partenaire.
2. Le serveur AS2 distant du partenaire signe et chiffre le contenu du fichier, puis envoie une requête HTTP POST à un point de terminaison entrant AS2 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 réponse MDN signée est renvoyée soit en ligne avec la réponse HTTP, soit de manière asynchrone via une requête HTTP POST distincte 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 messages AS2 via HTTPS

Cette section décrit comment configurer un serveur Transfer Family qui utilise le protocole AS2 pour envoyer et recevoir des messages via HTTPS.

Rubriques

- [Envoyer des messages AS2 via HTTPS](#)
- [Recevoir des messages AS2 via HTTPS](#)

Envoyer des messages AS2 via HTTPS

Pour envoyer des messages AS2 via HTTPS, créez un connecteur contenant les informations suivantes :

- Pour l'URL, spécifiez une URL HTTPS
- Pour l'algorithme de chiffrement, sélectionnez l'un des algorithmes disponibles.

 Note

Pour envoyer des messages à un serveur Transfer Family sans utiliser le chiffrement (c'est-à-dire si vous sélectionnez l'algorithme NONE de chiffrement), vous devez utiliser un Application Load Balancer (ALB).

- Fournissez les valeurs restantes pour le connecteur, comme décrit dans [Configuration des connecteurs AS2](#).

Recevoir des messages AS2 via HTTPS

AWS Transfer Family Les serveurs AS2 ne fournissent actuellement que le transport HTTP via le port 5080. Cependant, vous pouvez mettre fin au protocole TLS sur un réseau ou un équilibreur de charge d'application situé devant le point de terminaison VPC de votre serveur Transfer Family en utilisant un port et un certificat de votre choix. Avec cette approche, vous pouvez faire en sorte que les messages AS2 entrants utilisent le protocole HTTPS.

Conditions préalables

- Le VPC doit se trouver dans le même emplacement Région AWS que votre serveur Transfer Family.
- Les sous-réseaux de votre 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.

Vous pouvez configurer un Network Load Balance (NLB) ou un Application Load Balancer (ALB). Le tableau suivant répertorie les avantages et les inconvénients de chaque approche.

Le tableau ci-dessous indique les différences entre les fonctionnalités lorsque vous utilisez un NLB par rapport à un ALB pour mettre fin au protocole TLS.

Fonctionnalité	Network Load Balancer (NLB)	Application Load Balancer (ALB)
Latence	Temps de latence réduit car il fonctionne au niveau de la couche réseau.	Latence plus élevée car il fonctionne au niveau de la couche application.
Prise en charge des adresses IP statiques	Peut associer des adresses IP élastiques qui peuvent être statiques.	Impossible d'associer des adresses IP élastiques : fournit un domaine dont les adresses IP sous-jacentes peuvent changer.
Routage avancé	Ne prend pas en charge le routage avancé.	Supporte le routage avancé. Peut injecter X-Forwarded-Proto l'en-tête requis pour AS2 sans cryptage. Cet en-tête est décrit X-Forwarded-Proto sur le site web developer.mozilla.org .
TLS/SSL résiliation	Supporte TLS/SSL la résiliation	Supporte TLS/SSL la résiliation
TLS mutuel (mTLS)	Transfer Family ne prend actuellement pas en charge l'utilisation d'un NLB pour les MTL	Support pour les MTL

Configure NLB

Cette procédure décrit comment configurer un Network Load Balancer (NLB) connecté à Internet dans votre VPC.

Pour créer un Network Load Balancer et définir le point de terminaison VPC 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 Schéma, choisissez Internet-facing.
 - Pour le type d'adresse IP, choisissez IPv4.
5. Dans la section Cartographie du réseau, entrez les informations suivantes :
 - Pour le 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 le même VPC que celui que vous utilisez avec les points de terminaison de votre serveur.
 - Pour l'adresse IPv4 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 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 SSL/TLS Certificat par défaut.
8. Choisissez Create load balancer pour créer votre NLB.

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 connexion TLS est interrompue au niveau du NLB. Par conséquent, l'adresse IP source reflétée dans vos groupes de CloudWatch journaux Transfer Family AS2 est l'adresse IP privée de la NLB, et non l'adresse IP externe de votre partenaire commercial.

Configure ALB

Cette procédure décrit comment configurer un Application Load Balancer (ALB) dans votre VPC.

Pour créer un Application Load Balancer et définir le point de terminaison VPC 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 Application Load Balancer, choisissez Create (Créer).
4. Dans la console ALB, créez un nouvel écouteur HTTP sur le port 443 (HTTPS).
5. (Facultatif) Si vous souhaitez configurer l'authentification mutuelle (MTL), configurez les paramètres de sécurité et un trust store.
 - a. Joignez votre SSL/TLS certificat à l'écouteur.
 - b. Sous Gestion des certificats clients, sélectionnez Authentification mutuelle (mTLS).
 - c. Choisissez Verify with Trust Store.
 - d. Sous Paramètres mTLS avancés, choisissez ou créez un trust store en téléchargeant vos certificats CA.
6. Créez un nouveau groupe cible et ajoutez les adresses IP privées des points de terminaison de votre serveur Transfer Family AS2 en tant que cibles sur le port 5080. Pour en savoir plus sur la création d'un nouveau groupe cible, consultez [Pour créer un groupe cible](#).
7. Configurez les contrôles de santé pour que le groupe cible utilise le protocole HTTP sur le port 5080.
8. Créez une nouvelle règle pour transférer le trafic HTTPS de l'écouteur vers le groupe cible.
9. Configurez l'écouteur pour qu'il utilise votre SSL/TLS certificat.

Après avoir configuré l'équilibreur de charge, les clients communiquent avec l'équilibreur de charge 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 le protocole, votre sélection dépend de l'utilisation d'un ALB ou d'un NLB.
 - Pour un Network Load Balancer (NLB), choisissez TCP
 - Pour un Application Load Balancer (ALB), choisissez HTTP
 - Pour Port, entrez **5080**.
 - Pour le type d'adresse IP, choisissez IPv4.
 - Pour VPC, choisissez le VPC que vous avez créé pour votre serveur Transfer Family AS2.
3. Dans la section Health checks, choisissez le protocole Health check.
 - Pour un ALB, choisissez HTTP
 - Pour un NLB, choisissez TCP
4. Choisissez Suivant.
5. Sur la page Enregistrer les cibles, entrez les informations suivantes :
 - Pour Network, vérifiez que le VPC que vous avez créé pour votre serveur Transfer Family AS2 est spécifié.
 - Pour l'adresse IPv4, entrez l'adresse IPv4 privée des points de terminaison de votre serveur Transfer Family AS2.

Si vous avez plusieurs points de terminaison pour votre serveur, choisissez Ajouter une adresse IPv4 pour ajouter une autre ligne permettant de saisir une autre adresse IPv4. 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 Examiner les cibles, passez en revue vos cibles IP.
 7. Choisissez Créer un groupe cible, puis revenez à la procédure précédente de création de votre NLB et entrez le nouveau groupe cible à l'endroit indiqué.

Tester l'accès au serveur à partir d'une adresse IP élastique

Connectez-vous au serveur via le port personnalisé à l'aide d'une adresse IP élastique ou du nom DNS 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 \(ACL réseau\)](#) pour les sous-réseaux configurés sur l'équilibreur de charge. Les autorisations ACL 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.

Transfert de fichiers à l'aide d'un connecteur AS2

Les connecteurs AS2 établissent une relation entre les partenaires commerciaux pour les transferts de messages AS2 d'un serveur Transfer Family vers une destination externe appartenant au partenaire.

Vous pouvez utiliser Transfer Family pour envoyer des messages AS2 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 "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-
bucket/myfile2.txt"
```

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

```
aws transfer list-connectors
```

La `list-connectors` commande renvoie les identifiants de connecteur, les URL et les noms de ressources Amazon (ARN) de vos connecteurs.

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 son URL, ses rôles, ses profils, ses notifications de disposition des messages (mDNS), ses balises et ses mesures de surveillance.

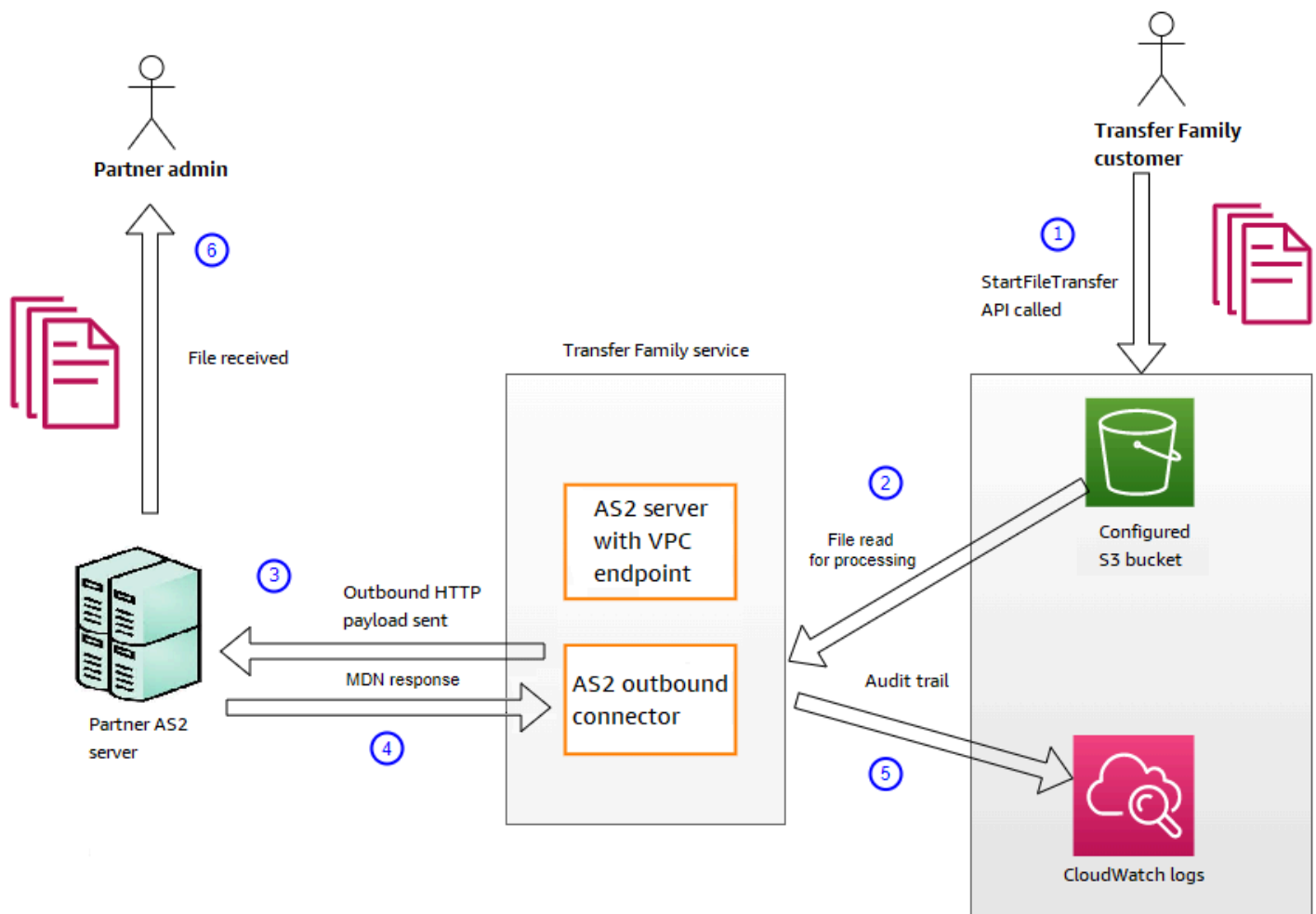
Vous pouvez vérifier que le partenaire a bien reçu les fichiers en consultant les fichiers JSON et MDN. Ces fichiers sont nommés conformément aux conventions décrites dans [Noms et emplacements des fichiers](#). Si vous avez configuré un rôle de journalisation lors de la création du connecteur, vous pouvez également vérifier l'état des messages AS2 dans vos CloudWatch journaux.

Pour consulter les détails du connecteur AS2, reportez-vous [Afficher les détails du connecteur AS2](#) à. Pour plus d'informations sur la création de connecteurs AS2, consultez [Configuration des connecteurs AS2](#).

Pour envoyer un message sortant AS2

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 l'opération `StartFileTransfer` API. Cette opération fait référence à une configuration de connecteur.
2. Transfer Family détecte une nouvelle demande de fichier et localise le fichier. Le fichier est compressé, signé et chiffré.
3. Un client HTTP de transfert exécute une requête HTTP POST pour transmettre la charge utile au serveur AS2 du partenaire.
4. Le processus renvoie la réponse MDN signée, en ligne avec la réponse HTTP (MDN synchrone ou asynchrone).
5. Au fur et à mesure que le fichier passe d'une étape de transmission à une autre, le processus fournit au client la réception de la réponse MDN et les détails du traitement.
6. Le serveur AS2 distant met le fichier déchiffré et vérifié à la disposition de l'administrateur partenaire.



Le traitement AS2 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 existantes AS2-enabled . Pour plus de détails sur les configurations prises en charge, consultez [Configurations AS2](#).

Noms et emplacements des fichiers

Cette section décrit les conventions de dénomination des fichiers pour les transferts AS2.

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, **/amzn-s3-demo-bucket/AS2-folder**.
- Si un fichier entrant est traité avec succès, le fichier (et le fichier JSON correspondant) est enregistré **/processed** dans le dossier. Par exemple, **/amzn-s3-demo-bucket/AS2-folder/processed**.

Le fichier JSON 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

- `failure-code`
- `transfer-size`
- Si un fichier entrant ne peut pas être traité correctement, le fichier (et le fichier JSON correspondant) est enregistré `/failed` dans le dossier. Par exemple, `/amzn-s3-demo-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 fichier JSON 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 MDN (Message Disposition Notice) 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'opération `StartFileTransfer` API (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'opération ou la `start-file-transfer` AWS CLI commande de l'`StartFileTransferAPI`. Par exemple :

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-bucket/AS2-folder/
file-to-send.txt
```

Si vous exécutez cette commande, les fichiers MDN et JSON sont enregistrés dans /amzn-s3-demo-bucket/AS2-folder/processed (pour les transferts réussis) ou /amzn-s3-demo-bucket/AS2-folder/failed (pour les transferts infructueux).

- Un fichier JSON est créé et enregistré sous le nom `original_filename.transferId.messageId.original_extension.json`.
- Un fichier MDN 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 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

Exemples de fichiers JSON

Cette section répertorie des exemples de fichiers JSON 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_0ID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_0ID",
  "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": "/amzn-s3-demo-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": "/amzn-s3-demo-bucket-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"
}

```

Personnalisation des en-têtes HTTP pour les messages AS2

Lorsque vous envoyez des messages AS2 à des partenaires commerciaux, vous devrez peut-être personnaliser les en-têtes HTTP pour répondre à des exigences spécifiques ou améliorer la compatibilité avec la configuration du serveur AS2 de votre partenaire. Ce CloudFormation modèle crée une infrastructure permettant d'activer des en-têtes HTTP personnalisés pour les messages AS2 envoyés. AWS Transfer Family II met en place une fonction Amazon API Gateway et Lambda agissant comme un proxy, permettant la modification dynamique des en-têtes requis par les serveurs AS2 des partenaires commerciaux.

Utilisez ce modèle pour effectuer les opérations suivantes :

- Ajouter des en-têtes HTTP personnalisés aux messages AS2 sortants
- Remplacer les valeurs d'en-tête par défaut par des valeurs personnalisées

 Important

Soyez prudent lorsque vous remplacez les valeurs d'en-tête par défaut, car cela peut entraîner des échecs d'envoi : certains en-têtes AS2 sont nécessaires.

- Garantir la compatibilité avec les partenaires commerciaux qui ont des exigences spécifiques en matière d'en-têtes

Présentation du modèle

Le modèle crée les principaux composants suivants :

- Une fonction Lambda qui traite et transmet les messages AS2
- Un Amazon API Gateway pour exposer la fonction Lambda
- Rôles et autorisations IAM pour la fonction Lambda
- Ressources conditionnelles pour le support HTTPS

Le fichier modèle est disponible ici : [Modèle d'en-têtes HTTP dynamiques](#).

Comment ça marche

1. Amazon API Gateway reçoit les messages AS2 entrants provenant de AWS Transfer Family.
2. La demande est transmise à la fonction Lambda.
3. La fonction Lambda traite la demande en ajoutant ou en modifiant des en-têtes selon les besoins.
4. La demande modifiée est ensuite transmise au serveur AS2 du partenaire.
5. La réponse du serveur du partenaire est renvoyée via Lambda et Amazon API Gateway à AWS Transfer Family

Fonctionnalités principales

- Modification dynamique de l'en-tête : permet de personnaliser l'en-tête du sujet et d'ajouter d'autres en-têtes requis.
- Support de protocole : fonctionne avec les protocoles HTTP et HTTPS.
- Configuration flexible : permet de spécifier l'hôte, le port et le chemin du partenaire.

Détails de l'implémentation

Le modèle implémente les composants clés suivants :

Fonction Lambda

Le cœur de la solution est une fonction Node.js Lambda qui :

- Reçoit les demandes de l'Amazon API Gateway
- Modifie les en-têtes en fonction de la configuration et des données de demande entrantes
- Transmet la demande modifiée au serveur AS2 du partenaire
- Gère les protocoles HTTP et HTTPS
- Inclut la gestion des erreurs et la journalisation

Amazon API Gateway

Une API HTTP est configurée pour :

- Recevoir les messages AS2 entrants
- Acheminer les demandes vers la fonction Lambda
- Retourner les réponses à AWS Transfer Family

Paramètres du modèle

Entrez les informations relatives aux paramètres du modèle comme suit. Notez que tous ces paramètres sont des chaînes de caractères.

- **Environment**: ce paramètre est utilisé pour nommer les ressources créées par le modèle : qu'elles soient destinées à un environnement de développement ou de production. Les valeurs valides sont dev et prod.
- **PartnerHost**: adresse IP ou nom d'hôte du serveur partenaire AS2.
- **PartnerPort**: le numéro de port du serveur partenaire AS2. Si ce n'est pas spécifié, la valeur par défaut est 80 pour HTTP et 443 pour HTTPS.
- **PartnerPath**: le chemin d'accès au point de terminaison AS2 sur le serveur partenaire
- **ProtocolType**: le protocole à utiliser pour la communication AS2 : les valeurs valides sont HTTP et HTTPS.

Ressources conditionnelles

Pour la prise en charge du protocole HTTPS, le modèle crée de manière conditionnelle :

- Une couche Lambda pour les certificats CA
- HTTPS-specific configuration dans la fonction Lambda

Déploiement et utilisation

Pour personnaliser les en-têtes HTTP AS2 à l'aide d'un modèle CloudFormation

1. Ouvrez la 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, choisissez Choisir un modèle existant.
5. Copiez ce lien, [modèle d'en-têtes HTTP dynamique](#), et collez-le dans le champ URL d'Amazon S3.
6. Choisissez Suivant.
7. Renseignez les détails des paramètres avec vos informations. Elles sont détaillées dans [Paramètres du modèle](#).
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 cela CloudFormation peut créer des ressources Gestion des identités et des accès AWS (IAM).

Après avoir déployé cette CloudFormation pile :

1. Notez l'URL du point de terminaison Amazon API Gateway fournie dans les sorties de la pile.
2. Mettez à jour votre AWS Transfer Family connecteur existant pour utiliser ce nouveau point de terminaison Amazon API Gateway.
3. La solution gère désormais les messages AS2, en ajoutant ou en modifiant les en-têtes tels que configurés.

 Warning

Modifiez uniquement l'en-tête du sujet ou ajoutez des en-têtes que votre partenaire attend explicitement. La modification d'autres en-têtes peut entraîner des échecs de transfert.

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 les AWS Transfer Family serveurs](#)

Métriques AS2

Métrique	Description
InboundMessage	Nombre total de messages AS2 reçus avec succès d'un partenaire commercial. Unités : nombre Période : 5 minutes

Métrique	Description
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. 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

Métrique	Description
DaysUntilExpiry	Le nombre de jours avant l'expiration d'un certificat est déterminé par le paramètre <code>InactiveDate</code> indiqué sur le certificat lors de l'importation. Unités : nombre Dimensions : <code>CertificateId</code> , <code>Description</code> (si fourni) Période : 1 jour Pour de plus amples informations, veuillez consulter Rotation des certificats AS2.

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 déchiffrement ont toutes deux ce statut.	Non
MDN_TRANSMIT	Le traitement des messages envoie une réponse MDN.	Non

Code	Description	Le traitement est terminé ?
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> - Impossible d'obtenir les informations d'identification avec ErrorCode : <i>error-code</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 nom du compartiment Amazon S3 ou contient des caractères non valides. Cela se produit également si Transfer Family

Code	Erreur	Description et résolution
		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 des autorisations nécessaires pour la clé AWS Key

Code	Erreur	Description et résolution
		Management Service (AWS KMS). 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 le message <i>message-ID</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 MIME part 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	Décryptage de la charge utile SMIME demandé à l'aide d'un algorithme non pris en charge avec l'ID : <i>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 fichier <i>file-name</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</i> a renvoyé le statut 400 pour un message avec ID= <i>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 connecteurs AS2. 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	Non applicable	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	Non applicable	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	Non applicable	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	Non applicable	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 le and/or chiffrement des signatures sur le connecteur pour répondre aux attentes du partenaire commercial.
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	Non applicable	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 répertoire <i>file-path</i> . Le chemin parent est introuvable.	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 fichier <i>file-path</i> est introuvable.	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	<i>server-ID</i> Le serveur 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'hôte <i>hostname</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 le message AS2 <i>message-ID</i> 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 pu être 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.

Surveillance de l'expiration des certificats

AWS Transfer Family surveille automatiquement les dates d'expiration des certificats AS2 et publie une CloudWatch métrique Amazon pour vous aider à savoir quand les certificats approchent de leur expiration. Cela vous permet de gérer de manière proactive les renouvellements de certificats et d'éviter les interruptions de service.

DaysUntilExpiry métrique

Lorsque vous importez un certificat pour une utilisation AS2, Transfer Family crée automatiquement une CloudWatch métrique appelée `DaysUntilExpiry`. Cette métrique permet de suivre le nombre de jours restant avant l'expiration du certificat en fonction du délai `InactiveDate` que vous avez spécifié lors de l'importation du certificat.

Détails du système métrique :

- Nom de la métrique : `DaysUntilExpiry`
- Espace de noms : `AWS/Transfer`
- Dimensions : `CertificateId` (toujours présentes), `Description` (si fournies lors de l'importation du certificat)
- Unités : Nombre (jours)
- Fréquence : Publié tous les jours

Important

L'importation d'un certificat peut prendre jusqu'à une journée pour que Transfer Family émette cette métrique sur votre compte.

La valeur de la métrique diminue d'un par jour lorsque le certificat approche de sa date d'inactivité. Par exemple, si un certificat doit expirer dans un délai de 30 jours, la métrique indiquera 30, puis 29 le jour suivant, etc.

Bonnes pratiques en matière de surveillance des certificats

Suivez les meilleures pratiques suivantes lors de la configuration de la surveillance de l'expiration des certificats :

- Définissez plusieurs seuils d'alerte : créez des alarmes pour différentes périodes (par exemple, 30 jours, 14 jours et 7 jours avant l'expiration) afin de prévoir un délai suffisant pour le renouvellement du certificat.
- Utilisez les statistiques appropriées : utilisez les `Maximum` statistiques lorsque vous créez des alarmes pour vous assurer de capturer la valeur de mesure la plus récente.
- Configurez les actions d'alarme appropriées : configurez des notifications pour avertir les membres de l'équipe concernés qui peuvent renouveler les certificats.
- Testez vos alertes : testez régulièrement votre système de notification pour vous assurer que les alertes sont correctement envoyées.
- Documentez votre processus : conservez la documentation concernant le processus de renouvellement de vos certificats et les personnes responsables des différents certificats.

Exemples de configurations d'alarme

Voici quelques exemples de configurations d'alarme pour différents scénarios de notification :

Avertissement d'expiration de 30 jours

Créez une alarme qui se déclenche lorsqu'un certificat expire dans un délai de 30 jours ou moins :

- Métrique : DaysUntilExpiry
- Statistique : maximum
- Période : 1 jour
- Seuil : 30
- Comparaison : inférieur ou égal au seuil
- Traitement des données manquantes : traitez les données manquantes comme bonnes (pas comme des violations)

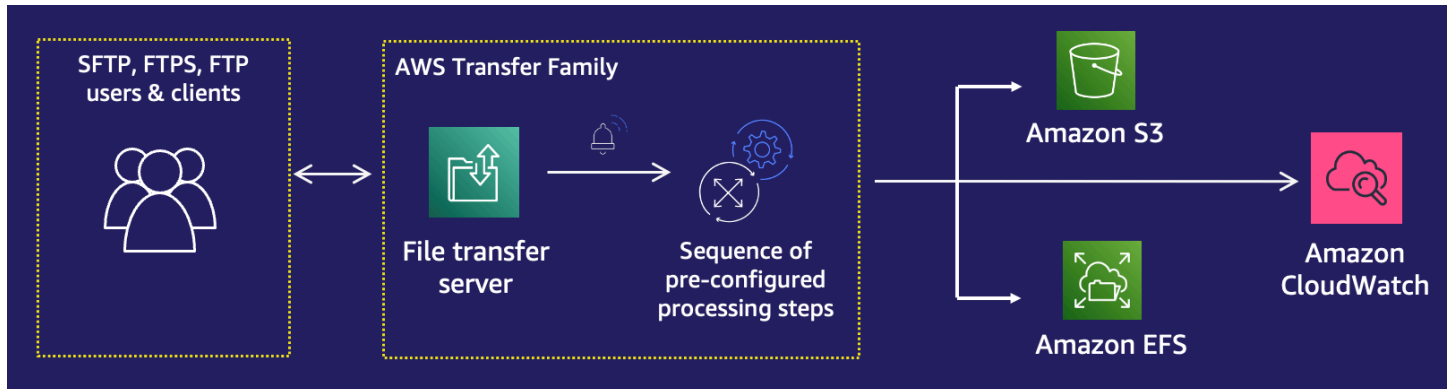
Avertissement d'expiration critique de 7 jours

Créez une alarme critique qui se déclenche lorsqu'un certificat expire dans un délai de 7 jours ou moins :

- Métrique : DaysUntilExpiry
- Statistique : maximum
- Période : 1 jour
- Seuil : 7
- Comparaison : inférieur ou égal au seuil
- Traitement des données manquantes : traitez les données manquantes comme bonnes (pas comme des violations)

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 démarrer un flux de travail après le transfert d'un fichier via 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 interentreprises (B2B) en coordonnant toutes les étapes nécessaires au traitement des fichiers. En outre, vous bénéficiez d'un audit et d'une visibilité de bout en bout.



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.
- Balisage 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. Built-in la gestion 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 [Politiques IAM pour les 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 de CloudWatch métriques pour les serveurs 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](#).
- Transfer Family propose un article de blog et un atelier qui vous guideront dans la création d'une solution de transfert de fichiers. Cette solution s'appuie sur les SFTP/FTPS points de terminaison gérés et sur Amazon Cognito et DynamoDB AWS Transfer Family pour la gestion des utilisateurs.

Le billet de blog est disponible sur [Utilisation d'Amazon Cognito en tant que fournisseur d'identité avec Amazon AWS Transfer Family S3](#). Vous pouvez consulter les détails de l'atelier [ici](#).

- Consultez [AWS Transfer Family Managed Workflows](#) pour une brève introduction aux flux de travail Transfer Family.
- [L'atelier suivant propose des ateliers pratiques pour créer des flux de travail entièrement automatisés et pilotés par des événements impliquant le transfert de fichiers vers ou depuis des serveurs SFTP externes vers Amazon S3, ainsi que le prétraitement et le post-traitement courants de ces fichiers : atelier MFT. Event-driven](#)

Cette vidéo présente un aperçu de cet atelier.

Rubriques

- [Création d'un flux de travail](#)
- [Utiliser des étapes prédéfinies](#)
- [Utiliser des étapes de traitement de fichiers personnalisées](#)
- [Politiques IAM pour les 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.
- Exception-handling étapes — Les gestionnaires d'exceptions sont des étapes de traitement de fichiers qui AWS Transfer Family s'exécutent au cas où des étapes nominales échoueraient ou entraîneraient des erreurs 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 de terminaison de serveur SFTP, FTPS ou FTP](#).
3. Sur la page de détails du serveur, faites défiler la page 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 [Politiques IAM pour les flux de travail](#). Choisissez 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]

Note

Si vous ne souhaitez plus qu'un flux de travail soit associé au serveur, vous pouvez supprimer l'association. Pour en savoir plus, 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 sessions SFTP 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 /amzn-s3-demo-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.

The screenshot shows the AWS Transfer Family console interface. On the left is a navigation sidebar with links to Servers, Connectors, AS2 Trading Partners, Certificates, Profiles, Workflows (selected), Feature Spotlight, What's New, and Documentation. The main content area displays details for a specific workflow.

Workflow Details:

- Description:** Name: Test my workflow; Workflow description: Test workflow A.
- Nominal steps (1):** A table with one step:

Number	Description	Type	Configuration
1	tag_step	TAG	Details
- Exception handlers (1):** A table with one handler:

Number	Description	Type	Configuration
1	delete_if_exception	DELETE	Details
- In-flight executions (0):** A section with a search bar and a table header. The table is empty, showing "No executions" and "No executions to display".
- Tags (1):** A section with a "Manage tags" button and a note: "Use tags to organize, search, and filter your Workflows. We recommend adding a tag with 'Name' as the key and a unique string as the value to easily identify your Workflow."

CLI

Pour afficher les détails du flux de travail, utilisez la commande `describe-workflow` CLI, 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": "amzn-s3-demo-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 CloudFormation console (<https://console.aws.amazon.com/cloudformation>).

Transfer Family > Workflows > w-

W-

Delete

This workflow belongs to the AWS CloudFormation stack **stack-transfer-notifications-blog**. [Manage this stack](#) on the CloudFormation console.

Description

Name

Stack-managed

Workflow description

Workflow for blogpost

Nominal steps (4) [Info](#)

Number	Description	Type	Configuration
1	Lambda	CUSTOM	Details
2	CopyFile	COPY	Details
3	TagFileNotified	TAG	Details
4	DeleteOriginalSourceFile	DELETE	Details

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 le test dossier de *amzn-s3-demo-destination-bucket*.

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 que vous avez chargé 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 `amzn-s3-demo-destination-bucket/richard-roe/processed/` dossier. Si l'utilisateur

mary-major télécharge un fichier, celui-ci est copié dans le amzn-s3-demo-destination-bucket/mary-major/processed/ dossier.

Configure parameters

Configure copy parameters

Step name

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

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 amzn-s3-demo-destination-bucket/2022-02-01/processed/ dossier.

Configure copy parameters

Step name

dynamic-copy-date

Destination bucket name

amzn-s3-demo-destination-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.

`${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/`

Autorisations IAM 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:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
```

```
"Effect": "Allow",
"Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

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 politique IAM.

- 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 simplement déchiffrer des fichiers sans écrire de code à l'aide des flux de travail Transfer Family Managed, [crypter et déchiffrer des fichiers avec](#) PGP et. AWS Transfer Family

Algorithmes de chiffrement symétriques pris en charge

Pour le déchiffrement PGP, Transfer Family prend en charge les algorithmes de chiffrement symétriques utilisés pour chiffrer les données réelles contenues dans les fichiers PGP.

- Pour des informations détaillées sur les algorithmes de chiffrement symétrique pris en charge, consultez [Algorithmes de chiffrement symétrique PGP](#).
- Pour plus d'informations sur les algorithmes de paires de clés PGP utilisés avec ces algorithmes symétriques, consultez. [Algorithmes de paires de clés PGP](#)

Utilisez le déchiffrement PGP dans votre flux de travail

Transfer Family dispose d'un support intégré pour le déchiffrement de Pretty Good Privacy (PGP). Vous pouvez utiliser le déchiffrement PGP sur les fichiers chargés via SFTP, FTPS ou FTP vers Amazon Simple Storage Service (Amazon S3) ou Amazon Elastic File System (Amazon EFS).

Pour utiliser le déchiffrement PGP, vous devez créer et stocker les clés privées PGP qui seront utilisées pour le déchiffrement de vos fichiers. Vos utilisateurs peuvent ensuite chiffrer les fichiers à l'aide des clés de chiffrement PGP 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 plus d'informations sur les algorithmes PGP pris en charge et les recommandations, consultez [Algorithmes de chiffrement et de déchiffrement PGP](#).

Pour utiliser le déchiffrement PGP dans votre flux de travail

1. Identifiez un serveur Transfer Family pour héberger votre flux de travail ou créez-en un nouveau. Vous devez avoir l'ID du serveur avant de pouvoir stocker vos clés PGP AWS Secrets Manager avec le nom secret correct.
2. Enregistrez votre clé PGP AWS Secrets Manager sous le nom secret requis. Pour en savoir plus, consultez [Gérer les clés PGP](#). Les flux de travail peuvent localiser automatiquement la clé PGP appropriée 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 la section [AWS Secrets Manager Tarification](#).

3. Chiffrez un fichier à l'aide de votre paire de clés PGP. (Pour une liste des clients pris en charge, voir [Clients PGP 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 clés PGP. `testfile.txt` Remplacez-le par le nom du fichier que vous souhaitez chiffrer.

```
gpg -e -r username@example.com testfile.txt
```

⚠ Important

Lorsque vous chiffrez des fichiers destinés à être utilisés avec AWS Transfer Family des flux de travail, assurez-vous toujours de spécifier un destinataire non anonyme à l'aide du `-t` paramètre. Le chiffrement anonyme (sans indication de destinataire) peut entraîner des échecs de déchiffrement dans le flux de travail, car le système ne sera pas en mesure d'identifier la clé à utiliser pour le déchiffrement. Les informations de débogage relatives à ce problème sont disponibles à l'adresse [Résoudre les problèmes de chiffrement des destinataires anonymes](#).

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 EFS dans le cadre de votre flux de travail. Pour plus de détails sur la configuration du déchiffrement, consultez [Utilisez le déchiffrement PGP 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 déchiffrement PGP.

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 fichiers Amazon EFS 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 Amazon EFS, 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.

Autorisations IAM 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:::amzn-s3-demo-destination-bucket"
  ]
}, {
  "Sid": "HomeDirObjectAccess",
  "Effect": "Allow",
  "Action": [
    "s3:PutObject",
    "s3:GetObject",
    "s3:DeleteObjectVersion",
    "s3:DeleteObject",
    "s3:GetObjectVersion"
  ],
  "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
  "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 politique IAM.

- 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:::amzn-s3-demo-bucket/*"
    ]
}

```

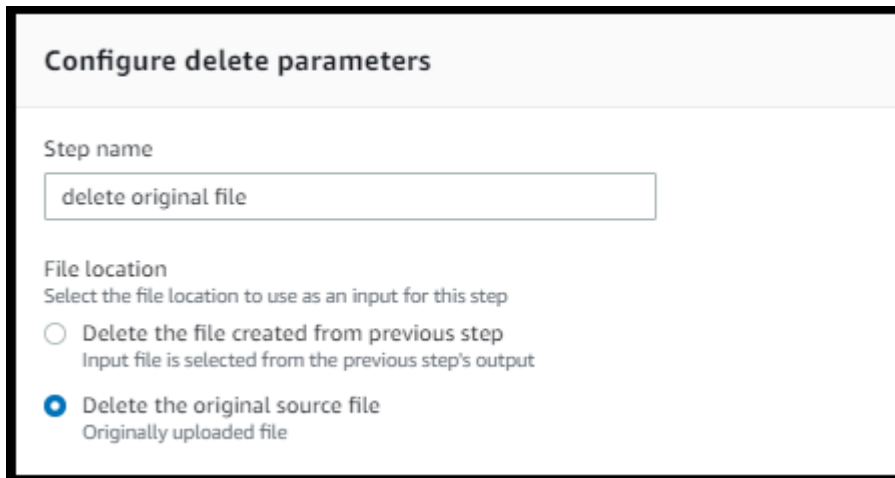
Note

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 politique IAM.

- 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

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 cliquez sur Suivant.
- c. Entrez le nom de l'étape, puis sélectionnez un compartiment de destination et un préfixe de clé.

The screenshot shows the 'Configure parameters' screen for Step 2 of the AWS Transfer Family console. On the left, a sidebar lists three steps: Step 1 (Choose step type), Step 2 (Configure parameters), and Step 3 (Review and create). The main area is titled 'Configure parameters' and contains a section 'Configure copy parameters'. This section includes three input fields: 'Step name' with the value 'copy-step-first-step', 'Destination bucket name' with a dropdown menu showing 'example-bucket', and 'Destination key prefix' with the value 'test/'. Below these fields is a checkbox labeled 'Overwrite existing' which is currently unchecked. A help text for the 'Destination key prefix' field states: '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.'

- 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": "amzn-s3-demo-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 de terminaison de serveur SFTP, FTPS ou FTP](#). Remplacez chaque *user input placeholder* par vos propres informations.

```
aws transfer update-server --server-id server-ID --region region-ID
```

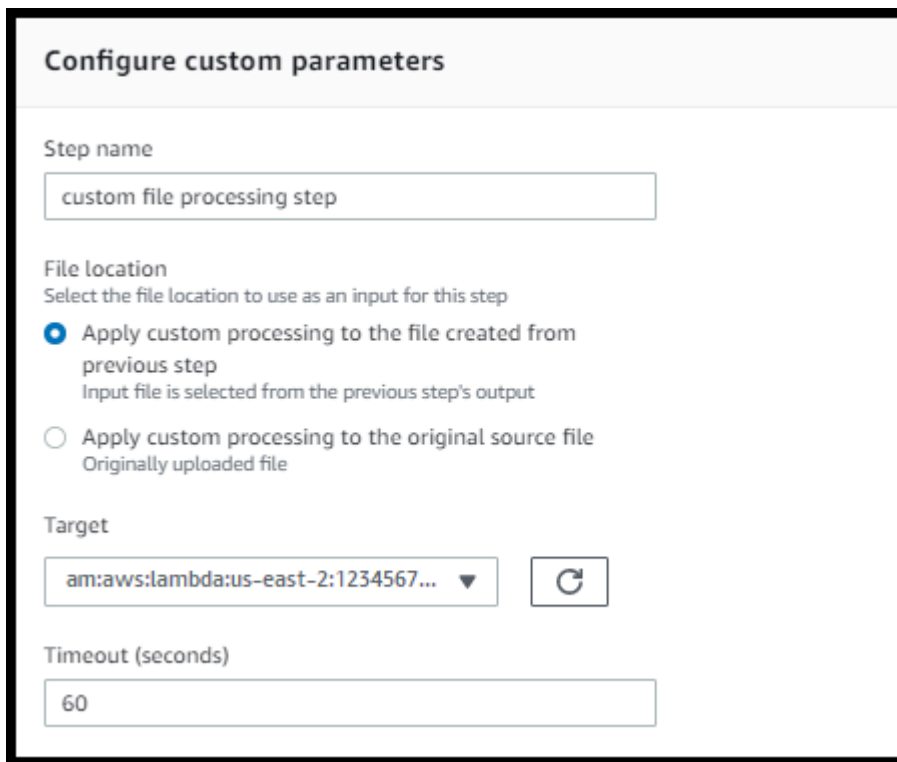
```
--workflow-details '{"OnUpload":[{"WorkflowId": "workflow-ID", "ExecutionRole": "execution-role-ARN"}]}'
```

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, consultez [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'opération d'[SendWorkflowStepState](#) API. `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'opération d'`SendWorkflowStepState` API 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'opération `SendWorkflowStepState` API, 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'opération d'`SendWorkflowStepState` API depuis votre fonction Lambda, vous devez utiliser une version du AWS SDK publiée après l'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 Lambda-processed renvoi du fichier pour l'utiliser 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` 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 Amazon EFS.

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": "amzn-s3-demo-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 concernant l'état d'exécution, puis appelle l'opération d'[SendWorkflowStepState](#) API pour renvoyer le statut au flux de travail de l'étape SUCCESS, soit. FAILURE Avant que votre fonction n'appelle l'opération 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)
    }
```

Autorisations IAM 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"  
]  
}
```

Politiques IAM pour les 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 Gestion des identités et des accès AWS (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 politique IAM.

- 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 rôle IAM et ajoutez-y la politique AWS `AWSTransferFullAccess` gérée. Pour plus d'informations sur la création d'un nouveau rôle IAM, consultez [the section called "Création d'un rôle et d'une politique IAM"](#).
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:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "AllObjectActions",
        "Effect": "Allow",
        "Action": "s3:*Object",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Sid": "GetObjectVersion",
        "Effect": "Allow",
        "Action": "s3:GetObjectVersion",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ]
    },
    {
        "Sid": "Custom",
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": [
            "arn:aws:lambda:us-east-1:123456789012:function:function-name"
        ]
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",

```

```

        "s3:PutObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-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 rôles IAM, 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 obtenir une description de ce problème, ainsi que des exemples permettant de l'éviter, reportez-vous à [the section called "Cross-service prévention confuse des adjoints"](#).

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 utiliser la politique IAM suivante. 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:::amzn-s3-demo-source-bucket/*"
},
{
    "Sid": "CopyWrite",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
},
{
    "Sid": "CopyList",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
},
{
    "Sid": "Tag",
    "Effect": "Allow",
    "Action": [
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
    "Condition": {
        "StringEquals": {
            "s3:RequestObjectTag/Archive": "yes"
        }
    }
},
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",

```

```

    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ],
  },
  {
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:GetObject",
      "s3:DeleteObjectVersion",
      "s3:DeleteObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
  },
  {
    "Sid": "Decrypt",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:us-east-1:123456789012: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 IAM suivante. 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:us-east-1:123456789012: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 format CSV
- Une étape de gestion des exceptions qui envoie un e-mail au cas où le fichier téléchargé n'est pas au format CSV 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

Name

Delete after upload

Workflow description

test-my-workflow

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

- Ouvrez la CloudWatch console Amazon à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
- Dans le volet de navigation de gauche, choisissez Logs, puis Log groups.
- Sur la page Groupes de journaux, dans la barre de navigation, choisissez la région appropriée pour votre AWS Transfer Family serveur.
- 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 du protocole de transfert de fichiers (SFTP) Secure Shell (SSH).
 - 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": "amzn-s3-demo-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": "amzn-s3-demo-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 de CloudWatch métriques pour les serveurs Transfer Family](#).

Création d'un flux de travail à partir d'un modèle

Vous pouvez déployer une 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 CloudFormation pile qui crée un AWS Transfer Family flux de travail et un serveur

1. Ouvrez la 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* par l'ARN d'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 l'ARN de votre fonction Lambda. Par exemple, `arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp`.

4. Suivez les instructions pour déployer une 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 serveur AWS Transfer Family SFTP qui utilise des utilisateurs gérés par le service, 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.

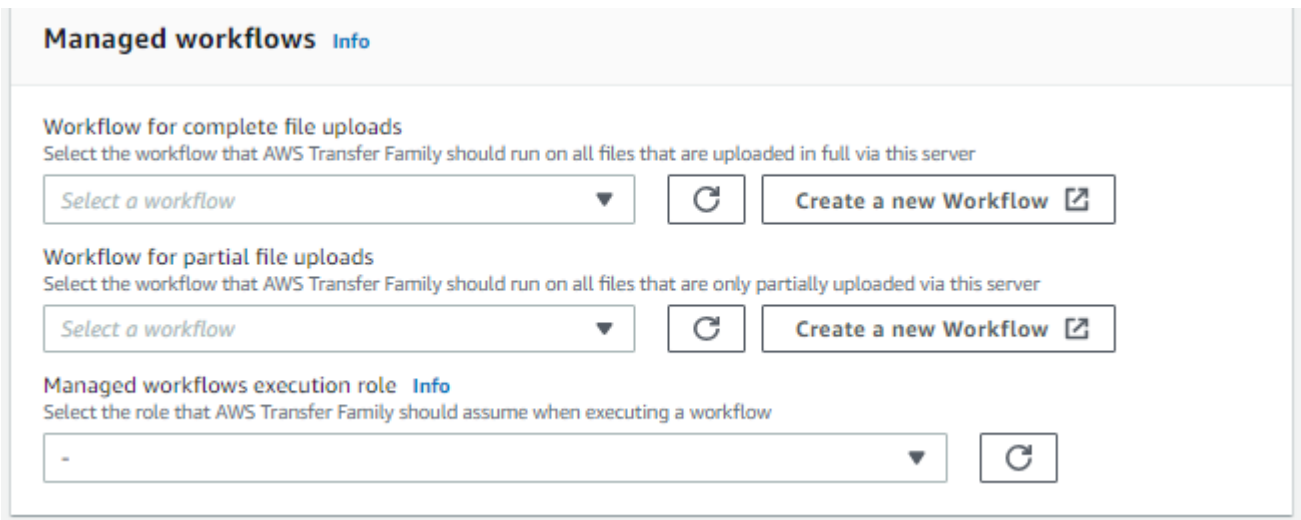
Console

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 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.



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

Select a workflow ▼  [Create a new Workflow](#) 

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

Select a workflow ▼  [Create a new Workflow](#) 

Managed workflows execution role [Info](#)
Select the role that AWS Transfer Family should assume when executing a workflow

- ▼ 

- Faites défiler l'écran vers le bas et choisissez Enregistrer pour enregistrer vos modifications.

CLI

Vous utilisez l'appel `update-server` (ou `UpdateServer` pour l'API) 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.

- Cross-account et les AWS Lambda fonctions interrégionales ne sont pas prises en charge. Vous pouvez toutefois effectuer des copies entre comptes, à condition que vos politiques Gestion des identités et des accès AWS (IAM) 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.
- Vous pouvez associer un flux de traitement de fichiers à un serveur Transfer Family qui utilise le protocole AS2. Toutefois, les messages AS2 n'exécutent pas les flux de travail attachés au serveur.

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 privées PGP, 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 sessions SFTP 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-enabled serveur.

Rubriques

- [Afficher la liste des serveurs](#)
- [Supprimer un serveur](#)
- [Afficher les détails des serveurs SFTP, FTPS et FTP](#)
- [Afficher les détails du serveur AS2](#)
- [Support IPv6 pour les serveurs Transfer Family](#)
- [Modifier les détails du serveur](#)
- [Modifier la configuration du fournisseur d'identité](#)
- [Gérez les clés d'hôte pour votre SFTP-enabled serveur](#)
- [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 les détails des serveurs SFTP, FTPS et FTP](#).

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 s'affiche **delete**, entrez le mot, 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 de la 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 les détails des serveurs SFTP, FTPS et FTP

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 serveurs AS2 est légèrement différente. Pour les serveurs AS2, voir [Afficher les détails du serveur AS2](#).

Protocols

[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider

[Edit](#)

Identity provider type
Service managed

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-](#)**Logging role** [Info](#)

-

Security Policy [Info](#)

TransferSecurityPolicy-PQ-SSH-Experimental-2023-04

Domain

Amazon S3

Login display banner[View the display message](#)**Optimized directories** [Info](#)

ENABLED

SetStat option

Ignore

TLS session resumption

-

Passive IP

-

Afficher les détails du serveur AS2

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 serveurs AS2, vous pouvez également afficher les adresses IP de sortie MDN asynchrones AS2.

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.

Chaque serveur AS2 se voit attribuer trois adresses IP statiques. Utilisez ces adresses IP pour envoyer des mDNS asynchrones à vos partenaires commerciaux via AS2.

AS2 asynchronous MDN egress IP details

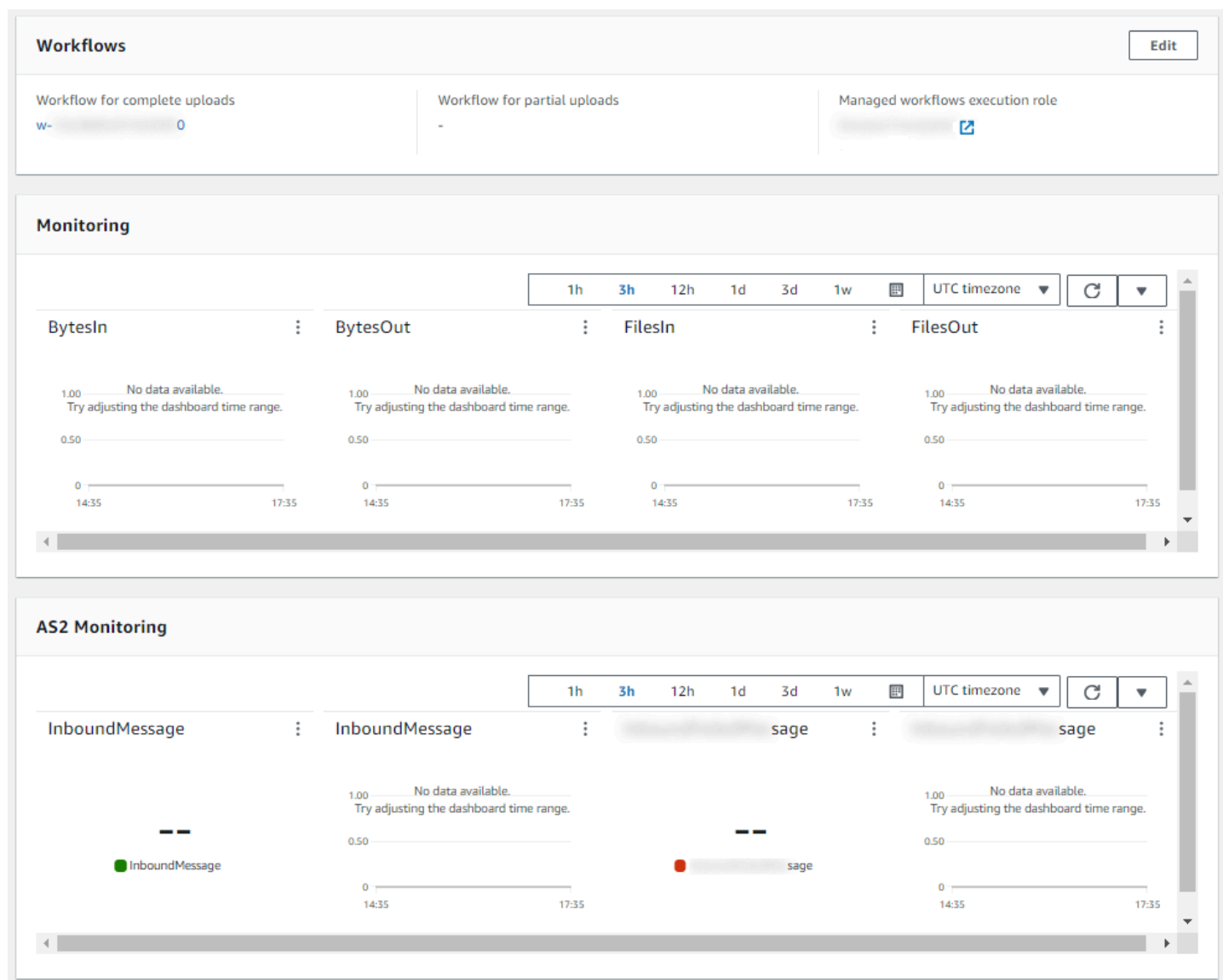
Below are the service managed static IP addresses used for sending your asynchronous MDNs to trading partners over AS2







La partie inférieure de la page de détails du serveur AS2 contient des informations sur tout flux de travail associé ainsi que des informations de surveillance et de balisage.



Support IPv6 pour les serveurs Transfer Family

AWS Transfer Family prend en charge les points de terminaison à double pile (IPv4 et IPv6) pour les ressources suivantes :

- Points de terminaison publics SFTP
- Points de terminaison internes VPC pour tous les protocoles (et AS2) SFTP/FTPS/FTP
- Points de terminaison publics pour les serveurs AS2-enabled Transfer Family, en suivant les étapes indiquées dans [Utilisation d'un Application Load Balancer pour la connectivité d'un serveur AS2 à double pile](#)
- Points de terminaison d'API

Grâce à la prise en charge du double stack, vos points de terminaison Transfer Family peuvent communiquer avec les clients compatibles IPv4 et IPv6. Cela vous permet de passer progressivement d'un système IPv4 à un système IPv6 sans avoir à tout changer en une seule fois, de respecter les exigences de conformité IPv6 et d'éliminer le besoin d'équipements réseau coûteux pour gérer la traduction d'adresses entre IPv4 et IPv6. Pour plus de détails, consultez la section [DNS et points de terminaison](#) dans la référence des AWS Transfer Family API. Pour une liste complète des points de terminaison disponibles, consultez la section Points de [AWS Transfer Family terminaison et quotas](#) dans le. Références générales AWS

Limitations du protocole IPv6

Les ressources Transfer Family suivantes ne prennent pas actuellement en charge le protocole IPv6 :

- VPC-Internet points de terminaison
- Type de point de terminaison VPC_ENDPOINT (obsolète)

Le protocole FTPS prend en charge les commandes PASV et EPSV pour demander un port de données ouvert pour les opérations de listage, d'obtention et de placement de fichiers. Cependant, le PASV ne fonctionne pas avec IPv6 car il nécessite une IPv4-specific réponse. L'EPSV continue de fonctionner car il renvoie uniquement les informations de port.

Pour utiliser le FTPS, nous recommandons l'une des solutions suivantes :

- Configurez votre client FTPS pour utiliser EPSV
- Utiliser IPv4 au lieu d'IPv6

Le SFTP prend en charge les protocoles IPv4 et IPv6. Nous recommandons d'utiliser le protocole SFTP au lieu du protocole FTPS lorsque vous travaillez avec des points de terminaison à double pile.

Configuration d'IPv6 pour les serveurs

Lors de la création d'un nouveau serveur ou de la mise à jour d'un serveur existant, vous pouvez choisir le type d'adresse IP :

- IPv4 (par défaut) : pour des raisons de rétrocompatibilité, le serveur n'accepte que les connexions IPv4.
- Dual-stack: Le serveur acceptera les connexions IPv4 et IPv6.

Pour mettre à jour le type d'adresse IP d'un serveur existant :

1. Arrêtez le serveur.
2. Modifiez les détails du point de terminaison.
3. Changez le type d'adresse IP en Dual-stack.
4. Démarrez le serveur .

 Note

Pour les VPC-Internet points de terminaison, le mode double pile n'est actuellement pas pris en charge.

Utilisation d'un Application Load Balancer pour la connectivité d'un serveur AS2 à double pile

Vous pouvez activer la connectivité à double pile (IPv4 et IPv6) avec votre serveur AS2 à l'aide d'un Application Load Balancer doté d'un point de terminaison public. Cela permet aux partenaires commerciaux de se connecter à votre serveur AS2 via IPv4 ou IPv6.

Pour configurer un Application Load Balancer à double pile pour votre serveur AS2

1. Créez un VPC avec les paramètres suivants :
 - VPC uniquement
 - Entrée CIDR IPv4 manuelle
 - Amazon-provided Bloc d'adresse CIDR IPv6
2. Créez au moins deux sous-réseaux dans différentes zones de disponibilité :
 - Ajouter des CIDR IPv6 aux sous-réseaux
 - Lorsque vous créez des sous-réseaux, allouez uniquement un sous-ensemble des adresses du VPC afin de laisser IPv4/IPv6 des adresses disponibles pour des sous-réseaux supplémentaires
3. Créez une passerelle Internet pour le VPC.
4. Modifiez la table de routage et ajoutez deux itinéraires :

- Un itinéraire avec Destination `0.0.0.0/0`
 - Un itinéraire avec Destination : `:/0`
 - Définissez les deux cibles de route vers la passerelle Internet que vous avez créée
5. Créez un AS2-enabled serveur dans le VPC que vous avez créé à l'étape 1. Assurez-vous de spécifier le `IpAddressType` `asDUALSTACK`.

Pour plus de détails sur la création d'un serveur Transfer Family utilisant le protocole AS2, consultez [Création d'un serveur AS2](#).

6. Créez un groupe cible :
- Pour Spécifier les détails du groupe, configurez :
 - Type de cible : adresses IP
 - Nom : Entrez un nom
 - Protocole : HTTP
 - Hafen : 5080
 - VPC : sélectionnez le VPC que vous avez créé
 - Version du protocole : HTTP/1
 - Contrôles de santé : utiliser les valeurs par défaut
 - Pour les cibles du registre :
 - Entrez l'adresse IPv4 privée de votre serveur AS2
 - Choisissez Inclure comme en attente ci-dessous
7. Créez un Application Load Balancer :
- Entrez un nom
 - Pour Schéma, sélectionnez Internet-facing
 - Pour le type d'adresse IP, choisissez Dualstack
 - Pour le mappage du réseau :
 - Sélectionnez le VPC que vous avez créé
 - Sélectionnez les zones de disponibilité dans lesquelles vous avez créé des sous-réseaux
 - Pour les groupes de sécurité, sélectionnez un groupe de sécurité qui autorise le trafic IPv4 et IPv6 entrant depuis n'importe quelle adresse IP sur le port 80
 - Pour les auditeurs et le routage :

- Protocole : HTTP
- Port : 80
- Action par défaut : Transférer vers le groupe cible que vous avez créé
- Choisissez Créer un équilibreur de charge

Après avoir créé l'Application Load Balancer, les partenaires commerciaux peuvent utiliser son nom DNS pour envoyer du trafic vers votre serveur AS2. Cette configuration permet à votre serveur AS2 d'accepter des connexions provenant de clients IPv4 et IPv6 via l'Application Load Balancer à double pile.

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 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, vous pouvez désormais passer d'un type de fournisseur d'identité à un autre (fournisseur géré par le service, AWS Directory Service ou fournisseur

d'identité personnalisé). Pour plus de détails sur la modification des types de fournisseurs d'identité et les informations requises pour chaque transition, consultez [Modifier la configuration du fournisseur d'identité](#).

- 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 ajouter AS2 en tant que protocole à votre serveur. Pour en savoir plus, 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-enabled serveur](#).
- 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-enabled serveur](#).
 - 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.
 - Reprise de session TLS : fournit un mécanisme permettant de reprendre ou de partager une clé secrète négociée entre le contrôle et la connexion de données pour une session FTPS. Pour plus de détails, consultez la TlsSessionResumptionMode documentation dans cette [ProtocolDetails](#) rubrique.
 - IP passive : indique le mode passif, pour les protocoles FTP et FTPS. Saisissez une adresse IPv4 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.

 Note

Évitez de placer des équilibreurs de charge réseau (NLB) ou des passerelles NAT devant les serveurs. AWS Transfer Family Cette configuration augmente les coûts et peut entraîner des problèmes de performances. Pour plus d'informations, consultez [Évitez de placer les NLB et les NAT devant AWS Transfer Family serveurs](#).

- 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[Edit](#)

Protocols over which clients can connect to your server's endpoint

- SFTP

Identity provider[Edit](#)

Identity provider type
Service managed

 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	SetStat option Ignore
Logging role Info -	Login display banner View the display message	TLS session resumption -
Security Policy Info TransferSecurityPolicy-PQ-SSH-Experimental-2023-04	Optimized directories Info ENABLED	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 (SFTP) Secure Shell (SSH) — transfert de fichiers via SSH

Pour plus d'informations sur le protocole SFTP, consultez [Création d'un SFTP-enabled serveur](#).

- File Transfer Protocol Secure (FTPS) : transfert de fichiers avec cryptage TLS

Pour plus d'informations sur le protocole FTP, consultez [Création d'un FTPS-enabled serveur](#).

- Protocole de transfert de fichiers (FTP) : transfert de fichiers non chiffré

Pour plus d'informations sur le FTPS, consultez [Création d'un FTP-enabled serveur](#).

Note

Si un serveur existant est activé uniquement pour le 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 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 via 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 dans ACM dans](#) le guide de l'AWS Certificate Manager utilisateur.

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

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

- RSA 2048 octets (RSA_2048)
- RSA 4 096 octets (RSA_4096)
- 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 certificat de SSL/TLS X.509 version 3 valide avec un nom de domaine complet ou une adresse IP spécifiée et contenir des informations sur l'émetteur.

3. Choisissez Enregistrer. Vous êtes renvoyé à la page des détails du serveur.

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. En outre, pour les points de terminaison VPC, vous pouvez modifier les informations de zone de disponibilité.

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. Avant de pouvoir modifier le type de point de terminaison, vous devez d'abord arrêter le serveur. Ensuite, sur la page Modifier la configuration du point de terminaison, pour le type de point de terminaison, vous pouvez choisir l'une des valeurs 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 le VPC, consultez. [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`.

- Alias DNS Amazon Route 53 — Pour utiliser un alias DNS créé automatiquement pour vous dans Route 53, choisissez cette option.
- Autre DNS — Pour utiliser un nom d'hôte que vous possédez déjà dans un service DNS externe, choisissez Autre DNS.

Le choix de l'alias DNS Amazon Route 53 ou d'un 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 nom DNS que vous fournissez et qu'un service DNS peut résoudre. Vous pouvez utiliser Route 53 comme résolveur DNS ou utiliser votre propre fournisseur de services DNS. 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. Pour les points de terminaison VPC, vous pouvez modifier les informations dans le volet Zones de disponibilité.
5. Choisissez 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 rôle IAM de CloudWatch journalisation pour vous lorsque vous avez créé un serveur, le rôle IAM 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. En fonction de votre configuration, choisissez entre un rôle de journalisation, une journalisation JSON structurée ou les deux. Pour de plus amples informations, veuillez consulter [Mettre à jour la journalisation d'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 c'est le cas de votre terminal FIPS-enabled, vous ne pouvez pas remplacer la politique de sécurité FIPS par une politique de sécurité non FIPS.

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 de l'algorithme 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 serveurs](#).

3. Choisissez 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 de la 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 serveurs](#).

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 [Politiques IAM pour les flux de travail](#). Choisissez 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 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 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 résoudre vos problèmes.

Modifier la configuration du fournisseur d'identité

Vous pouvez modifier le type de fournisseur d'identité de votre serveur de n'importe quel type à un autre. Les types de fournisseurs d'identité disponibles sont les suivants :

- Service géré : stockez les informations d'identification de l'utilisateur dans le service
- AWS Service d'annuaire : utilisez AWS Managed Microsoft AD ou AWS Directory Service pour les services de domaine Entra ID
- Personnalisé : utilisez la fonction Lambda ou Amazon API Gateway pour intégrer votre fournisseur d'identité existant

Lorsque vous modifiez le type de fournisseur d'identité, vous devez fournir des informations spécifiques en fonction de la transition que vous effectuez. Les sections suivantes décrivent les informations requises pour chaque type de modification.

Important

Points à prendre en compte lors du changement de fournisseur d'identité :

- Migration des utilisateurs : lors du changement de type de fournisseur d'identité, les configurations utilisateur existantes ne sont pas automatiquement migrées. Vous devrez configurer les utilisateurs dans le nouveau système de fournisseur d'identité.
- Tests : testez minutieusement la nouvelle configuration du fournisseur d'identité avant de modifier les environnements de production.
- Autorisations : assurez-vous que le nouveau fournisseur d'identité dispose des autorisations IAM nécessaires et que les rôles sont configurés avant d'effectuer la modification.

Passage à un fournisseur d'identité géré par des services

Lorsque vous passez d'un autre type de fournisseur d'identité à un fournisseur géré par des services, vous devez :

- Sélectionnez Service géré comme type de fournisseur d'identité
- Créez de nouveaux utilisateurs directement une AWS Transfer Family fois la modification terminée, car les configurations utilisateur existantes provenant d'autres fournisseurs d'identité ne seront pas transférées

Exemple : si vous passez d'un fournisseur d'identité personnalisé à un fournisseur géré par des services, vous devez recréer tous les comptes utilisateurs et les autorisations associées au sein du service. AWS Transfer Family

Passage au AWS Directory Service

Lorsque vous passez d'un autre type de fournisseur d'identité à AWS Directory Service, vous devez fournir :

- Annuaire — Sélectionnez un répertoire AWS Managed Microsoft AD ou AWS Directory Service pour Entra ID Domain Services existant
- Accès : choisissez de restreindre l'accès à un groupe spécifique ou d'autoriser l'accès à tous les utilisateurs de l'annuaire
- Rôle d'accès : rôle IAM qui permet d'accéder AWS Transfer Family à votre annuaire

Exemple : si vous passez d'un service géré à un service d' AWS annuaire, vous devez sélectionner votre d-1234567890 annuaire existant, choisir de restreindre l'accès au TransferUsers groupe et spécifier le rôle TransferDirectoryAccessRole IAM.

Passage à un fournisseur d'identité personnalisé

Lorsque vous passez d'un autre type de fournisseur d'identité à un fournisseur d'identité personnalisé, vous devez choisir entre la fonction Lambda ou Amazon API Gateway et fournir la configuration requise :

Utilisation de la fonction Lambda

Pour l'intégration de la fonction Lambda, fournissez :

- Fonction — Sélectionnez une fonction Lambda existante qui gère l'authentification
- Méthode d'authentification (pour le protocole SFTP) — Choisissez le mot de passe, la clé publique ou les deux

Exemple : si vous passez d'un fournisseur d' AWS identité Lambda personnalisé à un fournisseur d'identité Lambda personnalisé, vous devez sélectionner votre `TransferCustomAuth` fonction et choisir Password comme méthode d'authentification.

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

Utilisation d'Amazon API Gateway

Pour l'intégration d'Amazon API Gateway, fournissez :

- URL API Gateway : URL d'appel de votre point de terminaison API Gateway

- Rôle d'invocation : rôle IAM qui permet d' AWS Transfer Family appeler votre API Gateway
- Méthode d'authentification (pour le protocole SFTP) — Choisissez le mot de passe, la clé publique ou les deux

Exemple : si vous passez de la gestion des services à API Gateway, vous devez fournir l'URL `https://abcdef123.execute-api.us-east-1.amazonaws.com/prod`, spécifier le rôle `TransferApiGatewayInvocationRole` IAM et choisir la clé publique comme méthode d'authentification.

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

Passer de la fonction Amazon API Gateway à la fonction Lambda

Une transition courante consiste à passer d'Amazon API Gateway à la fonction Lambda pour l'intégration de fournisseurs d'identité personnalisés. Cette modification vous permet de simplifier votre architecture tout en conservant la même logique d'authentification.

Principales considérations relatives à cette transition :

- Même fonction, autorisations différentes — Vous pouvez utiliser la même fonction Lambda à la fois pour API Gateway et pour l'intégration directe de Lambda, mais la politique de ressources doit être mise à jour.
- Exigences en matière de politique de ressources — Lorsque vous passez à l'intégration Lambda directe, la politique de ressources de la fonction doit `transfer.amazonaws.com` autoriser l'appel de la fonction, en plus de `apigateway.amazonaws.com`

Pour effectuer cette modification

1. Mettez à jour la politique de ressources de votre fonction Lambda pour autoriser l'appel `transfer.amazonaws.com` de la fonction.
2. Dans la AWS Transfer Family console, remplacez le fournisseur d'identité par API Gateway par la fonction Lambda.
3. Sélectionnez votre fonction Lambda existante.
4. Testez la configuration pour vous assurer que l'authentification fonctionne correctement.

Exemple de politique de ressources pour l'intégration directe de Lambda :

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "transfer.amazonaws.com",
        "apigateway.amazonaws.com"
      ]
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
  }]
}
```

Préservation des utilisateurs lors des transitions entre fournisseurs d'identité

Lorsque vous changez de type de fournisseur d'identité, les configurations utilisateur existantes sont préservées dans des scénarios spécifiques afin de permettre une restauration efficace en cas de problème :

- Service-managed au fournisseur d'identité personnalisé et vice versa — Si vous passez d'un fournisseur d'identité géré par des services à un fournisseur d'identité personnalisé, puis que vous revenez à un fournisseur géré par des services, tous les utilisateurs sont conservés dans leur dernière configuration connue.
- AWS Directory Service vers un fournisseur d'identité personnalisé et vice versa : si vous passez d'un fournisseur d'identité personnalisé AWS Directory Service à un fournisseur d'identité personnalisé AWS Directory Service, puis revenez à, toutes les définitions des groupes d'accès délégué sont conservées dans leur dernière configuration connue.

Ce comportement de conservation vous permet de tester en toute sécurité des configurations de fournisseurs d'identité personnalisées et de revenir à votre configuration précédente sans perdre les configurations d'accès utilisateur.

Considérations importantes lors du changement de fournisseur d'identité

- Migration des utilisateurs : lors du changement de type de fournisseur d'identité, les configurations utilisateur existantes ne sont pas automatiquement migrées. Vous devrez configurer les utilisateurs dans le nouveau système de fournisseur d'identité.
- Tests : testez minutieusement la nouvelle configuration du fournisseur d'identité avant de modifier les environnements de production.
- Autorisations : assurez-vous que le nouveau fournisseur d'identité dispose des autorisations IAM nécessaires et que les rôles sont configurés avant d'effectuer la modification.

Gérez les clés d'hôte pour votre SFTP-enabled serveur

Les clés d'hôte du serveur sont des clés privées utilisées par le serveur Transfer Family pour fournir une identité unique à l'appelant et pour garantir qu'il s'agit du bon serveur. Cette garantie est renforcée par la présence de la clé publique correcte dans le `known_hosts` dossier de l'appelant. (Le `known_hosts` fichier est une fonctionnalité standard utilisée par la plupart des clients SSH pour stocker les clés publiques des serveurs auxquels vous êtes connecté.) Vous pouvez récupérer la clé

publique qui correspond à la clé d'hôte de votre serveur en exécutant la `ssh-keyscan` commande pour votre serveur.

 Important

La modification accidentelle de la clé d'hôte d'un serveur peut être perturbante. Selon la configuration de votre client SFTP, il 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 Génère par défaut des clés d'hôte pour votre SFTP-enabled serveur. Vous pouvez importer des clés d'hôte de serveur pour préserver l'identité de l'hôte et éviter de mettre à jour les banques de confiance des clients. [Quand importer les clés d'hôte](#) répertorie quelques raisons pour lesquelles vous pourriez vouloir le faire. Si vous ne fournissez pas de clés d'hôte, de nouvelles clés seront générées pour vous.

AWS Transfer Family prend en charge plusieurs clés hôtes de différents types (RSA, ECDSA et ED25519) afin d'assurer la compatibilité avec un plus large éventail d'algorithmes de signature hôte client. Différents types de clés activent des algorithmes spécifiques : les clés RSA activent les algorithmes `rsa-*`, les clés ECDSA activent les algorithmes `ecdsa-*` et les clés ED25519 activent les algorithmes `ed25519`. Planifiez vos types de clés au moment de la création du serveur, car l'introduction de types de clés supplémentaires une fois que les clients ont commencé à interagir avec le serveur peut perturber certains clients et être aussi problématique que le remplacement des clés d'hôte existantes.

Pour éviter que vos utilisateurs ne soient invités à vérifier à nouveau l'authenticité de votre SFTP-enabled serveur, importez la clé d'hôte de votre serveur local sur le SFTP-enabled serveur. Cette opération empêche également vos utilisateurs d'obtenir un avertissement à propos d'une attaque potentielle d'interposition.

Vous pouvez également effectuer une rotation périodique des clés d'hôte, par mesure de sécurité supplémentaire. Pour en savoir plus, consultez [Faites pivoter les clés de l'hôte du serveur](#).

 Note

Les clés d'hôte du serveur sont utilisées par les serveurs qui prennent en charge le protocole SFTP.

Quand importer les clés d'hôte

Bien que AWS Transfer Family vous puissiez générer des clés d'hôte automatiquement, il existe plusieurs scénarios dans lesquels l'importation de vos propres clés d'hôte présente des avantages opérationnels :

- **Migration de serveurs** : vous migrez d'un serveur existant vers un serveur existant AWS Transfer Family et vous souhaitez éviter de mettre à jour les banques de confiance (`known_hosts` fichiers) pour les clients existants.
- **Reprise après sinistre et basculement** : plusieurs AWS Transfer Family serveurs (par exemple, un dans l'est des États-Unis (Ohio) et un dans l'ouest des États-Unis (Oregon)) partagent le même nom DNS public. L'utilisation des mêmes clés d'hôte sur les deux serveurs garantit un basculement sans faille sans échec de l'authentification du client.
- **Continuité opérationnelle** : vous souhaitez que le matériel clé de l'hôte soit disponible pour être utilisé avec d'autres serveurs (AWS Transfer Family ou autrement) à l'avenir afin de maintenir une identité de serveur cohérente dans l'ensemble de votre infrastructure.
- **Contrôle des algorithmes** : vous souhaitez améliorer la compatibilité avec les clients en fournissant davantage d'algorithmes de clé hôte, ou vous souhaitez contrôler les algorithmes que les clients peuvent utiliser en proposant uniquement des clés compatibles avec des algorithmes spécifiques.

Les rubriques suivantes fournissent des procédures détaillées pour gérer les clés d'hôte du serveur :

- [Ajouter une clé d'hôte de serveur supplémentaire](#)- Ajoutez des clés d'hôte supplémentaires à votre serveur
- [Supprimer la clé d'hôte d'un serveur](#)- Supprimer les clés d'hôte de votre serveur
- [Faites pivoter les clés de l'hôte du serveur](#)- Faites pivoter les clés de l'hôte pour une sécurité renforcée
- [Informations supplémentaires sur la clé de l'hôte du serveur](#)- Afficher et gérer les informations clés de l'hôte

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 clé RSA, vous pouvez ajouter une clé ECDSA supplémentaire.

Note

Le client SFTP se connecte à l'aide de la plus ancienne clé de la configuration qui correspond à l'algorithme de la clé. La clé la plus ancienne pour chaque type de clé (RSA, ECDSA ou ED25519) est la clé active du serveur pour ce type.

Remarque de sécurité lorsqu'un serveur Transfer Family possède plusieurs types de clés d'hôte

Si un serveur possède plusieurs types de clés d'hôte, le client SFTP peut attribuer une préférence par type. Ainsi, lorsqu'il existe des clés d'hôte RSA, ECDSA et ED25519 pour le serveur, le choix dépend de la préférence par type.

Les clients SFTP modernes préfèrent les clés d'hôte ECDSA et ED25519 lorsqu'elles existent. Cela devient important si vous souhaitez ajouter une clé ECDSA ou ED25519 alors que le serveur ne possédait auparavant que des clés RSA. L'ajout de la nouvelle clé ECDSA ou ED25519 pourrait se traduire par un avertissement de sécurité pour un client.

Pour le client, la clé apparaîtra comme ayant changé, alors qu'en fait elle n'a pas été modifiée : la nouvelle clé a été ajoutée en plus de la clé RSA existante. Gardez cela à l'esprit si vous décidez d'ajouter de nouveaux types de clés d'hôte de serveur.

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 utilisant le protocole SFTP.
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 (2)							Actions	Add host key
Find resources							< 1 >	
☐	Name	Host key ID	Fingerprint	Description	Key type	Date imported		
☐	Default host key	hostkey-	SHA256:	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

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, entrez une clé privée RSA, ECDSA ou ED25519 utilisée pour identifier votre serveur lorsque des clients s'y connectent via le serveur. SFTP-enabled

 Note

Lorsque vous créez une clé d'hôte de serveur, assurez-vous de la spécifier -N "" (pas de phrase secrète). Consultez [Création de clés SSH sous macOS, Linux ou Unix](#) pour plus de détails sur la façon de générer des paires de clés.

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'opération d'[ImportHostKey](#) API et fournissez la nouvelle clé d'hôte. Si vous créez un nouveau SFTP-enabled serveur, vous fournissez votre clé d'hôte en tant que paramètre dans le cadre de l'opération [CreateServer](#) d'API. 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-enabled serveur 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 utilisant le protocole SFTP.
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 (2)							Actions ▾	Add host key
Find resources							< 1 >	
☐	Name	Host key ID ▾	Fingerprint Info	Description ▾	Key type ▾	Date imported ▾		
☐	Default host key	hostkey-	SHA256:	Default	ssh-rsa	2023-06-30		
☐	ecdsa-521	hostkey-	SHA256:	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13		

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 s'affiche **delete**, entrez le mot, 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'opération d'[DeleteHostKey](#) API 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-enabled serveur 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

Régulièrement, vous pouvez faire pivoter la clé d'hôte de votre serveur. Cette rubrique décrit comment le serveur choisit la clé à appliquer, ainsi que la procédure de rotation de ces touches.

Comment le client choisit une clé d'hôte de serveur

La manière dont Transfer Family choisit la clé de serveur à appliquer dépend des conditions du client SFTP, comme expliqué ici. L'hypothèse est qu'il existe une clé plus ancienne et une clé plus récente.

- Un client SFTP ne possède aucune clé d'hôte publique préalable pour le serveur. La première fois que le client se connecte au serveur, l'une des situations suivantes se produit :
 - Le client échoue à établir la connexion s'il est configuré pour cela.
 - Ou bien, le client choisit la première clé qui correspond aux algorithmes disponibles possibles et demande à l'utilisateur si cette clé est fiable. Si tel est le cas, le client met automatiquement à jour le `known_hosts` fichier (ou tout autre fichier de configuration local ou ressource utilisé par le client pour enregistrer les décisions de confiance) et entre cette clé.

- Un client SFTP possède une ancienne clé dans son `known_hosts` fichier. Le client préfère utiliser cette clé, même s'il en existe une plus récente, que ce soit pour l'algorithme de cette clé ou pour un autre algorithme. Cela est dû au fait que le client a un niveau de confiance plus élevé pour la clé contenue dans son `known_hosts` fichier.
- Un client SFTP possède la nouvelle clé (dans tous les algorithmes disponibles) dans son fichier de `known_hosts` clés. Le client ignore les anciennes clés parce qu'elles ne sont pas fiables et utilise la nouvelle clé.
- Un client SFTP possède les deux clés dans son `known_hosts` fichier. Le client choisit la première clé par index qui correspond à la liste des clés disponibles proposées par le serveur.

Transfer Family préfère que le client SFTP ait toutes les clés dans son `known_hosts` fichier, car cela permet une plus grande flexibilité lors de la connexion à un serveur Transfer Family. La rotation des clés est basée sur le fait que plusieurs entrées peuvent exister dans le `known_hosts` fichier pour le même serveur Transfer Family.

Procédure de rotation de la clé hôte du serveur

Supposons par exemple que vous ayez ajouté le jeu de clés d'hôte de serveur suivant à votre serveur Transfer Family.

Clés d'hôte du serveur

Type de clé d'hôte	Date d'ajout au serveur
RSA	1er avril 2020
ECDSA	1er février 2020
ED25519	1 décembre 2019
RSA	1er octobre 2019
ECDSA	1er juin 2019
ED25519	1 mars 2019

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](#).
3. Toutes les touches sont visibles et peuvent être actives, sous réserve du comportement décrit précédemment dans [Comment le client choisit une clé d'hôte de serveur](#).

Informations supplémentaires sur la clé de l'hôte du serveur

Vous pouvez sélectionner une clé d'hôte pour afficher les détails de cette clé.

Transfer Family > Servers > s-3fe215d89f074ed2a > Hostkey: hostkey-a6fed60bcb704ea9b

hostkey-a6fed60bcb704ea9b

Delete

Host key configuration

Edit

Name

ecdsa-521

Fingerprint

SHA256: [redacted]

Description

ECDSA host key

Key type

ecdsa-sha2-nistp521

Date imported

Thu, 13 Jun 2024 17:08:59 GMT

Amazon Resource Name (ARN)

[redacted]

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.

Server host keys (2)

Find resources

Actions

Edit

Delete

Add host key

< 1 >

	Name	Host key ID	Fingerprint	Description	Key type	Date imported
☐	Default host key	hostkey-[redacted]	SHA256:[redacted]	Default	ssh-rsa	2023-06-30
☒	ecdsa-521	hostkey-[redacted]	SHA256:[redacted]	ECDSA host key	ecdsa-sha2-nistp521	2024-06-13

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 en savoir plus, consultez [Afficher les détails des serveurs SFTP, FTPS et FTP](#). Le tableau suivant décrit les indicateurs disponibles pour Transfer Family.

Namespace	Métrique	Description
AWS/Transfer	BytesIn	Nombre total d'octets transférés vers le serveur. Critères d'établissement de rapports : • Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis. • Pour AS2 : lorsque le client reçoit un message sur son serveur AS2 et émis dès que le traitement du message entrant est terminé Unités : nombre Durée : 5 minutes
	BytesOut	Nombre total d'octets transférés hors du serveur. Critères d'établissement de rapports : • Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis. • Pour AS2 : lorsque le client appelle <code>StartFile Transfer</code> depuis son connecteur AS2 et qu'il est émis dès que le traitement du message sortant est terminé. Unités : nombre

Namespace	Métrique	Description
		Durée : 5 minutes
	FilesIn	Le nombre total de fichiers transférés sur le serveur. Pour les serveurs utilisant le protocole AS2, cette métrique représente le nombre de messages reçus. Critères d'établissement de rapports : • Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis. • Pour AS2 : lorsque le client reçoit un message sur son serveur AS2 et qu'il est émis dès que le traitement du message entrant est terminé. Unités : nombre Durée : 5 minutes

Namespace	Métrique	Description
	FilesOut	Le nombre total de fichiers transférés hors du serveur. Critères d'établissement de rapports : • Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis. • Pour AS2 : lorsque le client appelle <code>StartFile Transfer</code> depuis son connecteur AS2 et qu'il est émis dès que le traitement du message sortant est terminé. Unités : nombre Durée : 5 minutes
	InboundMessage	Nombre total de messages AS2 reçus avec succès d'un partenaire commercial. Critères de signalement : lorsque le client reçoit un message sur son serveur AS2 et qu'il est émis dès que le traitement du message entrant est terminé avec succès Unités : nombre Durée : 5 minutes

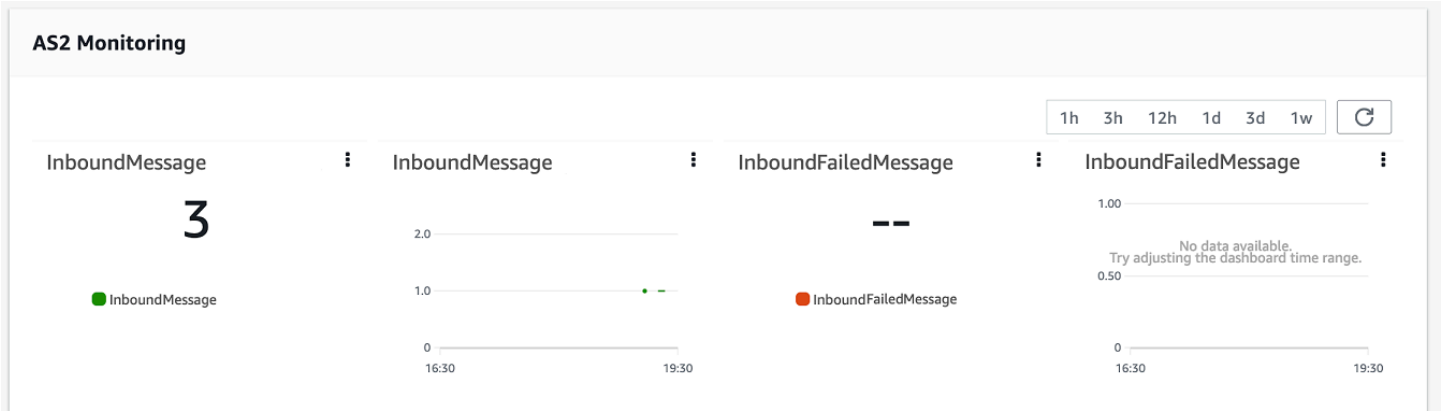
Namespace	Métrique	Description
	InboundFailedMessage	Nombre total de messages AS2 reçus sans succès d'un partenaire commercial. En d'autres termes, un partenaire commercial a envoyé un message, mais le serveur Transfer Family n'a pas réussi à le traiter. Critères de signalement : lorsque le client reçoit un message sur son serveur AS2 et qu'il est émis dès que le traitement du message entrant s'est terminé sans succès Unités : nombre Durée : 5 minutes
	OnUploadExecutionsStarted	Nombre total d'exécutions de flux de travail démarrées sur le serveur. Critères de reporting : déclenché chaque fois qu'une exécution commence Unités : nombre Durée : 1 minute
	OnUploadExecutionsSuccess	Nombre total d'exécutions de flux de travail réussies sur le serveur. Critères de reporting : déclenché chaque fois qu'une exécution se termine avec succès Unités : nombre Durée : 1 minute

Namespace	Métrique	Description
	OnUploadExecutionsFailed	Nombre total d'exécutions de flux de travail infructueuses sur le serveur. Critères de reporting : déclenché chaque fois qu'une exécution échoue Unités : nombre Durée : 1 minute
	OutboundMessage	Nombre total de messages AS2 envoyés avec succès à un partenaire commercial. Critères de signalement : lorsque le client appelle <code>StartFileTransfer</code> depuis son connecteur AS2 et qu'il est émis dès que le message sortant a été traité avec succès Unités : nombre Durée : 5 minutes
	OutboundFailedMessage	Nombre total de messages AS2 envoyés sans succès à un partenaire commercial. Critères de signalement : lorsque le client appelle <code>StartFileTransfer</code> depuis son connecteur AS2 et est émis dès que le traitement du message sortant s'est terminé sans succès Unités : nombre Durée : 5 minutes

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 protocole AS2 est activé, une section de surveillance AS2 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 Gestion des identités et des accès AWS (IAM). Une politique IAM est une déclaration, généralement au format JSON, qui autorise un certain niveau d'accès à une ressource. Vous utilisez une politique IAM pour définir les opérations sur les fichiers que vous souhaitez autoriser ou non vos utilisateurs à effectuer. Vous pouvez également utiliser une politique IAM pour définir le ou les compartiments Amazon S3 auxquels vous souhaitez donner accès à vos utilisateurs. Pour spécifier ces politiques pour les utilisateurs, vous créez un rôle IAM auquel AWS Transfer Family la politique IAM et la relation de confiance sont associées.

Un rôle IAM est attribué à chaque utilisateur. Le type de rôle IAM AWS Transfer Family utilisé est appelé rôle de service. Lorsqu'un utilisateur se connecte à votre serveur, il AWS Transfer Family assume le rôle IAM mappé à l'utilisateur. Pour en savoir plus sur la création d'un rôle IAM qui fournit à un utilisateur l'accès à un compartiment Amazon S3, consultez la section [Création d'un rôle pour déléguer des autorisations à un AWS service](#) dans le guide de l'utilisateur IAM.

Vous pouvez accorder un accès en écriture seule aux objets Amazon S3 en utilisant certaines autorisations dans le cadre d'une politique IAM. Pour en savoir plus, 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 en savoir plus, consultez [Protection et chiffrement des données](#). En outre, vous pouvez obtenir plus d'informations sur [les politiques de session](#) dans le guide de l'utilisateur IAM.

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](#)

- [Approches dynamiques de gestion des autorisations](#)

Autoriser l'accès en lecture et en écriture à un compartiment Amazon S3

Cette section explique comment créer une politique IAM qui autorise l'accès en lecture et en écriture à un compartiment Amazon S3 spécifique. L'attribution à votre utilisateur d'un rôle IAM doté de cette politique IAM permet à celui-ci d'accéder au compartiment Amazon S3 spécifié.

La politique suivante fournit un accès programmatique en lecture, écriture et balisage à un compartiment Amazon S3. Les `PutObjectACL` et `GetObjectACL` 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:::amzn-s3-demo-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:::amzn-s3-demo-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 Amazon Resource Names (ARN).

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 Gestion des identités et des accès AWS (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 Amazon EFS, vous utilisez les autorisations de fichier POSIX 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 rôle IAM.

Note

La longueur maximale d'une politique de session est de 2 048 caractères. Pour plus de détails, consultez le [paramètre de demande Policy](#) pour l'`CreateUser` action dans la référence de l'API.

Pour créer une stratégie de session, utilisez les variables de stratégie suivantes dans votre stratégie IAM :

- `${transfer:HomeBucket}`
- `${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 rôle IAM. Vous créez ces variables dans une politique IAM et vous les fournissez directement lors de la configuration de votre utilisateur. Vous ne pouvez pas non plus utiliser la `${aws:Username}` variable dans cette politique de session. Cette variable fait référence à un nom d'utilisateur IAM et non au nom d'utilisateur requis par AWS Transfer Family.

Exemple de politique de session

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 (ARN) S3 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 Transfer Family soit `/home/bob/amazon/stuff/`.

- `transfer:HomeBucket` est défini sur `/home`.
- `transfer:HomeFolder` est défini 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 `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 rôles et des politiques IAM 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 l'utilisateur IAM.

 Note

AWS Transfer Family stocke le JSON de la politique, au lieu de l'Amazon Resource Name (ARN) de la politique. Ainsi, lorsque vous modifiez la politique dans la console IAM, vous devez revenir à la AWS Transfer Family console et mettre à jour vos utilisateurs avec le

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)"
```

Substitutions imbriquées pour les politiques de session

Les substitutions imbriquées ne sont pas effectuées dans les politiques de session Transfer Family. Les politiques de session peuvent utiliser des variables imbriquées, telles que `${transfer:HomeDirectory}`. Lorsque la politique est traitée, la variable externe (par exemple, `${transfer:HomeDirectory}`) peut être remplacée par une valeur contenant une autre variable (par exemple, `{amzn-s3-demo-bucket:/${transfer:UserName}}`). Cependant, la variable imbriquée n'est plus remplacée par le nom d'utilisateur réel (par exemple, `johndoe`).

Cela signifie que lorsque vous créez des politiques de session pour Transfer Family, vous devez tenir compte de ce comportement et vous assurer que la structure des politiques et l'utilisation des variables sont conçues en conséquence. Il est possible que les variables imbriquées ne soient pas résolues comme prévu et que la politique n'accorde pas les autorisations prévues. Il est important de tester et de valider minutieusement les politiques de session pour s'assurer qu'elles fonctionnent comme prévu. Ce comportement est un élément clé à prendre en compte lors de la mise en œuvre du contrôle d'accès et des autorisations pour votre environnement Transfer Family.

L'une des solutions à ce problème consiste à utiliser le nom réel du compartiment Amazon S3 dans votre politique de session. Ainsi, par exemple, plutôt que de le spécifier `${transfer:HomeDirectory}` dans votre politique de session, utilisez ce qui suit, où `amzn-s3-demo-bucket` est votre véritable bucket : `${amzn-s3-demo-bucket/transfer:UserName}`

Approches dynamiques de gestion des autorisations

Comprendre l'architecture des autorisations Transfer Family

AWS Transfer Family prend en charge la gestion dynamique des autorisations par le biais de politiques de session, qui vous permettent de restreindre les autorisations effectives des rôles IAM

lors de l'exécution. Cette approche fonctionne à la fois pour les utilisateurs gérés par des services et pour les utilisateurs de fournisseurs d'identité personnalisés, mais elle n'est prise en charge que lors du transfert de fichiers vers ou depuis Amazon S3 (et non Amazon EFS).

Chaque AWS Transfer Family utilisateur fonctionne avec un modèle d'autorisation qui comprend :

1. Rôle IAM de base : définit les autorisations de base pour l'utilisateur
2. Politique de session facultative : restreint (étend vers le bas) les autorisations de base lors de l'exécution

Les autorisations effectives se situent à l'intersection des autorisations relatives au rôle de base et des autorisations liées à la politique de session. Les politiques de session ne peuvent que restreindre les autorisations ; elles ne peuvent pas accorder d'autorisations supplémentaires au-delà de ce que permet le rôle de base.

Cette architecture s'applique aux deux types d'utilisateurs :

- Service-managed utilisateurs - Les politiques de session peuvent être configurées directement dans les paramètres utilisateur
- Utilisateurs du fournisseur d'identité personnalisé : les politiques de session peuvent être renvoyées dans le cadre de la réponse d'authentification ou stockées dans AWS Secrets Manager

Deux approches de gestion des autorisations

Lorsque vous concevez des autorisations pour les utilisateurs de Transfer Family qui ont besoin de modèles d'accès uniques, vous pouvez choisir entre deux approches principales :

Un rôle par utilisateur

Créez un rôle IAM distinct pour chaque utilisateur de Transfer Family avec des autorisations spécifiques adaptées aux besoins de cet utilisateur. Utilisez cette approche lorsque :

- Chaque utilisateur a besoin d'autorisations très différentes
- L'administration des autorisations est gérée par différentes personnes au sein de votre organisation
- Vous avez besoin d'un contrôle précis de l'accès des utilisateurs individuels

Rôle partagé avec politiques de session

Utilisez un rôle IAM unique avec des autorisations étendues (telles que l'accès à un compartiment Amazon S3 complet contenant plusieurs répertoires personnels d'utilisateurs) et appliquez des politiques de session pour restreindre chaque utilisateur à sa zone spécifique. Cette approche réduit considérablement les frais administratifs par rapport à la gestion de rôles distincts pour chaque utilisateur. Utilisez cette approche lorsque :

- Les utilisateurs ont besoin de types d'accès similaires mais à des ressources différentes (par exemple, tous les utilisateurs doivent read/write avoir accès, mais chacun uniquement à son propre dossier)
- Vous souhaitez simplifier la gestion des rôles et éviter de créer des dizaines ou des centaines de rôles individuels
- Les utilisateurs ne doivent accéder qu'à leurs répertoires de base désignés dans un compartiment partagé
- L'administration des autorisations est centralisée au sein de votre organisation

Par exemple, au lieu de créer des rôles distincts pour les utilisateurs « alice », « bob » et « charlie », vous pouvez créer un rôle avec accès à l'ensemble du `s3://company-transfers/` bucket, puis utiliser des politiques de session pour restreindre alice à `s3://company-transfers/alice/`, bob à `s3://company-transfers/bob/`, etc.

Mise en œuvre des politiques de session

Les politiques de session fonctionnent en limitant les autorisations effectives du rôle IAM de base attribué à un utilisateur. Les autorisations finales se situent à l'intersection des autorisations du rôle et des autorisations de la politique de session.

Vous pouvez implémenter des politiques de session dynamiques de deux manières :

Substitution de variables

Utilisez les variables de politique Transfer Family telles que `${transfer:Username}${transfer:HomeDirectory}`, et `${transfer:HomeBucket}` dans les politiques de votre session. Ces variables sont automatiquement remplacées par les valeurs réelles lors de l'exécution. Pour plus d'informations sur ces variables, consultez [Création d'une politique de session pour un compartiment Amazon S3](#).

Génération dynamique

Pour les fournisseurs d'identité personnalisés, générez des politiques de session à la volée dans le cadre de la réponse d'authentification de votre fonction Lambda ou de votre méthode API Gateway. Cette approche vous permet de créer des politiques hautement personnalisées basées sur les attributs des utilisateurs, les appartenances à des groupes ou les sources de données externes au moment de l'authentification.

Vous pouvez également stocker des politiques de session prégénérées AWS Secrets Manager en incluant une clé nommée `Policy` avec la politique de session JSON comme valeur. Cela vous permet d'utiliser le même rôle IAM étendu pour plusieurs utilisateurs tout en conservant des contrôles d'accès spécifiques à l'utilisateur.

Note

Les politiques de session ne sont prises en charge que pour les transferts de fichiers vers et depuis Amazon S3. Ils ne s'appliquent pas aux systèmes de fichiers Amazon EFS. Pour Amazon EFS, les autorisations sont régies par le système de fichiers lui-même UID/GID et les bits d'autorisation sont appliqués dans celui-ci.

Implémentation par type d'utilisateur

Service-managed utilisateurs

Pour les utilisateurs gérés par des services, vous pouvez spécifier des politiques de session directement dans la configuration utilisateur via la AWS Transfer Family console, l'API ou la CLI. Pour de plus amples informations, veuillez consulter [Travailler avec des utilisateurs gérés par des services](#).

Utilisateurs du fournisseur d'identité personnalisé

Pour les utilisateurs de fournisseurs d'identité personnalisés, vous pouvez fournir des politiques de session de deux manières :

- AWS Secrets Manager En incluant une clé nommée `Policy` avec la politique de session comme valeur
- Directement dans la réponse de la fonction Lambda ou dans la réponse API Gateway dans le cadre du résultat de l'authentification

Pour de plus amples informations, veuillez consulter [Solution de fournisseur d'identité personnalisée](#).

Exemple : simplification de la gestion des rôles avec des politiques de session

Cet exemple montre comment la gestion dynamique des autorisations peut réduire considérablement les frais administratifs tout en préservant la sécurité.

Scénario

Votre organisation compte 50 utilisateurs qui ont besoin d'un accès SFTP pour transférer des fichiers. Chaque utilisateur ne doit accéder qu'à son propre dossier dans un compartiment Amazon S3 partagé appelé `company-transfers`. Sans politiques de session, vous devriez créer 50 rôles IAM distincts.

Approche traditionnelle (sans politiques de session)

- Créez 50 rôles IAM : `TransferRole-Alice`, `TransferRole-Bob`, `TransferRole-Charlie`, etc.
- Chaque rôle dispose d'autorisations spécifiques uniquement pour le dossier de cet utilisateur
- La gestion des autorisations nécessite la mise à jour des rôles individuels
- L'ajout de nouveaux utilisateurs nécessite la création de nouveaux rôles

Approche dynamique (avec politiques de session)

- Création d'un rôle IAM : `TransferRole-Shared` avec des autorisations étendues pour l'ensemble du bucket
- Utilisez les politiques de session pour limiter chaque utilisateur à son dossier spécifique au moment de l'exécution
- La gestion des autorisations nécessite la mise à jour d'un modèle de politique de rôle ou de session
- L'ajout de nouveaux utilisateurs ne nécessite aucun nouveau rôle, juste une configuration utilisateur

Mise en œuvre

Voici comment implémenter l'approche dynamique (en utilisant le `company-transfers` bucket comme exemple à remplacer par votre bucket Amazon S3 actuel) :

Pour implémenter la gestion dynamique des autorisations

1. Créez un rôle IAM partagé avec des autorisations Amazon S3 étendues :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers"
    }
  ]
}
```

2. Créez un modèle de politique de session qui restreint l'accès au dossier de l'utilisateur :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],

```

```
    "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
  },
  {
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::company-transfers",
    "Condition": {
      "StringLike": {
        "s3:prefix": "${transfer:Username}*"
      }
    }
  }
]
```

3. Configurez chaque utilisateur avec :

- Le rôle IAM partagé
- La politique de session s'appliquait comme suit :
 - Service-managed utilisateurs : utilisez l'API ou la CLI pour appliquer le JSON via le paramètre Policy lors de la création ou de la modification d'utilisateurs (la console propose uniquement des options de stratégie prédéfinies)
 - Utilisateurs du fournisseur d'identité personnalisé : renvoyez-le dans le cadre de la réponse de la fonction Lambda lors de l'authentification ou stockez-le AWS Secrets Manager sous forme de clé nommée « Policy » à côté des informations d'identification de l'utilisateur
- Répertoire personnel : /company-transfers/\${transfer:Username}/

AWS CloudTrail connexion 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.

- Cette rubrique traite de l'intégration avec CloudTrail un AWS service qui crée un enregistrement des actions entreprises au sein de votre Compte AWS. Il surveille et enregistre en permanence les opérations d'API pour des activités telles que les connexions à la console, AWS Command Line Interface les commandes et SDK/API les opérations. 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](#).
- [Amazon CloudWatch Logging pour les AWS Transfer Family serveurs](#) couvre l'intégration avec CloudWatch 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](#).

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 opérations de l'API publique. Ils n'apparaissent donc pas dans un ordre spécifique.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour AWS Transfer Family, créez un parcours. 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 enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les 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 faite avec les informations Gestion des identités et des accès AWS d'identification root ou utilisateur.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour 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](#)
- [Exemples de journaux d'accès aux données](#)

Activer la AWS CloudTrail journalisation

Vous pouvez surveiller les opérations AWS Transfer Family d'API à l'aide de AWS CloudTrail. En surveillant les opérations des API, vous pouvez obtenir des informations opérationnelles et de sécurité utiles. Si la [journalisation au niveau des objets Amazon S3 est activée](#), elle RoleSessionName est contenue dans le champ Demandeur sous [AWS:Role Unique Identifiant]/username.sessionid@server-id la forme. Pour plus d'informations sur les identifiants uniques de rôle Gestion des identités et des accès AWS (IAM), consultez la section Identifiants [uniques dans le guide](#) de l'Gestion des identités et des accès AWS utilisateur.

Important

La longueur maximale du RoleSessionName est de 64 caractères. S'il RoleSessionName est plus long, il est server-id tronqué.

Activation des événements de données Amazon S3

Pour suivre les opérations de fichiers effectuées AWS Transfer Family sur vos compartiments Amazon S3, vous devez activer les événements de données pour ces compartiments. Les événements de données fournissent une activité d'API au niveau de l'objet et sont particulièrement utiles pour suivre les chargements de fichiers, les téléchargements et les autres opérations effectuées par les utilisateurs. AWS Transfer Family

Pour activer les événements de données Amazon S3 pour votre AWS Transfer Family serveur :

1. Ouvrez la CloudTrail console à l'adresse <https://console.aws.amazon.com/cloudtrail/>.
2. Dans le volet de navigation, choisissez Sentiers, puis sélectionnez un parcours existant ou créez-en un nouveau.
3. Sous Événements liés aux données, sélectionnez Modifier.
4. Pour le type d'événement Data, sélectionnez S3.
5. Choisissez les compartiments Amazon S3 pour lesquels enregistrer les événements de données. Vous pouvez enregistrer les événements de données pour tous les compartiments ou spécifier des compartiments individuels.
6. Choisissez de consigner les événements de lecture, d'écriture ou les deux.
7. Sélectionnez Enregistrer les modifications.

Après avoir activé les événements de données, vous pouvez accéder à ces journaux dans le compartiment Amazon S3 configuré pour votre CloudTrail parcours. Les journaux incluent des informations telles que l'utilisateur qui a effectué l'action, l'horodatage de l'action, l'objet spécifique concerné et le `onBehalfOf` champ qui permet de suivre `userId` les actions effectuées. AWS Transfer Family

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'`CreateServer` action.

```
{
  "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"
}

```

Exemples de journaux d'accès aux données

Lorsque vous activez les événements de données Amazon S3 pour votre suivi CloudTrail, vous pouvez suivre les opérations sur les fichiers effectuées via AWS Transfer Family. Ces journaux vous aident à contrôler qui a accédé à quelles données, quand et comment.

Exemple d'entrée de journal pour un accès aux données réussi

L'exemple suivant montre une entrée de CloudTrail journal indiquant une opération de téléchargement de fichier réussie via AWS Transfer Family.

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:TransferSessionUser",
    "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/TransferSessionUser",
    "accountId": "123456789012",
    "accessKeyId": "ASIAEXAMPLEKEY",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
        "accountId": "123456789012",
        "userName": "TransferS3AccessRole"
      },
      "attributes": {
        "creationDate": "2025-07-15T16:12:05Z",
        "mfaAuthenticated": "true"
      }
    },
    "invokedBy": "transfer.amazonaws.com"
  },
  "eventTime": "2025-07-15T16:15:22Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "transfer.amazonaws.com",
  "userAgent": "transfer.amazonaws.com",
  "requestParameters": {
    "bucketName": "my-transfer-bucket",
    "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
    "Host": "my-transfer-bucket.s3.amazonaws.com",
    "x-amz-request-payer": "requester"
  },
  "responseElements": null,
  "additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "bytesTransferredIn": 0,
    "bytesTransferredOut": 2458732,
  }
}

```

```

    "x-amz-id-2":
"EXAMPLE123456789+abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ="
  },
  "requestID": "EXAMPLE123456789",
  "eventID": "example12-3456-7890-abcd-ef1234567890",
  "readOnly": true,
  "resources": [
    {
      "type": "AWS::S3::Object",
      "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-
report-2025-Q2.pdf"
    },
    {
      "accountId": "123456789012",
      "type": "AWS::S3::Bucket",
      "ARN": "arn:aws:s3:::my-transfer-bucket"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "123456789012",
  "eventCategory": "Data",
  "requestParameters": {
    "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
  }
}

```

Dans cet exemple, notez les champs importants suivants :

- `eventName`: indique l'opération d'API S3 qui a été effectuée (GetObject pour le téléchargement d'un fichier).
- `requestParameters.bucketName` et `requestParameters.key` : indique quel objet S3 a été consulté.
- `additionalEventData.bytesTransferredOut`: indique la taille du fichier téléchargé en octets.
- `requestParameters.x-amz-onBehalfOf`: contient le AWS Transfer Family nom d'utilisateur et l'identifiant de session, ce qui vous permet de savoir quel AWS Transfer Family utilisateur a effectué l'action.

Ce `x-amz-onBehalfOf` champ est particulièrement important car il relie l'appel de l'API S3 à l' AWS Transfer Family utilisateur spécifique qui a initié l'action. Ce champ suit le format `username.sessionid@server-id` suivant :

- `username` est le AWS Transfer Family nom d'utilisateur.
- `sessionid` est un identifiant unique pour la session de l'utilisateur.
- `server-id` est l'ID du AWS Transfer Family serveur.

Opérations communes d'accès aux données

Lorsque vous surveillez l'accès aux données via AWS Transfer Family, vous verrez généralement les opérations d'API S3 suivantes dans vos CloudTrail journaux :

Opérations S3 courantes dans les AWS Transfer Family journaux

Fonctionnement de l'API S3	AWS Transfer Family Action	Description
GetObject	Téléchargement du fichier	L'utilisateur a téléchargé un fichier depuis le serveur
PutObject	Chargement d'un fichier	L'utilisateur a chargé un fichier sur le serveur
DeleteObject	Suppression de fichiers	L'utilisateur a supprimé un fichier du serveur
ListObjects ou ListObjects V2	Liste des annuaires	Fichiers listés par l'utilisateur dans un répertoire
CopyObject	Copie de fichier	L'utilisateur a copié un fichier sur le serveur

En surveillant ces opérations dans vos CloudTrail journaux, vous pouvez suivre toutes les activités relatives aux fichiers effectuées via votre AWS Transfer Family serveur, ce qui vous aide à respecter les exigences de conformité et à détecter les accès non autorisés.

Amazon CloudWatch Logging pour les AWS Transfer Family serveurs

Amazon CloudWatch est un puissant service de surveillance et d'observabilité qui fournit une visibilité complète de vos AWS ressources, notamment AWS Transfer Family.

- **Real-time surveillance** : CloudWatch surveille les ressources et les applications de Transfer Family en temps réel, ce qui vous permet de suivre et d'analyser leurs performances.
- **Collecte de métriques** : CloudWatch collecte et suit diverses métriques pour vos ressources et applications, qui sont des variables que vous pouvez mesurer et utiliser à des fins d'analyse.
- **CloudWatch page d'accueil** : La page d'accueil de CloudWatch affiche automatiquement les statistiques relatives à Transfer Family et AWS aux autres services que vous utilisez, offrant ainsi une vue centralisée de vos données de surveillance.
- **Tableaux de bord personnalisés** : vous pouvez créer des tableaux de bord personnalisés CloudWatch pour afficher des indicateurs spécifiques à vos applications personnalisées et aux ressources que vous choisissez de surveiller.
- **Alarmes et notifications** : vous CloudWatch permet de créer des alarmes qui surveillent vos indicateurs et déclenchent des notifications ou des actions automatisées lorsque certains seuils sont dépassés. Cela peut être utile pour surveiller l'activité de transfert de fichiers sur vos serveurs Transfer Family et dimensionner les ressources en conséquence.
- **Optimisation des coûts** : vous pouvez utiliser les données collectées par CloudWatch pour identifier les ressources sous-utilisées et prendre des mesures, telles que l'arrêt ou la suppression d'instances, afin d'optimiser vos coûts.

Dans l'ensemble, ses fonctionnalités de surveillance complètes en CloudWatch font un outil précieux pour gérer et optimiser votre infrastructure Transfer Family et les applications qui y sont exécutées.

Les informations relatives à la CloudWatch connexion aux applications Web Transfer Family sont disponibles dans [CloudTrail enregistrement pour les applications Web Transfer Family](#).

Types de CloudWatch journalisation pour Transfer Family

Transfer Family propose deux méthodes pour enregistrer des événements sur CloudWatch :

- **Journalisation structurée JSON**

- Journalisation via un rôle de journalisation

Pour les serveurs Transfer Family, vous pouvez choisir le mécanisme de journalisation que vous préférez. Pour les connecteurs et les flux de travail, seuls les rôles de journalisation sont pris en charge.

Journalisation structurée JSON

Pour consigner les événements du serveur, nous vous recommandons d'utiliser la journalisation structurée JSON. Cela fournit un format de journalisation plus complet qui permet d'interroger les CloudWatch journaux. Pour ce type de journalisation, la politique IAM de l'utilisateur qui crée le serveur (ou modifie la configuration de journalisation du serveur) doit contenir les autorisations suivantes :

- `logs:CreateLogDelivery`
- `logs>DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

Voici un exemple de politique .

```
{
  "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": "*"
}
]
}

```

Pour plus de détails sur la configuration de la journalisation structurée JSON, consultez [Création, mise à jour et affichage de la journalisation pour les serveurs](#).

Rôle de journalisation

Pour consigner les événements d'un flux de travail géré attaché à un serveur, ainsi que pour les connecteurs, vous devez spécifier un rôle de journalisation. Pour définir l'accès, vous devez créer une politique IAM basée sur les ressources et un rôle IAM qui fournit ces informations d'accès. Voici un exemple de politique permettant de consigner Compte AWS les événements du serveur.

```

{
  "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/*"
    }
  ]
}

```

Pour plus de détails sur la configuration d'un rôle de journalisation pour consigner les événements du flux de travail, consultez [Gestion de la journalisation des flux de travail](#).

Création, mise à jour et affichage de la journalisation pour les serveurs

Pour tous les AWS Transfer Family serveurs, nous proposons une journalisation structurée. Nous vous recommandons d'utiliser une journalisation structurée pour tous les serveurs Transfer Family nouveaux et existants. Les avantages de l'utilisation de la journalisation structurée sont les suivants :

- Recevez les journaux au format JSON structuré.
- Interrogez vos journaux avec Amazon CloudWatch Logs Insights, qui découvre automatiquement les champs au format JSON.
- 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.

Pour activer la journalisation des flux de travail attachés à des serveurs, vous devez utiliser un rôle de journalisation.

Note

Lorsque vous ajoutez un rôle de journalisation, le groupe de journalisation existe toujours `/aws/transfer/your-serverID` et ne peut pas être modifié. Cela signifie qu'à moins que vous n'envoyiez les journaux de votre serveur structuré au même groupe, vous vous connecterez à deux groupes de journalisation distincts.

Si vous savez que vous allez associer un flux de travail à votre serveur et que vous devez donc ajouter un rôle de journalisation, vous pouvez configurer une journalisation structurée pour qu'elle se connecte au groupe de journaux par défaut de `/aws/transfer/your-serverID`.

Pour modifier votre groupe de journalisation, consultez [StructuredLogDestinations](#) la référence de l'AWS Transfer Family API.

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'opération `UpdateServer` API pour modifier votre configuration de journalisation. Pour en savoir plus, consultez [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'opération `CreateServer` ou de l'`UpdateServer` API, 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 journalisation JSON 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 journalisation JSON structurée via la console à tout moment.
- L'activation de la journalisation JSON 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 journalisation JSON structurée, vous ne pourrez pas la désactiver ultérieurement via la console.
- Si vous activez la journalisation JSON structurée, vous pouvez modifier à tout moment la destination du groupe de journaux via la console.
- Si vous activez la journalisation JSON structurée, vous ne pouvez pas modifier le rôle de journalisation via la console si vous avez activé les deux types de journalisation via l'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 l'API ou du SDK

- Si vous créez un nouveau serveur via l'API, vous pouvez configurer l'un ou les deux types de journalisation, ou choisir de ne pas enregistrer de journalisation.
- Pour les serveurs existants, activez et désactivez la journalisation JSON structurée à tout moment.
- Vous pouvez modifier le groupe de journaux via l'API à tout moment.
- Vous pouvez modifier le rôle de journalisation via l'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](#)
- [Mettre à jour la journalisation d'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

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](#).

Mettre à jour la journalisation d'un serveur

Les informations relatives à la journalisation dépendent du scénario de votre mise à jour.

Note

Lorsque vous optez pour la journalisation JSON 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 format JSON. 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 journalisation JSON 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





[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





 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 journalisation JSON 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 journalisation JSON 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 journalisation JSON structurée est activée.

Additional details
Edit

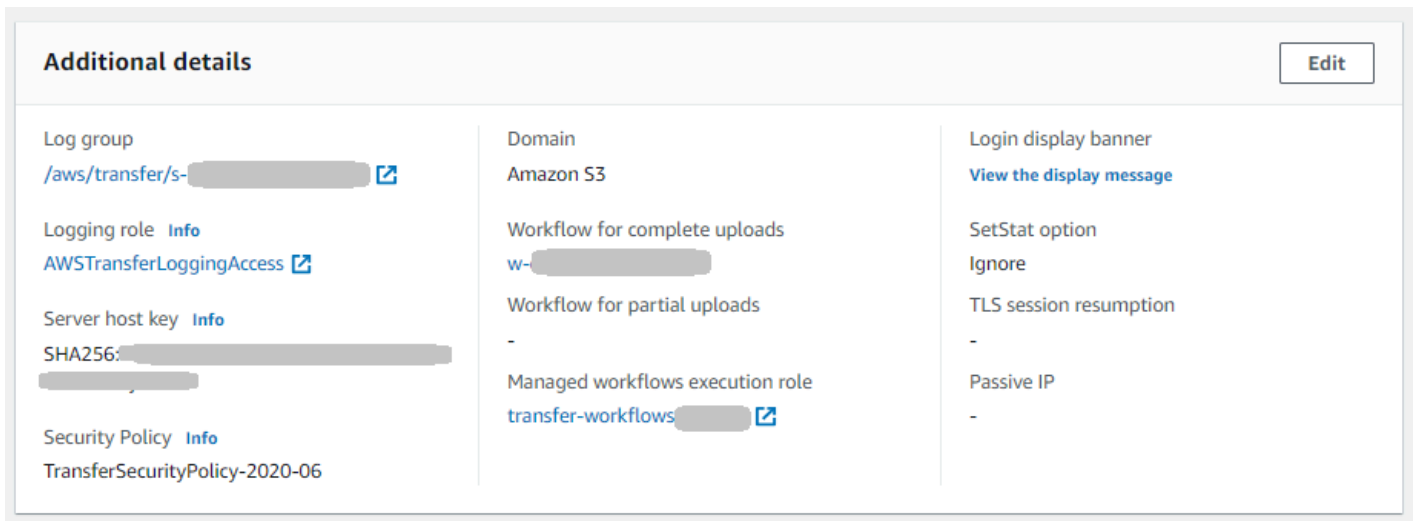
Log group /aws/transfer/s[redacted]	Domain Amazon S3	Login display banner View the display message
Logging role Info -	Workflow for complete uploads -	SetStat option Ignore
Server host key Info SHA256: [redacted]	Workflow for partial uploads -	TLS session resumption -
Security Policy Info TransferSecurityPolicy-2020-06	Managed workflows execution role -	Passive IP -

- Le rôle de journalisation est activé, mais la journalisation JSON structurée n'est pas activée.

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 journalisation JSON structurée) sont activés.



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 de CloudWatch métriques pour les serveurs 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 du protocole de transfert de fichiers (SFTP) Secure Shell (SSH).
- 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": "amzn-s3-demo-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":"amzn-s3-demo-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 politique IAM basée sur les ressources et un rôle IAM qui fournit ces informations d'accès.

Pour activer la CloudWatch journalisation Amazon, vous devez commencer par créer une politique IAM qui active la CloudWatch journalisation. Vous créez ensuite un rôle IAM 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 politiques IAM 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": "*"
    }
  ]
}
```

Dans l'exemple de politique précédent, pour le **Resource**, remplacez le *region-id* et *Compte AWS* par vos valeurs. Par exemple, **"Resource": "arn:aws::logs:us-east-1:11112223333:log-group:/aws/transfer/*"**

Vous créez ensuite un rôle et associez la politique de CloudWatch journalisation que vous avez créée.

Pour créer un rôle IAM et attacher une stratégie

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 rôle IAM. 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 CloudWatch Logs 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.

CloudWatch ×

Favorites and recents ▶

Dashboards

▶ Alarms 0 4 0

▼ Logs

Log groups

Logs Insights

▼ Metrics

All metrics

Explorer

Streams

▶ X-Ray traces

▶ Events

▶ Application monitoring

▶ Insights

Settings

Getting Started

CloudWatch > Log groups > /aws/transfer/s-

/aws/transfer/s- Actions View in Logs Insights Search log group

▼ Log group details

ARN
arn:aws:logs:us-east-2:5:log-group:/aws/transfer/s-.*

Creation time
2 years ago

Retention
Never expire

Stored bytes
39.39 MB

Metric filters
0

Subscription filters
0

Contributor Insights rules
-

Data protection - new
Inactive

Sensitive data found - new
-

KMS key ID
-

Log streams Metric filters Subscription filters Contributor Insights Tags Data protection - new

Log streams (10) [Refresh] [Delete] [Create log stream] [Search all log streams]

Q Filter log streams or try prefix search ☐ Exact match ☐ Show expired Info < 1 > [Settings]

☐	Log stream	Last event
☐	ERRORS	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-
☐	scooterstack4-	2023-

4. Vous pouvez sélectionner un flux de journal pour afficher les détails et les entrées individuelles du flux.
 - S'il existe une liste d'ERREURS, vous pouvez la sélectionner pour afficher le détail 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](#)

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](#)

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
2023-03-21T13:37:57.795-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
2023-03-21T14:12:02.850-04:00	{ "type": "StepStarted", "details": { "input": { "fileLocation": { "backingStore": "S3", "bucket": "...", "key": "decrypt-...
2023-03-21T14:12:03.464-04:00	{ "type": "StepCompleted", "details": { "output": {}, "stepType": "DECRYPT", "stepName": "decrypt-step", "workflowId": "w-...

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,
});
```

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 opérations de l'API Amazon S3 dans les journaux d'accès S3

Note

Cette section ne s'applique pas aux applications Web Transfer Family.

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 rôle IAM assumé pour gérer 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 rôle IAM appelé. `IamRoleName` Pour plus d'informations sur les identifiants uniques des rôles IAM, consultez la section [Identifiants uniques](#) du guide de l'Gestion des identités et des accès AWS 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 [Cross-service prévention confuse des adjoints](#).

Note

Dans les exemples suivants, remplacez chacune *user input placeholder* par vos propres informations.

Dans ces exemples, vous pouvez supprimer les détails de l'ARN d'un flux de travail si aucun flux de travail n'est associé à votre serveur.

L'exemple de logging/invoke politique 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": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

L'exemple de logging/invoke politique 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": "111122223333"
      },
      "ArnEquals": {
        "aws:SourceArn": [
          "arn:aws:transfer:us-west-2:111122223333:server/server-id",
          "arn:aws:transfer:us-west-2:111122223333: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 du journal pour les SFTP/FTP/FTPS actions Transfer Family, dans le nouveau format de journal structuré JSON.

Champ	Description	Exemple d'entrée
type d'activité	L'action de l'utilisateur	Les types d'activités disponibles sont les suivants : AUTH_FAILURE CONNECTED ,DISCONNECTED ,,ERROR,EXIT_REAS

Champ	Description	Exemple d'entrée
		ON ,CLOSE,CREATE_SY MLINK ,DELETE,MKDIR,OPEN,PARTIA LOSE ,RENAME,RMDIR,SETSTAT,TLS_ E_FAILURE .
octets entrants	Nombre d'octets téléchargés par l'utilisateur	29238420042
octets sortants	Nombre d'octets téléchargés par l'utilisateur	23094032490328
ciphers	Spécifie le chiffrement SSH négocié pour la connexion (les chiffrements disponibles sont répertoriés dans) Algorithmes cryptographiques	aes256-gcm@openssh.com
client	Le logiciel client de l'utilisateur	SSH-2.0-OpenSSH_7,4
home-dir	Le répertoire sur lequel l'utilisateur final atterrit lorsqu'il se connecte au point de terminaison si son type de répertoire de PATH base est : s'il possède un répertoire de base logique, cette valeur est toujours /	/user-home- bucket/test
kex	Spécifie l'échange de clés SSH (KEX) négocié pour la connexion (les KEX disponibles sont répertoriés dans) Algorithmes cryptographiques	diffie-hellman-group14-sha256
message	Fournit des informations supplémentaires relatives à l'erreur	<string>

Champ	Description	Exemple d'entrée
méthode	La méthode d'authentification	publickey
mode	Spécifie la manière dont un client ouvre un fichier	CRÉER TRONQUER ÉCRIRE
fonctionnement	L'opération du client sur un fichier	OUVRIR FERMER
path	Chemin de fichier réel affecté	/amzn-s3-demo- -file-1.pdf bucket/test
clé publique SSH	Le corps de la clé publique pour l'utilisateur qui se connecte	AAAAC3NzaC1lZDI1NT E5AAAAIA9OY0qV6XYV HaaOiWAcj2spDJVbgj rqDPY4pxd6GnHl
empreinte digitale de clé publique SSH	L'empreinte de la clé publique, telle qu'elle apparaît dans la console pour les utilisateurs gérés par le service lors de la liste de leurs clés utilisateur.	SHA256:BY3gNMHwTfj d4n2VuT4pTyLOk82zW Zj4KEYEu7y4r/0

 Note

Dans la console, l'empreinte digitale est affichée avec les caractères de remplissage (le cas échéant) : de 0 à 3 signes égaux (=) à la fin. Dans l'entrée du journal, ce rembourrage est supprimé de la sortie.

Champ	Description	Exemple d'entrée
type de clé publique SSH	Type de clé publique : Transfer Family prend en charge le RSA-, l'ECDSA- et les clés ED25519-formatted	ssh-ed25519
source de ressources	Identifiant unique attribué par le système pour une ressource spécifique (par exemple, un serveur)	arn:aws:transfer:ap-northeast-1:12346789012 : -1234567890akeu2js2 server/s
rôle	Le rôle IAM de l'utilisateur	arn:aws:iam : :0293883675 : -role role/testuser
session-id	Identifiant unique attribué par le système pour une seule session	9ca9a0e1cec6ad9d
adresse IP source	Adresses IP client	18,323,0,129
user	Le nom d'utilisateur de l'utilisateur final	myname192
politique utilisateur	Les autorisations spécifiées pour l'utilisateur final : ce champ est renseigné si la politique de l'utilisateur est une politique de session.	Le code JSON pour la politique de session utilisée

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 +b7 +A +HXG0C7L1JIZ0" SourceIP=3.8.172.211 SHA256:Lfz3R2nmLY4raK Rb1rSvUIbAE
COPY/TAG/DELETE/DECRYPT flux de travail	{ "type" : "StepStarted", "details" : { "input" : { "FileLocation" : { "BackingStore" : "EFS", "FileSystemID" : "fs-12345678", "path" : "/lhr/regex.py" }, "StepType" : "COPY/TAG", "StepName" : "successful_tag_step", "WorkflowID" : "w-1111aaaa2222bbbb3", "ID d'exécution" : "81234abcd-1234-efgh-5678-ijklmnopqr90", "TransferDetails" : { "serverID" : "s-1234abcd5678efghi", "nom d'utilisateur" : "lhr", "ID de session" : "1234567890abcdef0" } } }
Flux de travail par étapes personnalisé	{ "type" : "CustomStepInvoked", "details" : { "output" : { "token" : "CustomStepInvoked", "StepType" : "CUSTOM", "StepName" : "2.1.efs-s3_copy_2", "MzM4Mjg5YWUtYTEzMy00YjIzLWI3OGMtYzU4OGI2ZjQyMzE5", "WorkflowId" : "1_w-9283e49d33297c3f7", "ExecutionID" : "2.1.1234abcd-1234-efgh-5678-ijklmnopqr90", "TransferDetails" : { "serverID" : "s-zzzz1111aaaa22223", "nom d'utilisateur" : "lhr", "ID de session" : "1234567890abcdef0" } } }
Suppressions	lhr.33a8fb495ffb383b SUPPRIMER LE CHEMIN=/ /123.jpg bucket/user

Action	Journaux correspondants dans Amazon CloudWatch Logs
Téléchargements	lhr.33a8fb495ffb383b CHEMIN OUVERT =/ /123.jpg MODE=LIRE bucket/user llhr.33a8fb495ffb383b FERMER LE CHEMIN=/ /123.jpg =3618546 bucket/user BytesOut
Logins/Logouts	user.914984e553bcddb6 CONNECTED SourceIP=1.22.111.222 User=LHR =LOGICAL Client= _7.4 Role=ARN:AWS : :iam : :12345678 9012 : -s3-access HomeDir SSH-2.0-OpenSSH role/sftp user.914984e553bcddb6 DÉCONNECTÉ
Renomme	lhr.33a8fb495ffb383b RENOMMER LE CHEMIN=/ /lambo.png =/ /ferrari.png bucket/us er NewPath bucket/user
Exemple de journal des erreurs du flux de travail	<pre>{ "type" : "StepErrored", "details" : { "ErrorType" : "BAD_REQUEST", "ErrorMessage" : "Impossible de baliser le fichier Efs", "StepType" : "Successfull", "StepName" : "successful_tag_step", "ExecutionID" : "81234abcd-1234-efghi-5678-ijklmnopqr90", "TransferDetails" : { "serverID" : "s-1234abcd5678efghi", "nom d'utilisateur" : "lhr", "ID de session" : "?1234567890abcdef0" } } }</pre>
Liens symboliques	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs- /pqr.jpg =abc.jpg LinkPath 12345678/lhr TargetPath

Action	Journaux correspondants dans Amazon CloudWatch Logs
Chargements	lhr.33a8fb495ffb383b OPEN Path=/ /123.jpg MODE=Créer Truncate Écrire bucket/user lhr.33a8fb495ffb383b FERMER LE CHEMIN=/ /123.jpg =3618546 bucket/user BytesIn
Flux de travail	<pre>{ "type": "ExecutionStarted", "details": { "input": { "initial": { "BackingStore": "EFS", "FileSystemID": "fs-12345678", "FileLocation": { "path": "/lhr/regex.py" } }, "WorkflowID": "w-1111aaaa2222bbbb3", "ExecutionID": "1234abcd-1234-efgh-568-78-ijklmnopqr90", "TransferDetails": { "serverID": "s-zzzz1111aaaa22223", "nom d'utilisateur": "lhr", "ID de session": "1234567890abcdef0" } } } }</pre> <pre>{ "type": "StepStarted", "details": { "input": { "Emplacement du fichier": { "BackingStore": "EFS", "FileSystemID": "fs-12345678", "path": "/lhr/regex.py" }, "StepType": "efs-s3_copy_2", "WorkflowID": "w-9283e49Ed33297c3f7", "ID d'exécution": "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 connecteurs SFTP](#)
- [Exemples d'entrées de journal pour les connecteurs VPC Lattice](#)
- [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 utilisateur SFTP se connecte à un serveur Transfer Family, télécharge un fichier, puis se déconnecte de la session.

L'entrée de journal suivante indique qu'un utilisateur SFTP se connecte à un serveur Transfer Family.

```
{
  "role": "arn:aws:iam::500655546075:role/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": "/test/log-me",
  "ssh-public-key":
"AAAAC3NzaC1lZDI1NTE5AAAAIA90Y0qV6XYVHaa0iWAcj2spDJVbgjrQDPY4pxd6GnH1",
  "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyL0k82zWZj4KEYEu7y4r/0",
  "ssh-public-key-type": "ssh-ed25519",
  "user": "log-me",
  "kex": "ecdh-sha2-nistp256",
  "session-id": "9ca9a0e1cec6ad9d"
}
```

L'entrée de journal suivante indique que l'utilisateur SFTP télécharge un fichier dans son compartiment Amazon S3.

```
{
  "mode": "CREATE|TRUNCATE|WRITE",
  "path": "/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'utilisateur SFTP s'est déconnecté de sa session SFTP. Tout d'abord, le client ferme la connexion au bucket, puis il déconnecte la session SFTP.

```
{
  "path": "/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"
}
```

Note

Les types d'activités disponibles sont les suivants :

AUTH_FAILURE, RECONNECTED, DISCONNECTED, ERROR, EXIT_REASON, CLOSE, CREATE_SYMLINK, DELETE

Exemples d'entrées de journal pour les connecteurs SFTP

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 connecteur SFTP. Les entrées de journal pour les connecteurs SFTP sont générées lorsque vous exécutez une `StartDirectoryListing` commande `StartFileTransfer` ou.

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:account-id:connector/connector-id",
"local-directory-path": "/connectors-localbucket",
"bytes": 514,
"egress-type": "SERVICE_MANAGED"
}

```

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:account-id:connector/connector-id",
  "local-directory-path": "/connectors-localbucket",
  "egress-type": "SERVICE_MANAGED"
}

```

Cette entrée de journal concerne une opération SEND réussie.

```

{
  "operation": "SEND",
  "timestamp": "2024-04-24T18:16:12.513207284Z",
  "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": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-east-1-2024-01-02.csv",
    "status-code": "COMPLETED",
    "start-time": "2024-04-24T18:16:12.295235884Z",
    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "bytes": 275,
    "egress-type": "SERVICE_MANAGED"
  }

```

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 une seule opération d'`start-file-transfer` API, 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 connecteurs VPC Lattice

Cette section contient des exemples de journaux pour les connecteurs VPC Lattice. Pour les connecteurs VPC Lattice, les journaux incluent des champs supplémentaires qui fournissent des informations sur la configuration du connecteur et la configuration du réseau.

Cette entrée de journal concerne une opération SEND du connecteur VPC Lattice qui s'est terminée avec succès.

```

{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-east-1-2025-03-22.csv"",
  "status-code": "COMPLETED",

```

```

"start-time": "2025-09-05T14:20:19.434072509Z",
"end-time": "2025-09-05T14:20:19.481453346Z",
"account-id": "account-id",
"connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
"remote-directory-path": "/test-bucket/test-folder/",
"bytes": 262,
"egress-type": "VPC_LATTICE",
"vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/resource-configuration-arn-id",
"vpc-lattice-port-number": 22
}

```

Les journaux du connecteur VPC Lattice incluent les champs supplémentaires suivants :

- `egress-type`- Type de configuration de sortie pour le connecteur
- `vpc-lattice-resource-configuration-arn`- ARN de la configuration des ressources du réseau VPC qui définit l'emplacement du serveur SFTP cible
- `vpc-lattice-port-number`- Numéro de port pour la connexion au serveur SFTP via VPC Lattice

Exemples d'entrées de journal pour les défaillances de l'algorithme d'échange de clés

Cette section contient des exemples de journaux où l'algorithme d'échange de clés (KEX) a échoué. Voici des exemples tirés du flux de journaux ERRORS 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 non-concordance KEX.

```
{
  "activity-type": "KEX_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-99999999999999999999",
  "message": "no matching key exchange method found",
  "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}
```

Utilisation de CloudWatch métriques pour les serveurs 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.

Namespace	Métrique	Description
AWS/Transfer	BytesIn	Nombre total d'octets transférés vers le serveur. Critères d'établissement de rapports : Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis.

Namespace	Métrique	Description
		Pour AS2 : lorsque le client reçoit un message sur son serveur AS2 et émis dès que le traitement du message entrant est terminé Unités : nombre Durée : 5 minutes
	BytesOut	Nombre total d'octets transférés hors du serveur. Critères d'établissement de rapports : - Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis. - Pour AS2 : lorsque le client appelle <code>StartFile Transfer</code> depuis son connecteur AS2 et qu'il est émis dès que le traitement du message sortant est terminé. Unités : nombre Durée : 5 minutes

Namespace	Métrique	Description
	FilesIn	Le nombre total de fichiers transférés sur le serveur. Pour les serveurs utilisant le protocole AS2, cette métrique représente le nombre de messages reçus. Critères d'établissement de rapports : • Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis. • Pour AS2 : lorsque le client reçoit un message sur son serveur AS2 et qu'il est émis dès que le traitement du message entrant est terminé. Unités : nombre Durée : 5 minutes
	FilesOut	Le nombre total de fichiers transférés hors du serveur. Critères d'établissement de rapports : • Pour SFTP/FTP/FTPS : émis toutes les 5 minutes lorsqu'une connexion est établie avec le serveur Transfer Family. Si aucun fichier ou octet n'est transféré pendant la période, « 0 » est émis. • Pour AS2 : lorsque le client appelle <code>StartFile Transfer</code> depuis son connecteur AS2 et qu'il est émis dès que le traitement du message sortant est terminé. Unités : nombre Durée : 5 minutes

Namespace	Métrique	Description
	InboundMessage	Nombre total de messages AS2 reçus avec succès d'un partenaire commercial. Critères de signalement : lorsque le client reçoit un message sur son serveur AS2 et qu'il est émis dès que le traitement du message entrant est terminé avec succès Unités : nombre Durée : 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. Critères de signalement : lorsque le client reçoit un message sur son serveur AS2 et qu'il est émis dès que le traitement du message entrant s'est terminé sans succès Unités : nombre Durée : 5 minutes
	OnUploadExecutionsStarted	Nombre total d'exécutions de flux de travail démarrées sur le serveur. Critères de reporting : déclenché chaque fois qu'une exécution commence Unités : nombre Durée : 1 minute

Namespace	Métrique	Description
	OnUploadExecutionsSuccess	Nombre total d'exécutions de flux de travail réussies sur le serveur. Critères de reporting : déclenché chaque fois qu'une exécution se termine avec succès Unités : nombre Durée : 1 minute
	OnUploadExecutionsFailed	Nombre total d'exécutions de flux de travail infructueuses sur le serveur. Critères de reporting : déclenché chaque fois qu'une exécution échoue Unités : nombre Durée : 1 minute
	OutboundMessage	Nombre total de messages AS2 envoyés avec succès à un partenaire commercial. Critères de signalement : lorsque le client appelle <code>StartFileTransfer</code> depuis son connecteur AS2 et qu'il est émis dès que le message sortant a été traité avec succès Unités : nombre Durée : 5 minutes

Namespace	Métrique	Description
	OutboundFailedMessage	Nombre total de messages AS2 envoyés sans succès à un partenaire commercial. Critères de signalement : lorsque le client appelle <code>StartFileTransfer</code> depuis son connecteur AS2 et qu'il est émis dès que le traitement du message sortant s'est terminé sans succès Unités : nombre Durée : 5 minutes

Dimensions de Transfer Family

Une dimension est une name/value paire 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 les CloudWatch dimensions de Transfer Family.

Dimension	Description
ServerId	L'identifiant unique du serveur.
ConnectorId	L'identifiant unique du connecteur. Utilisé pour AS2, pour et OutboundMessage OutboundFailedMessage

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 par email, via des notifications de chat [Amazon Q Developer dans les applications de chat](#) ou via des notifications push de l'[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.

Utilisation de requêtes pour filtrer les entrées du journal

Vous pouvez utiliser CloudWatch des requêtes pour filtrer et identifier les entrées du journal pour Transfer Family. Cette section contient quelques exemples.

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Vous pouvez créer des requêtes ou des règles.
 - Pour créer une requête Logs Insights, choisissez Logs Insights dans le panneau de navigation de gauche, puis entrez les détails de votre requête.
 - Pour créer une règle Contributor Insights, choisissez Insights > Contributor Insights dans le panneau de navigation de gauche, puis entrez les détails de votre règle.
3. Exécutez la requête ou la règle que vous avez créée.

Afficher les principaux contributeurs aux échecs d'authentification

Dans vos journaux structurés, une entrée du journal des échecs d'authentification ressemble à ce qui suit :

```
{
  "method": "password",
  "activity-type": "AUTH_FAILURE",
  "source-ip": "999.999.999.999",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "message": "Invalid user name or password",
  "user": "exampleUser"
```

```
}
```

Exécutez la requête suivante pour connaître les principaux responsables des échecs d'authentification.

```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10
```

Plutôt que d'utiliser CloudWatch Logs Insights, vous pouvez créer une règle CloudWatch Contributors Insights pour visualiser les échecs d'authentification. Créez une règle similaire à la suivante.

```
{
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "$.activity-type",
        "In": [
          "AUTH_FAILURE"
        ]
      }
    ],
    "Keys": [
      "$.user"
    ]
  },
  "LogFormat": "JSON",
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "LogGroupARNs": [
    "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
  ]
}
```

Afficher les entrées du journal où un fichier a été ouvert

Dans vos journaux structurés, une entrée du journal de lecture d'un fichier ressemble à ce qui suit :

```
{
  "mode": "READ",
  "path": "/fs-0df669c89d9bf7f45/avtester/example",
  "activity-type": "OPEN",
  "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "session-id": "0049cd844c7536c06a89"
}
```

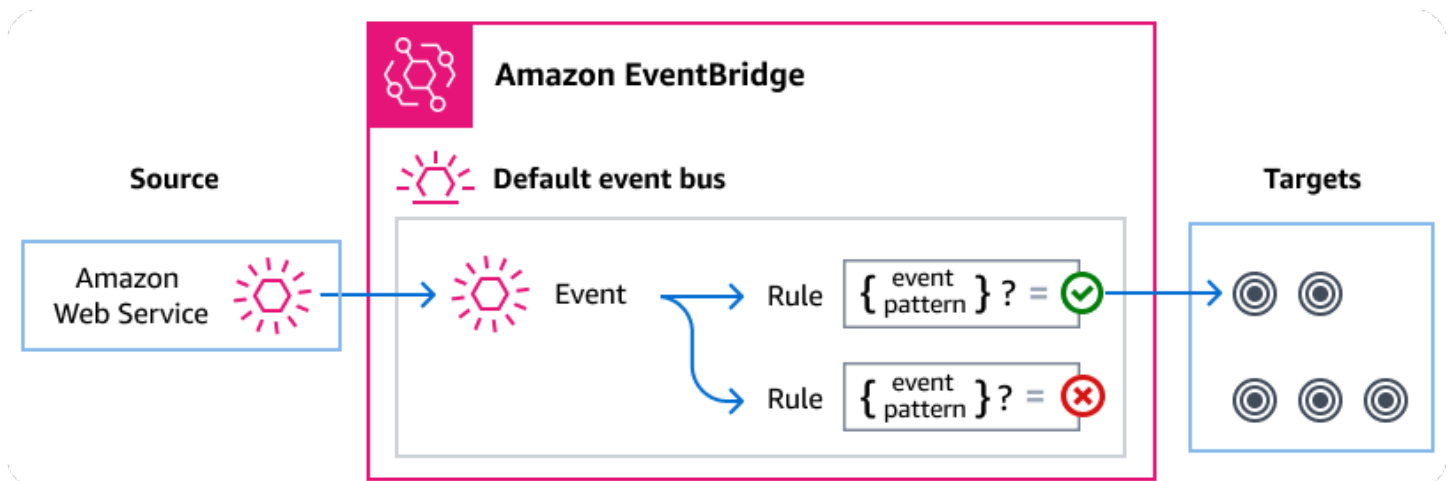
Exécutez la requête suivante pour afficher les entrées du journal indiquant qu'un fichier a été ouvert.

```
filter `activity-type` = 'OPEN'
| display @timestamp, @logStream, `session-id`, mode, path
```


Gestion Transfer Family événements utilisant 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. Event-driven L'architecture est un style de construction de systèmes logiciels faiblement couplés qui fonctionnent ensemble en émettant des événements et en y répondant. Les événements représentent une modification d'une ressource ou d'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'événement de la règle. Si l'événement correspond, le bus d'événements envoie l'événement à une ou plusieurs cibles spécifiées.



Rubriques

- [Transfer Family events](#)
- [Envoi Transfer Family événements en utilisant EventBridge rules](#)
- [Amazon EventBridge des autorisations](#)
- [Additionnel EventBridge resources](#)
- [Transfer Family référence détaillée des événements](#)

Transfer Family events

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 le meilleur des cas ou de manière durable (notez que certains événements peuvent être livrés dans le mauvais ordre). Ces niveaux de livraison sont décrits dans [Niveau de livraison pour les événements de AWS service](#) dans Amazon EventBridge Events Reference.

- Server-level les événements pour les serveurs SFTP, FTPS et FTP sont fournis dans la mesure du possible.
- Les événements du connecteur SFTP sont fournis de manière durable.
- Les événements AS2 sont organisés sur une base durable.

Les événements suivants sont générés par Transfer Family. Pour plus d'informations, consultez les [EventBridge événements](#) dans le guide de Amazon EventBridge l'utilisateur.

Événements relatifs aux serveurs SFTP, FTPS et FTP

Les tableaux suivants répertorient les événements pour les serveurs SFTP, FTPS et FTP, organisés par type d'événement.

Événements relatifs au chargement et au téléchargement de fichiers

Type de détail d'événement	Description
Téléchargement du fichier du serveur FTP terminé	Un fichier a été téléchargé avec succès pour le protocole FTP.
Échec du téléchargement du fichier du serveur FTP	Une tentative de téléchargement de fichier a échoué pour le protocole FTP.
Téléchargement du fichier sur le serveur FTP terminé	Un fichier a été chargé avec succès pour le protocole FTP.

Type de détail d'événement	Description
<u>Échec du téléchargement du fichier sur le serveur FTP</u>	Une tentative de téléchargement de fichier a échoué pour le protocole FTP.
<u>Téléchargement du fichier du serveur FTPS terminé</u>	Un fichier a été téléchargé avec succès pour le protocole FTPS.
<u>Échec du téléchargement du fichier du serveur FTPS</u>	Une tentative de téléchargement de fichier a échoué pour le protocole FTPS.
<u>Téléchargement du fichier du serveur FTPS terminé</u>	Un fichier a été chargé avec succès pour le protocole FTPS.
<u>Échec du téléchargement du fichier sur le serveur FTPS</u>	Une tentative de téléchargement de fichier a échoué pour le protocole FTPS.
<u>Téléchargement du fichier du serveur SFTP terminé</u>	Un fichier a été téléchargé avec succès pour le protocole SFTP.
<u>Échec du téléchargement du fichier du serveur SFTP</u>	Une tentative de téléchargement de fichier a échoué pour le protocole SFTP.
<u>Téléchargement du fichier du serveur SFTP terminé</u>	Un fichier a été chargé avec succès pour le protocole SFTP.
<u>Échec du téléchargement du fichier sur le serveur SFTP</u>	Une tentative de téléchargement de fichier a échoué pour le protocole SFTP.

Autres événements liés aux opérations sur les fichiers

Type de détail d'événement	Description
<u>Création du répertoire du serveur FTP terminée</u>	Un répertoire a été créé avec succès pour le protocole FTP.
<u>La création du répertoire du serveur FTP a échoué</u>	Une tentative de création d'un répertoire a échoué pour le protocole FTP.

Type de détail d'événement	Description
<u>Suppression du répertoire du serveur FTP terminée</u>	Un répertoire a été supprimé avec succès pour le protocole FTP.
<u>La suppression du répertoire du serveur FTP a échoué</u>	Une tentative de suppression d'un répertoire a échoué pour le protocole FTP.
<u>Suppression du fichier du serveur FTP terminée</u>	Un fichier a été supprimé avec succès pour le protocole FTP.
<u>Échec de la suppression du fichier du serveur FTP</u>	Une tentative de suppression d'un fichier a échoué pour le protocole FTP.
<u>Renommage du fichier du serveur FTP terminé</u>	Un fichier a été renommé avec succès pour le protocole FTP.
<u>Échec du renommage du fichier du serveur FTP</u>	Une tentative de renommer un fichier a échoué pour le protocole FTP.
<u>Création du répertoire du serveur FTPS terminée</u>	Un répertoire a été créé avec succès pour le protocole FTPS.
<u>La création du répertoire du serveur FTPS a échoué</u>	Une tentative de création d'un répertoire a échoué pour le protocole FTPS.
<u>Suppression du répertoire du serveur FTPS terminée</u>	Un répertoire a été supprimé avec succès pour le protocole FTPS.
<u>La suppression du répertoire du serveur FTPS a échoué</u>	Une tentative de suppression d'un répertoire a échoué pour le protocole FTPS.
<u>Suppression du fichier du serveur FTPS terminée</u>	Un fichier a été supprimé avec succès pour le protocole FTPS.
<u>La suppression du fichier du serveur FTPS a échoué</u>	Une tentative de suppression de fichier a échoué pour le protocole FTPS.
<u>Renommage du fichier du serveur FTPS terminé</u>	Un fichier a été renommé avec succès pour le protocole FTPS.

Type de détail d'événement	Description
Échec du renommage du fichier du serveur FTPS	Une tentative de renommer un fichier a échoué pour le protocole FTPS.
Création du répertoire du serveur SFTP terminée	Un répertoire a été créé avec succès pour le protocole SFTP.
La création du répertoire du serveur SFTP a échoué	Une tentative de création d'un répertoire a échoué pour le protocole SFTP.
Suppression du répertoire du serveur SFTP terminée	Un répertoire a été supprimé avec succès pour le protocole SFTP.
La suppression du répertoire du serveur SFTP a échoué	Une tentative de suppression d'un répertoire a échoué pour le protocole SFTP.
Suppression du fichier du serveur SFTP terminée	Un fichier a été supprimé avec succès pour le protocole SFTP.
Echec de la suppression du fichier du serveur SFTP	Une tentative de suppression de fichier a échoué pour le protocole SFTP.
Renommage du fichier du serveur SFTP terminé	Un fichier a été renommé avec succès pour le protocole SFTP.
Échec du renommage du fichier du serveur SFTP	Une tentative de renommer un fichier a échoué pour le protocole SFTP.

Événements relatifs au connecteur SFTP

Note

Ces événements sont diffusés à un EventBridge niveau durable, comme décrit dans la section [Niveau de livraison pour les événements de AWS service](#) dans Amazon EventBridge Events Reference.

Type de détail d'événement	Description
Envoi du fichier du connecteur SFTP terminé	Un transfert de fichier d'un connecteur vers un serveur SFTP distant s'est terminé avec succès.
Échec de l'envoi du fichier du connecteur SFTP	Un transfert de fichier d'un connecteur vers un serveur SFTP distant a échoué.
Récupération du fichier du connecteur SFTP terminée	Un transfert de fichier d'un serveur SFTP distant vers un connecteur s'est terminé avec succès.
Échec de la récupération du fichier du connecteur SFTP	Un transfert de fichier d'un serveur SFTP distant vers un connecteur a échoué.
La liste des répertoires du connecteur SFTP est terminée	Un appel de liste du répertoire de fichiers de démarrage qui s'est terminé avec succès.
Échec de la liste des répertoires du connecteur SFTP	Une liste de répertoires de fichiers de démarrage qui a échoué.
Déplacement à distance du connecteur SFTP terminé	Les fichiers ou les répertoires ont été déplacés ou renommés avec succès sur le serveur distant.
Échec du déplacement à distance du connecteur SFTP	Les fichiers ou les répertoires n'ont pas pu être déplacés ou renommés sur le serveur distant.
Suppression à distance du connecteur SFTP terminée	Les fichiers ou les répertoires ont été correctement supprimés sur le serveur distant.
Échec de la suppression à distance du connecteur SFTP	Les fichiers ou les répertoires n'ont pas pu être supprimés sur le serveur distant.

Événements AS2

Note

Ces événements sont diffusés à un EventBridge niveau durable, comme décrit dans la section [Niveau de livraison pour les événements de AWS service](#) dans Amazon EventBridge Events Reference.

Type de détail d'événement	Description
Réception de la charge utile AS2 terminée	La charge utile d'un message AS2 a été reçue.
Échec de réception de la charge utile AS2	La charge utile d'un message AS2 n'a pas été reçue.
Envoi de la charge utile AS2 terminé	La charge utile d'un message AS2 a été envoyée avec succès.
Échec de l'envoi de la charge utile AS2	La charge utile d'un message AS2 n'a pas pu être envoyée.
Réception AS2 MDN terminée	La notification de disposition d'un message AS2 a été reçue.
Échec de la réception MDN AS2	La notification de disposition d'un message AS2 n'a pas été reçue.
Envoi MDN AS2 terminé	La notification de disposition d'un message AS2 a été envoyée avec succès.
Échec de l'envoi MDN AS2	La notification de disposition d'un message AS2 n'a pas pu être envoyée.

Envoi Transfer Family événements en utilisant EventBridge rules

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.

Pour capturer AWS Transfer Family événements sur Amazon EventBridge

1. Connectez-vous à la EventBridge console Amazon AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/events/>.
2. Dans le volet de navigation, choisissez Rules, puis Create rule.
3. Entrez un nom descriptif pour la règle, et entrez éventuellement une description.
4. Pour Type de règle, sélectionnez Règle avec un modèle d'événement, puis cliquez sur Suivant.
5. Dans la section Source de l'événement, sélectionnez AWS des événements ou des événements EventBridge partenaires.
6. Dans la section Méthode de création, choisissez Utiliser le formulaire de modèle.
7. Dans la section Modèle d'événement, fournissez les informations suivantes.
 - a. Pour Source d'événement, choisissez Services AWS .
 - b. Pour le AWS service, choisissez Transfer.
 - c. Dans Type d'événement, choisissez le type d'événement Transfer Family pour lequel vous souhaitez déclencher votre règle.

Selon le type d'événement que vous avez sélectionné, une section Spécification du type d'événement 1 peut vous être présentée.

- d. Si vous voyez la section Spécification du type d'événement 1, sélectionnez les événements spécifiques que vous souhaitez capturer (ou sélectionnez N'importe quel événement pour capturer tous les événements correspondant au type d'événement sélectionné).
 - e. (Facultatif) Utilisez l'éditeur de modèles d'événements pour définir des filtres pour les détails des événements.
 - f. Choisissez Suivant.
8. Choisissez une cible parmi les choix disponibles dans Sélectionner des cibles. Choisissez parmi les cibles disponibles suivantes.
 - AWS service. Les options les plus populaires sont les fonctions Lambda pour le calcul sans serveur, les files d'attente Amazon SQS pour le traitement des messages, les rubriques

Amazon SNS pour les notifications et pour l'orchestration des flux de travail. AWS Step Functions

- EventBridge Destination de l'API. Si vous souhaitez envoyer des événements à un point de terminaison HTTP en dehors de AWS, vous pouvez utiliser une destination d'API comme cible.
- EventBridge bus événementiel. Vous pouvez envoyer des événements vers un autre bus d'événements, soit dans le même compte et dans la même région, soit dans un compte ou une région différents.

Pour obtenir des instructions complètes sur la création de règles de bus d'événements, consultez la section [Création de règles qui réagissent aux événements](#) dans le guide de EventBridge l'utilisateur Amazon.

Pour obtenir de l'aide sur la sélection d'une cible, consultez la section [Sélectionner des cibles](#) dans le guide de EventBridge l'utilisateur Amazon.

9. Configurez toutes les options supplémentaires pour votre cible, puis choisissez Next.
10. (Facultatif) Ajoutez des balises à votre règle et choisissez Next.
11. Dans l'écran Réviser et créer, si tout semble correct, choisissez Créer une règle.

Création de modèles d'événements pour Transfer Family events

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 objet JSON 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 rechercher.

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 connecteur SFTP :

```
{
  "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 téléchargements SFTP 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'événements pour Transfer Family événements à 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 des 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.

Additionnel EventBridge resources

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 les autres destinations auxquels 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 Server File 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

- [Événements relatifs aux serveurs SFTP, FTPS et FTP](#)
- [Événements relatifs au connecteur SFTP](#)
- [Événements AS2](#)

Événements relatifs aux serveurs SFTP, FTPS et FTP

Les champs de détail relatifs aux événements des serveurs SFTP, FTPS et FTP sont les suivants :

- Création du répertoire du serveur FTP terminée
- La création du répertoire du serveur FTP a échoué
- Suppression du répertoire du serveur FTP terminée
- La suppression du répertoire du serveur FTP a échoué
- Suppression du fichier du serveur FTP terminée

- Echec de la suppression du fichier du serveur FTP
- Téléchargement du fichier du serveur FTP terminé
- Echec du téléchargement du fichier du serveur FTP
- Renommage du fichier du serveur FTP terminé
- Echec du renommage du fichier du serveur FTP
- Téléchargement du fichier sur le serveur FTP terminé
- Echec du téléchargement du fichier sur le serveur FTP
- Création du répertoire du serveur FTPS terminée
- La création du répertoire du serveur FTPS a échoué
- Suppression du répertoire du serveur FTPS terminée
- La suppression du répertoire du serveur FTPS a échoué
- Suppression du fichier du serveur FTPS terminée
- La suppression du fichier du serveur FTPS a échoué
- Téléchargement du fichier du serveur FTPS terminé
- Echec du téléchargement du fichier du serveur FTPS
- Renommage du fichier du serveur FTPS terminé
- Echec du renommage du fichier du serveur FTPS
- Téléchargement du fichier du serveur FTPS terminé
- Echec du téléchargement du fichier sur le serveur FTPS
- Création du répertoire du serveur SFTP terminée
- La création du répertoire du serveur SFTP a échoué
- Suppression du répertoire du serveur SFTP terminée
- La suppression du répertoire du serveur SFTP a échoué
- Suppression du fichier du serveur SFTP terminée
- Echec de la suppression du fichier du serveur SFTP
- Téléchargement du fichier du serveur SFTP terminé
- Echec du téléchargement du fichier du serveur SFTP
- Renommage du fichier du serveur SFTP terminé
- Le changement de nom du fichier du serveur SFTP a échoué
- Téléchargement du fichier du serveur SFTP terminé

- Échec du téléchargement du fichier sur le serveur SFTP

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",
    "original-file-path" : "string",
    "renamed-file-path" : "string",
    "directory-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 d'événements de serveur SFTP, FTPS ou FTP répertoriés précédemment.

source

Identifie le service qui a généré l'événement. Pour les événements Transfer Family, cette valeur est `aws.transfer`.

detail

Un objet JSON qui contient 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, supprimé ou utilisé d'une autre manière.

original-file-path

Pour les événements de renommage de fichier, le chemin d'origine du fichier avant de le renommer.

renamed-file-path

Pour les événements de renommage de fichier, le nouveau chemin du fichier après le changement de nom.

directory-path

Pour les événements de création et de suppression d'un répertoire, le chemin du répertoire.

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, horodatage du début du traitement des fichiers.

Exemple Exemple d'événement d'échec du téléchargement du fichier du serveur SFTP

L'exemple suivant montre un événement au cours duquel un téléchargement a échoué sur un serveur SFTP (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 Exemple d'événement de téléchargement de fichier sur le serveur FTP terminé

L'exemple suivant montre un événement au cours duquel un téléchargement s'Amazon S3 est terminé avec succès sur un serveur FTP (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": "/amzn-s3-demo-bucket/test/1mb_file",
    "server-id": "s-1111aaaa2222bbbb3",
    "username": "test",
    "session-id": "event-ID",
    "start-timestamp": "2024-01-29T16:31:42.462088327Z"
  }
}

```

```
}  
}
```

Exemple Exemple d'événement de suppression du fichier du serveur SFTP terminé

L'exemple suivant montre un événement au cours duquel un fichier a été correctement supprimé sur un serveur SFTP.

```
{  
  "version": "0",  
  "id": "event-ID",  
  "detail-type": "SFTP Server File Delete Completed",  
  "source": "aws.transfer",  
  "account": "958412138249",  
  "time": "2025-05-15T14:30:27Z",  
  "region": "us-east-1",  
  "resources": [  
    "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"  
  ],  
  "detail": {  
    "status-code": "COMPLETED",  
    "protocol": "SFTP",  
    "client-ip": "IP-address",  
    "end-timestamp": "2025-05-15T14:30:27.749749117Z",  
    "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",  
    "server-id": "s-1234abcd5678efghi",  
    "username": "test",  
    "session-id": "session-ID",  
    "start-timestamp": "2025-05-15T14:30:26.706282454Z"  
  }  
}
```

Exemple Exemple d'événement terminé pour renommer le fichier du serveur SFTP

L'exemple suivant montre un événement au cours duquel un fichier a été renommé avec succès sur un serveur SFTP.

```
{  
  "version": "0",  
  "id": "event-ID",  
  "detail-type": "SFTP Server File Rename Completed",  
  "source": "aws.transfer",  
  "account": "958412138249",
```

```

    "time": "2025-05-15T15:45:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "SFTP",
        "client-ip": "IP-address",
        "end-timestamp": "2025-05-15T15:45:12.749749117Z",
        "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",
        "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
        "server-id": "s-1234abcd5678efghi",
        "username": "test",
        "session-id": "session-ID",
        "start-timestamp": "2025-05-15T15:45:11.706282454Z"
    }
}

```

Exemple Exemple d'événement Create Completed dans le répertoire du serveur SFTP

L'exemple suivant montre un événement au cours duquel un répertoire a été créé avec succès sur un serveur SFTP.

```

{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server Directory Create Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2025-05-15T16:20:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "SFTP",
        "client-ip": "IP-address",
        "end-timestamp": "2025-05-15T16:20:05.749749117Z",
        "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
        "server-id": "s-1234abcd5678efghi",
        "username": "test",
    }
}

```

```
    "session-id": "session-ID",  
    "start-timestamp": "2025-05-15T16:20:04.706282454Z"  
  }  
}
```

Événements relatifs au connecteur SFTP

Note

Ces événements sont diffusés à un EventBridge niveau durable, comme décrit dans la section [Niveau de livraison pour les événements de AWS service](#) dans Amazon EventBridge Events Reference.

Les champs de détail relatifs aux événements du connecteur SFTP sont les suivants :

- Envoi du fichier du connecteur SFTP terminé
- Échec de l'envoi du fichier du connecteur SFTP
- Récupération du fichier du connecteur SFTP terminée
- Échec de la récupération du fichier du connecteur SFTP
- La liste des répertoires du connecteur SFTP est terminée
- Échec de la liste des répertoires du connecteur SFTP
- Déplacement à distance du connecteur SFTP terminé
- Échec du déplacement à distance du connecteur SFTP
- Suppression à distance du connecteur SFTP terminée
- Échec de la suppression à distance du connecteur SFTP

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",
  "max-items" : "number",
  "connector-id" : "string",
  "output-directory-path" : "string",
  "listing-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",
  "item-count" : "number",
  "truncated" : "boolean",
  "bytes" : "number",
  "egress-type" : "string",
  "vpc-lattice-resource-configuration-arn" : "string",
  "vpc-lattice-port-number" : "number",
  "local-file-location" : {
    "domain" : "string",
    "bucket" : "string",
    "key" : "string"
  },
  "output-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 connecteur SFTP répertoriés précédemment.

source

Identifie le service qui a généré l'événement. Pour les Transfer Family événements, cette valeur est `aws.transfer`.

detail

Un objet JSON qui contient 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 :

max-items

Le nombre maximum de directory/file noms à renvoyer.

operation

Si la `StartFileTransfer` demande consiste à envoyer ou à récupérer un fichier.

Valeurs : `SEND` | `RETRIEVE`.

connector-id

Identifiant unique du connecteur SFTP utilisé.

output-directory-path

Le chemin (compartiment et préfixe) dans Amazon S3 pour stocker les résultats de la file/directory liste.

listing-id

Identifiant unique pour le fonctionnement de `StartDirectoryListing` l'API. Cet identifiant peut être utilisé pour consulter les CloudWatch journaux afin de connaître l'état de la demande d'inscription.

transfer-id

L'identifiant unique de l'événement de transfert (une `StartFileTransfer` demande).

file-transfer-id

Identifiant unique du fichier transféré.

url

URL du point de terminaison AS2 ou SFTP du partenaire.

file-path

L'emplacement et le 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.

Valeurs :ASSUME_ROLE_ERROR | UNSUPPORTED_OPERATION_ERROR | CONNECTION_ERROR | READ_FILE_ERROR | WRITE_FILE_ERROR | TIMEOUT_ERROR | LIST_DIRECTORY_ERROR | SEND_FILE_NOT_FOUND | RETRIEVE_FILE_NOT_FOUND | DIRECTORY_NOT_FOUND | FILE_NOT_FOUND | PATH_NOT_FOUND | RENAME_ERROR | DELETE_ERROR | INTERNAL_ERROR | UNKNOWN_ERROR.

failure-message

Pour les transferts ayant échoué, les détails expliquant pourquoi le transfert a échoué.

start-timestamp

Pour les transferts réussis, 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 serveur SFTP 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 serveur SFTP du partenaire. Dans ce cas, ce champ est vide.

item-count

Le nombre d'éléments (répertoires et fichiers) renvoyés pour la demande de listage.

truncated

Si la sortie de la liste contient tous les éléments contenus dans le répertoire distant ou non.

bytes

Le nombre d'octets transférés. La valeur est 0 pour les transferts échoués.

egress-type

Type de configuration de sortie pour le connecteur. Valeurs : SERVICE_MANAGED ou VPC_LATTICE.

vpc-lattice-resource-configuration-arn

ARN de la configuration des ressources VPC_LATTICE qui définit l'emplacement du serveur SFTP cible. Ce champ est nul pour les connecteurs gérés par des services.

vpc-lattice-port-number

Numéro de port pour la connexion au serveur SFTP via VPC_LATTICE.

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.

output-file-location

Ce paramètre contient les détails de l'emplacement où stocker les résultats de la liste des répertoires dans le AWS 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 Exemple d'événement d'échec de l'envoi du fichier du connecteur SFTP

L'exemple suivant montre un événement au cours duquel un connecteur SFTP a échoué alors qu'il tentait d'envoyer un fichier à un serveur SFTP 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": "/amzn-s3-demo-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": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}
```

Exemple Exemple d'événement terminé pour récupérer le fichier du connecteur SFTP

L'exemple suivant montre un événement au cours duquel un connecteur SFTP a réussi à récupérer un fichier envoyé par un serveur SFTP 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": "/amzn-s3-demo-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": "amzn-s3-demo-bucket",
      "key": "testfile.txt"
    }
  }
}
```

Exemple Exemple d'événement terminé avec la liste des répertoires du connecteur SFTP

L'exemple suivant montre un événement au cours duquel un appel de liste de répertoire de démarrage a extrait un fichier de liste d'un serveur SFTP distant.

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "SFTP Connector Directory Listing 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": {
  "max-items": 10000,
  "connector-id": "c-fc68000012345aa18",
  "output-directory-path": "/amzn-s3-demo-bucket/example/file-listing-output",
  "listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
  "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

  "status-code": "COMPLETED",
  "remote-directory-path": "/home",
  "item-count": 10000,
  "truncated": true,
  "start-timestamp": "2024-01-24T18:28:07.632388Z",
  "end-timestamp": "2024-01-24T18:28:07.774898Z",
  "output-file-location": {
    "domain": "S3",
    "bucket": "amzn-s3-demo-bucket",
    "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
  }
}
}

```

Événements AS2

Note

Ces événements sont diffusés à un EventBridge niveau durable, comme décrit dans la section [Niveau de livraison pour les événements de AWS service](#) dans Amazon EventBridge Events Reference.

Les champs de détail relatifs aux événements AS2 sont les suivants :

- Réception de la charge utile AS2 terminée
- Échec de réception de la charge utile AS2
- Envoi de la charge utile AS2 terminé
- Échec de l'envoi de la charge utile AS2

- Réception AS2 MDN terminée
- Échec de la réception MDN AS2
- Envoi MDN AS2 terminé
- Échec de l'envoi MDN AS2

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 événements AS2 répertoriés précédemment.

source

Identifie le service qui a généré l'événement. Pour les Transfer Family événements, cette valeur est `aws.transfer`.

detail

Un objet JSON qui contient 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 événements MDN, il identifie également le compartiment et la clé du fichier MDN.

file-bucket

Le conteneur de l'objet dans Amazon S3.

file-key

Le nom attribué à l'objet dans Amazon S3.

json-bucket

Pour les transferts TERMINÉS ou ÉCHOUÉS, le conteneur du fichier JSON.

json-key

Pour les transferts TERMINÉS ou ÉCHOUÉS, le nom attribué au fichier JSON dans Amazon S3.

mdn-bucket

Pour les événements MDN, conteneur du fichier MDN.

`mdn-key`

Pour les événements MDN, nom attribué au fichier MDN dans Amazon S3.

`mdn-subject`

Pour les événements MDN, une description textuelle de la disposition du message.

`mdn-message-id`

Pour les événements MDN, un identifiant unique pour le message MDN.

`disposition`

Pour les événements MDN, catégorie de disposition.

`bytes`

Le nombre d'octets contenus dans le message.

`as2-from`

Le partenaire commercial AS2 qui envoie le message.

`as2-message-id`

Identifiant unique pour le message AS2 transféré.

`as2-to`

Le partenaire commercial AS2 qui reçoit le message.

`connector-id`

Pour les messages AS2 envoyés depuis un serveur Transfer Family à un partenaire commercial, identifiant unique du connecteur AS2 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'accord AS2.

`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, 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 de messages AS2. 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 Exemple d'événement AS2 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": "amzn-s3-demo-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 Exemple d'événement d'échec de réception MDN AS2

```

{
  "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": "amzn-s3-demo-bucket1",
      "file-key": "/as2Integ/TestOutboundWrongCert.dat",
      "file-bucket": "amzn-s3-demo-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. Pour plus d'informations sur votre responsabilité en matière de conformité lors de l'utilisation Services AWS, consultez [AWS la documentation de sécurité](#).

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.

Nous proposons un atelier qui fournit des conseils prescriptifs et un laboratoire pratique sur la manière de créer une architecture de transfert de fichiers évolutive et sécurisée AWS sans avoir à modifier les applications existantes ou à gérer l'infrastructure de serveurs. Vous pouvez consulter les détails de cet atelier [ici](#).

Rubriques

- [Avantages de la connectivité VPC en termes de sécurité](#)
- [Politiques de sécurité pour AWS Transfer Family serveurs](#)
- [Politiques de sécurité pour AWS Transfer Family Connecteurs SFTP](#)
- [Utilisation de l'échange de clés post-quantique hybride avec AWS Transfer Family](#)

- [Protection et chiffrement des données](#)
- [Gestion des clés SSH et PGP dans Transfer Family](#)
- [Gestion des identités et des accès pour AWS Transfer Family](#)
- [Validation de conformité pour AWS Transfer Family](#)
- [Résilience dans AWS Transfer Family](#)
- [Créez une connexion privée entre un VPC et AWS Transfer Family API](#)
- [Sécurité de l'infrastructure dans AWS Transfer Family](#)
- [Ajouter un pare-feu pour applications Web](#)
- [Cross-service prévention confuse des adjoints](#)
- [AWS politiques gérées pour AWS Transfer Family](#)

Avantages de la connectivité VPC en termes de sécurité

Les connecteurs SFTP avec sortie VPC offrent des avantages Cross-VPC de sécurité accrus grâce à l'accès aux ressources :

- Isolation du réseau : tout le trafic reste dans votre environnement VPC, ce qui permet une isolation complète du réseau par rapport à l'Internet public pour les connexions de points de terminaison privés.
- Contrôle IP source : les serveurs SFTP distants ne voient que les adresses IP de votre plage d'adresses CIDR VPC, ce qui vous donne un contrôle total sur les adresses IP source utilisées pour les connexions.
- Accès aux terminaux privés : connectez-vous directement aux serveurs SFTP de votre VPC à l'aide d'adresses IP privées, éliminant ainsi toute exposition à l'Internet public.
- Connectivité hybride : accédez en toute sécurité aux serveurs SFTP sur site via des connexions VPN ou Direct Connect établies, sans exposition supplémentaire à Internet.
- Contrôles de sécurité VPC : exploitez les groupes de sécurité VPC, les NACL et les politiques de routage existants pour contrôler et surveiller le trafic des connecteurs SFTP.

Modèle de sécurité VPC Lattice

La connectivité VPC pour les connecteurs SFTP utilise le réseau AWS VPC Lattice avec des réseaux de services pour fournir un accès mutualisé sécurisé :

- Prévention de la confusion chez les adjoints : les contrôles d'authentification et d'autorisation garantissent que les connecteurs ne peuvent accéder qu'aux ressources spécifiques pour lesquelles ils sont configurés, empêchant ainsi tout accès non autorisé entre locataires.
- IPv6-only réseau de services : utilise l'adressage IPv6 pour éviter les conflits d'adresses IP potentiels et améliorer l'isolation de sécurité.
- Session d'accès direct (FAS) : la gestion temporaire des informations d'identification élimine le besoin de stockage à long terme des informations d'identification ou de partage manuel des ressources.
- Resource-level contrôle d'accès : Chaque connecteur est associé à une configuration de ressources spécifique, garantissant un contrôle d'accès granulaire aux serveurs SFTP individuels.

Bonnes pratiques de sécurité pour la connectivité VPC

Lorsque vous utilisez des connecteurs de sortie VPC, suivez les meilleures pratiques de sécurité suivantes :

- Groupes de sécurité : configurez les groupes de sécurité pour autoriser le trafic SFTP (port 22) uniquement entre les ressources nécessaires. Limitez les plages d'adresses IP source et de destination au minimum requis.
- Emplacement des passerelles de ressources : déployez les passerelles de ressources dans des sous-réseaux privés lorsque cela est possible, et assurez-vous qu'elles s'étendent sur au moins deux zones de disponibilité pour garantir une haute disponibilité.
- Surveillance du réseau : utilisez les journaux de flux VPC et Amazon CloudWatch pour surveiller les modèles de trafic réseau et détecter les activités anormales.
- Journalisation des accès : activez la journalisation des connecteurs pour suivre les activités de transfert de fichiers et gérer les pistes d'audit relatives aux exigences de conformité.
- Gestion de la configuration des ressources : passez régulièrement en revue et mettez à jour les configurations des ressources pour vous assurer qu'elles pointent vers les serveurs SFTP appropriés et qu'elles utilisent les paramètres réseau appropriés.

Politiques de sécurité pour AWS Transfer Family serveurs

Les politiques de sécurité du serveur vous AWS Transfer Family permettent de limiter l'ensemble des algorithmes cryptographiques (codes d'authentification des messages (MAC), échanges de clés

(KEX), suites de chiffrement, chiffrements de contenu et algorithmes de hachage) associés à votre serveur.

AWS Transfer Family prend en charge les politiques de sécurité post-quantique qui utilisent des algorithmes d'échange de clés hybrides, combinant des méthodes cryptographiques traditionnelles avec des algorithmes post-quantiques pour renforcer la sécurité contre les futures menaces informatiques quantiques. Pour de plus amples informations, veuillez consulter [Utilisation de l'échange de clés post-quantique hybride avec AWS Transfer Family](#).

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 [Gestion des clés SSH et PGP dans Transfer Family](#).

 Note

À compter de 2025, toutes les nouvelles politiques AWS Transfer Family de sécurité incluent un support cryptographique post-quantique utilisant des algorithmes d'échange de clés hybrides. Pour plus d'informations sur la sécurité post-quantique, consultez [Utilisation de l'échange de clés post-quantique hybride avec AWS Transfer Family](#).

 Note

Nous vous recommandons vivement de mettre vos serveurs à jour conformément à notre politique de sécurité la plus récente.

- `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, de l'API ou de la CLI.
- Si vous créez un serveur Transfer Family en utilisant CloudFormation et acceptez la politique de sécurité par défaut, le serveur est assigné `TransferSecurityPolicy-2018-11`.

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](#).

 Note

Les politiques post-quantiques antérieures (TransferSecurityPolicy-PQ-SSH-Experimental-2023-04 et TransferSecurityPolicy-PQ-SSH-FIPS-Experimental-2023-04) sont obsolètes. Nous vous recommandons plutôt d'utiliser les nouvelles politiques.

Pour plus d'informations sur la sécurité dans Transfer Family, consultez les articles de blog suivants :

- [Six conseils pour améliorer la sécurité de votre AWS Transfer Family serveur](#)
- [Comment Transfer Family peut vous aider à créer une solution de transfert de fichiers gérée sécurisée et conforme](#)

Rubriques

- [Algorithmes cryptographiques](#)
- [Détails de la politique de sécurité](#)

Algorithmes cryptographiques

Pour les clés d'hôte, nous prenons en charge les algorithmes suivants :

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`
- `ssh-ed25519`

En outre, les politiques de sécurité suivantes permettent `ssh-rsa` :

- `TransferSecurityPolicy-2018-11`
- `TransferSecurityPolicy-2020-06`
- `TransferSecurityPolicy-FIPS-2020-06`
- `TransferSecurityPolicy-FIPS-2023-05`

- TransferSecurityPolicy-FIPS-2024-01

 Note

Il est important de comprendre la distinction entre le type de clé RSA (qui est toujours le cas) `ssh-rsa` et l'algorithme de clé d'hôte RSA, qui peut être n'importe lequel des algorithmes pris en charge.

Voici 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.

- Les serveurs SFTP utilisent uniquement des algorithmes dans les `SshMacsections` `SshCiphersSshKexs`, et.
- Les serveurs FTPS utilisent uniquement les algorithmes de `TlsCiphers` cette section.
- Les serveurs FTP, puisqu'ils n'utilisent pas de chiffrement, n'utilisent aucun de ces algorithmes.
- Les serveurs AS2 utilisent uniquement des algorithmes dans les `HashAlgorithmssections` `ContentEncryptionCiphers` et `set`. Ces sections définissent les algorithmes utilisés pour chiffrer et signer le contenu des fichiers.
- Les politiques FIPS-2024-01 de sécurité FIPS-2024-05 et sont identiques, sauf que FIPS-2024-05 cela ne prend pas en charge l'`ssh-rsa` algorithme.
- Transfer Family a introduit de nouvelles politiques restreintes qui sont étroitement parallèles aux politiques existantes :
 - Les politiques TransferSecurityPolicy-2018-11 de sécurité TransferSecurityPolicy-Restricted-2018-11 et sont identiques, sauf que la politique restreinte ne prend pas en charge le `chacha20-poly1305@openssh.com` chiffrement.
 - Les politiques TransferSecurityPolicy-2020-06 de sécurité TransferSecurityPolicy-Restricted-2020-06 et sont identiques, sauf que la politique restreinte ne prend pas en charge le `chacha20-poly1305@openssh.com` chiffrement.

* Dans le tableau suivant, le chacha20-poly1305@openssh.com chiffrement est inclus uniquement dans la politique non restreinte,

Politique de sécurité	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-FIPS-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
SshCiphers											
aes128-CTR	◆	◆	◆	◆	◆				◆	◆	◆
aes128-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes192-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-ctr	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
aes256-gcm@openssh.com	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Politique de sécurité	Transfer Security-2025-03	Transfer Security-2025-08	Transfer Security-2025-08	Transfer Security-2025-07	Transfer Security-2024-01	Transfer Security-2024-05	Transfer Security-2023-05	Transfer Security-2023-03	Transfer Security-2023-06	Transfer Security-2020-06	Transfer Security-2018-11
chacha20-poly1305@openssh.com										*	*
SshKexs											
mlkem768x25519-sha256	◆		◆								
mlkem768nistp256-sha256	◆		◆								
mlkem1024nistp384-sha384	◆		◆								
curve25519-sha256		◆	◆	◆		◆		◆			◆

Politique de sécurité	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-FIPS-2024-01	TransferSecurityPolicy-2025-05	TransferSecurityPolicy-FIPS-2023-05	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-06	TransferSecurityPolicy-FIPS-2020-06	TransferSecurityPolicy-2018-11
		Compliant-2025-02	Restricted-2025-07			TransferSecurityPolicy-2024-05				TransferSecurityPolicy-2020-06		TransferSecurityPolicy-2018-11
curve25519-sha256@libssh.org		◆	◆	◆		◆		◆				◆
diffie-hellman-group14-sha1												◆
diffie-hellman-group14-sha256									◆	◆	◆	

Politique de sécurité	Transfer Security Policy-2025-03	Transfer Security Policy-FIPS-2025-08	Transfer Security Policy-SshA	Transfer Security Policy-AS2R	Transfer Security Policy-Comes	Transfer Security Policy-Restricted-2025-07	Transfer Security Policy-2024-01/	Transfer Security Policy-FIPS-2024-05	Transfer Security Policy-2023-05	Transfer Security Policy-2020-06	Transfer Security Policy-Rest	Transfer Security Policy-Rest	Transfer Security Policy-Rest	Transfer Security Policy-Rest
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gro														
up16-sha512														
diffie-he	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
llman-gro														
up18-sha512														
diffie-he	◆	◆	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆	◆
llman-gro														
up-exchan														
ge-sha256														

Politique de sécurité	Transfer Security Policy-2025-03	Transfer Security Policy-2025-08	Transfer Security Policy-2025-08	Transfer Security Policy-2025-08	Transfer Security Policy-2025-07	Transfer Security Policy-2024-01/2024-05	Transfer Security Policy-2023-05	Transfer Security Policy-2023-06	Transfer Security Policy-2020-06	Transfer Security Policy-2020-06	Transfer Security Policy-2018-11
ecdh-sha2-nistp255	◆	◆		◆	◆	◆			◆	◆	◆
ecdh-sha2-nistp384	◆	◆		◆	◆	◆			◆	◆	◆
ecdh-sha2-nistp521	◆	◆		◆	◆	◆			◆	◆	◆
SshMacs											
hmac-sha1											◆
hmac-sha1											◆
etm@openssh.com											

Politique de sécurité	Transfer Security-2025-03	Transfer Security-2025-08	Transfer Security-2025-08	Transfer Security-2025-08	Transfer Security-2025-07	Transfer Security-2024-01	Transfer Security-2023-05	Transfer Security-2023-05	Transfer Security-2023-06	Transfer Security-2020-06	Transfer Security-2018-11
		FIPS	SshA	AS2R		FIPS	FIPS			FIPS	
		-2025-08	ditComes	stricted		-2024-01/	-2023-05			-2020-06	
			iant-2025-02			TransferS			TransferS		TransferS
						ecurityPo			ecurityPo		ecurityPo
						licy-			licy-		licy-
						FIPS			Rest		Rest
						-2024-05			ricted-20		ricted-20
									20-06		18-11
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	Transfer Security Policy-2025-03	Transfer Security Policy-FIPS-2025-08	Transfer Security Policy-SshA	Transfer Security Policy-AS2R	Transfer Security Policy-Comes	Transfer Security Policy-Restricted-2025-07	Transfer Security Policy-2024-01	Transfer Security Policy-FIPS-2024-05	Transfer Security Policy-2023-05	Transfer Security Policy-2020-06	Transfer Security Policy-2020-06	Transfer Security Policy-FIPS-2020-06	Transfer Security Policy-Rest	Transfer Security Policy-Rest
umac-128@openssh.com														
umac-64-etm@openssh.com														
umac-64@openssh.com														
ContentEncryptionCiphers														
aes256-cbc														
aes192-cbc														
aes128-cbc														
3des-CBC														

Politique de sécurité	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-2025-08	TransferSecurityPolicy-SshA	TransferSecurityPolicy-AS2R	TransferSecurityPolicy-2025-01	TransferSecurityPolicy-2024-01	TransferSecurityPolicy-2023-05	TransferSecurityPolicy-2023-03	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11
			Compliant-2025-02	Restricted-2025-07		TransferSecurityPolicy-2024-05			TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2020-06	TransferSecurityPolicy-2018-11

HashAlgorithms

sha256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha512	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
sha1	◆	◆	◆		◆	◆	◆	◆	◆	◆	◆

TlsCiphers

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Politique de sécurité	Transfer Security Policy-2025-03	Transfer Security Policy-2025-08	Transfer Security Policy-2025-08	Transfer Security Policy-2025-08	Transfer Security Policy-2025-07	Transfer Security Policy-2024-01/2024-05	Transfer Security Policy-2023-05	Transfer Security Policy-2023-05	Transfer Security Policy-2023-06	Transfer Security Policy-2020-06	Transfer Security Policy-2020-06	Transfer Security Policy-2018-11
		FIPS	SshA	AS2R		FIPS		FIPS			FIPS	
		-2025-08	ditCom	restricted		-2024-01/		-2023-05		et	-2020-06	t
			iant-2025-02	2025-07		TransferS				TransferS		TransferS
						ecurityPo				ecurityPo		ecurityPo
					licy-	licy-				licy-		licy-
					FIPS	FIPS				Rest		Rest
					-2024-05					ricted-20		ricted-20
										20-06		18-11
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆

Politique de sécurité	TransferSecurity-2025-03	TransferSecurity-FIPS-2025-08	TransferSecurity-SshA	TransferSecurity-AS2R	TransferSecurity-2025-01	TransferSecurity-FIPS-2024-01	TransferSecurity-2025-05	TransferSecurity-FIPS-2023-05	TransferSecurity-2025-03	TransferSecurity-2025-06	TransferSecurity-FIPS-2020-06	TransferSecurity-2018-11
		Compliant-2025-02	Restricted-2025-07			TransferSecurity-2024-05				Restricted-2020-06		TransferSecurity-2018-11
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆	◆
TLS_RSA_WITH_AES_128_CBC_SHA256												◆
TLS_RSA_WITH_AES_128_CBC_SHA256												◆

Détails de la politique de sécurité

Les sections suivantes contiennent la représentation JSON de chaque politique de sécurité.

TransferSecurityPolicy-2025-03

Voici la politique de TransferSecurityPolicy-2025-03 sécurité.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "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"
    ],
    "Type": "SERVER",
    "Protocols": [
      "SFTP",
      "FTPS"
    ]
  }
}

```

TransferSecurityPolicy-FIPS-2025-03

Voici la politique de TransferSecurityPolicy-FIPS-2025-03 sécurité.

```

{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr",
      "aes128-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512"
    ]
  }
}

```

```

    ],
    "SshMac": [
        "hmac-sha2-512-etm@openssh.com",
        "hmac-sha2-256-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-AS2Restricted-2025-07

Cette politique de sécurité est conçue pour les transferts de fichiers AS2 qui nécessitent une sécurité renforcée en excluant les algorithmes cryptographiques existants. Il prend en charge le cryptage AES moderne et les algorithmes de SHA-2 hachage tout en supprimant la prise en charge des algorithmes plus faibles tels que 3DES et SHA-1.

Note

Cette politique de sécurité est identique à TransferSecurityPolicy-2025-03, sauf qu'elle ne prend pas en charge 3DES (in ContentEncryptionCiphers) ni SHA1 (in HashAlgorithms). Il inclut tous les algorithmes de 2025-03, y compris les algorithmes cryptographiques post-quantiques (mlkem* KEXs).

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "mlkem768x25519-sha256",
      "mlkem768nistp256-sha256",
      "mlkem1024nistp384-sha384",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
    ],
    "HashAlgorithms": [
```

```

        "sha256",
        "sha384",
        "sha512"
    ],
    "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"
    ],
    "Type": "SERVER",
    "Protocols": [
        "SFTP",
        "FTPS"
    ]
}

```

TransferSecurityPolicy-SshAuditCompliant-2025-02

Voici la politique de TransferSecurityPolicy-SshAuditCompliant-2025-02 sécurité.

Note

Cette politique de sécurité est conçue autour des recommandations fournies par l'ssh-auditoutil et est 100 % conforme à cet outil.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [
      "aes128-gcm@openssh.com",

```

```
    "aes256-gcm@openssh.com",
    "aes128-ctr",
    "aes256-ctr",
    "aes192-ctr"
  ],
  "SshKexs": [
    "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"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "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"
  ],
  "Type": "SERVER"
}
```

TransferSecurityPolicy-2024-01

Voici la politique de TransferSecurityPolicy-2024-01 sécurité.

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "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"
    ]
}
}

```

TransferSecurityPolicy-FIPS-2024-01/TransferSecurityPolicy-FIPS-2024-05

Vous trouverez ci-dessous les politiques TransferSecurityPolicy-FIPS-2024-05 de sécurité TransferSecurityPolicy-FIPS-2024-01 et.

Note

Le point de terminaison TransferSecurityPolicy-FIPS-2024-01 et les politiques de TransferSecurityPolicy-FIPS-2024-05 sécurité du service FIPS ne sont disponibles que dans certaines AWS régions. Pour plus d'informations, consultez [Points de terminaison et quotas AWS Transfer Family](#) dans le document Références générales AWS.

La seule différence entre ces deux politiques de sécurité est qu'elles TransferSecurityPolicy-FIPS-2024-01 supportent l'`ssh-rsa` algorithm, TransferSecurityPolicy-FIPS-2024-05 et non.

```

{
  "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-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"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ]
}
}

```

TransferSecurityPolicy-2023-05

Voici la politique de TransferSecurityPolicy-2023-05 sécurité.

```

{
  "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"
    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ]
}

```

TransferSecurityPolicy-FIPS-2023-05

Les détails de la certification FIPS sont AWS Transfer Family disponibles à l'adresse <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Voici la politique de TransferSecurityPolicy-FIPS-2023-05 sécurité.

 Note

La politique de TransferSecurityPolicy-FIPS-2023-05 sécurité et de point de terminaison du service FIPS n'est disponible que dans certaines AWS régions. 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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "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"
    ]
}
}

```

TransferSecurityPolicy-2022-03

Voici la politique de TransferSecurityPolicy-2022-03 sécurité.

```

{
  "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"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",

```

```

    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "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"
  ]
}
}

```

TransferSecurityPolicy-2020-06 et TransferSecurityPolicy-Restricted-2020-06

Voici la politique de TransferSecurityPolicy-2020-06 sécurité.

Note

Les politiques TransferSecurityPolicy-2020-06 de sécurité TransferSecurityPolicy-Restricted-2020-06 et sont identiques, sauf que la politique restreinte ne prend pas en charge le `chacha20-poly1305@openssh.com` chiffrement.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
      "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"
  ],
  "ContentEncryptionCiphers": [
    "aes256-cbc",
    "aes192-cbc",
    "aes128-cbc",
    "3des-cbc"
  ],
  "HashAlgorithms": [
    "sha256",
    "sha384",
    "sha512",
    "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"
  ]
}
```

```
}
```

TransferSecurityPolicy-FIPS-2020-06

Les détails de la certification FIPS sont AWS Transfer Family disponibles à l'adresse <https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all>

Voici la politique de TransferSecurityPolicy-FIPS-2020-06 sécurité.

Note

Le point de terminaison et la politique TransferSecurityPolicy-FIPS-2020-06 de sécurité du service FIPS ne sont disponibles que dans certaines AWS régions. 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"
    ]
  }
}
```



```

    ],
    "ContentEncryptionCiphers": [
        "aes256-cbc",
        "aes192-cbc",
        "aes128-cbc",
        "3des-cbc"
    ],
    "HashAlgorithms": [
        "sha256",
        "sha384",
        "sha512",
        "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"
    ]
}
}

```

TransferSecurityPolicy-2018-11 et TransferSecurityPolicy-Restricted-2018-11

Voici la politique de TransferSecurityPolicy-2018-11 sécurité.

Note

Les politiques TransferSecurityPolicy-2018-11 de sécurité TransferSecurityPolicy-Restricted-2018-11 et sont identiques, sauf que la politique restreinte ne prend pas en charge le `chacha20-poly1305@openssh.com` chiffrement.

```

{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [

```

```
"chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2018-11
  "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"
],
"ContentEncryptionCiphers": [
  "aes256-cbc",
  "aes192-cbc",
  "aes128-cbc",
  "3des-cbc"
],
"HashAlgorithms": [
  "sha256",
  "sha384",
  "sha512",
  "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"  
]  
}  
}
```

Politiques de sécurité pour AWS Transfer Family Connecteurs SFTP

Les politiques de sécurité du connecteur SFTP vous AWS Transfer Family permettent de limiter l'ensemble des algorithmes cryptographiques (codes d'authentification des messages (MAC), échanges de clés (KEX) et suites de chiffrement) associés à votre connecteur SFTP. Voici une liste des algorithmes cryptographiques pris en charge pour chaque politique de sécurité du connecteur SFTP.

Note

`TransferSFTPConnectorSecurityPolicy-2024-03` est la politique de sécurité par défaut appliquée aux connecteurs SFTP.

Vous pouvez modifier la politique de sécurité de votre connecteur. Sélectionnez **Connectors** dans le volet de navigation de gauche de Transfer Family, puis sélectionnez votre connecteur. Sélectionnez ensuite **Modifier** dans la section de configuration **Sftp**. Dans la section **Options** de l'algorithme cryptographique, choisissez n'importe quelle politique de sécurité disponible dans la liste déroulante du champ **Politique de sécurité**.

Algorithmes cryptographiques

Pour les clés d'hôte, les connecteurs SFTP prennent en charge tous les algorithmes pris en charge par les serveurs Transfer Family, à l'exception de ed25519 :

- rsa-sha2-256
- rsa-sha2-512
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp521

De plus, nous prenons en charge les clés d'hôte ssh-rsa, mais uniquement pour TransferSFTPConnectorSecurityPolicy-2023-07.

Pour l'authentification, les connecteurs SFTP prennent en charge les types de clés suivants :

- ssh-rsa
- ecdsa

Détails de la politique de sécurité du connecteur SFTP

Le tableau suivant indique les algorithmes cryptographiques spécifiques pris en charge par chaque politique de sécurité du connecteur SFTP.

Politique de sécurité	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
Ciphers			
aes128-CTR			◆
aes128-gcm@openssh.com	◆	◆	◆
aes192-ctr		◆	◆

Politique de sécurité	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
aes256-ctr		◆	◆
aes256-gcm@openssh.com	◆	◆	◆
Kexs			
curve25519-sha256		◆	◆
curve25519-sha256@libssh.org		◆	◆
diffie-hellman-group14-sha1			◆
diffie-hellman-group16-sha512		◆	◆
diffie-hellman-group18-sha512		◆	◆
diffie-hellman-group-exchange-sha256		◆	◆
ecdh-sha2-nistp255	◆		
ecdh-sha2-nistp384	◆		
ecdh-sha2-nistp521	◆		
Macs			
hmac-sha2-512-etm@openssh.com		◆	◆
hmac-sha2-256-etm@openssh.com		◆	◆

Politique de sécurité	TransferSFTPConnectorSecurityPolicy-FIPS-2024-10	TransferSFTPConnectorSecurityPolicy-2024-03	TransferSFTPConnectorSecurityPolicy-2023-07
hmac-sha2-512	◆	◆	◆
hmac-sha2-256	◆	◆	◆
hmac-sha1			◆
hmac-sha1-96			◆
Host Key Algorithms			
rsa-sha2-256	◆	◆	◆
rsa-sha2-512	◆	◆	◆
ecdsa-sha2-nistp256	◆	◆	◆
ecdsa-sha2-nistp384		◆	◆
ecdsa-sha2-nistp521		◆	◆
ssh-rsa			◆

Utilisation de l'échange de clés post-quantique hybride avec AWS Transfer Family

Transfer Family prend en charge une option hybride d'établissement de clés post-quantiques pour le protocole Secure Shell (SSH). Post-quantum un établissement clé 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 attaque « store-now-harvest-later ».

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). Post-quantum l'établissement de clés hybrides en SSH introduit des mécanismes d'établissement de clés post-quantiques, qu'il utilise conjointement avec des algorithmes d'échange de clés classiques. Les clés SSH 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.

Pour 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-Quantumcryptographie](#).

Table des matières

- [À propos de l'échange de clés hybrides post-quantiques en SSH](#)
- [Comment fonctionne l'établissement de clés hybrides post-quantiques dans Transfer Family](#)
 - [Pourquoi ? ML-KEM](#)
 - [Post-quantum échange de clés SSH hybride et exigences cryptographiques \(FIPS 140\)](#)
- [Test de l'échange de clés hybrides post-quantiques dans Transfer Family](#)
 - [Activez l'échange de clés hybrides post-quantiques sur votre point de terminaison SFTP](#)
 - [Configurer un client SFTP qui prend en charge l'échange de clés hybrides post-quantiques](#)
 - [Confirmer l'échange de clés hybrides post-quantiques dans SFTP](#)

À propos de l'échange de clés hybrides post-quantiques en SSH

Transfer Family prend en charge les suites de chiffrement hybrides post-quantiques par échange de clés, qui utilisent à la fois l'algorithme d'échange de clés classique [Elliptic Curve Diffie-Hellman](#)

(ECDH) et. ML-KEM ML-KEM 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 continuent à échanger des clés ECDH. De plus, le serveur encapsule un secret partagé post-quantique dans la clé publique KEM post-quantique du client, qui est annoncée dans le message d'échange de clés SSH du 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 la protection des poignées de main tant que l'ECDH ou le secret partagé post-quantique ne peuvent pas être brisés.

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 dans le cadre des transferts de fichiers SFTP vers. AWS Transfer Family adapte en toute sécurité les transferts de fichiers interentreprises vers les services de AWS stockage à l'aide du protocole SFTP et d'autres protocoles. Le SFTP est une version plus sécurisée du protocole de transfert de fichiers (FTP) qui fonctionne via SSH. La prise en charge de l'échange de clés post-quantique de Transfer Family élève la barre de sécurité pour les transferts de données via SFTP.

Le support SFTP pour l'échange de clés hybride post-quantique dans Transfer Family inclut la combinaison d'algorithmes post-quantiques et ML-KEM-768 ML-KEM-1024, avec l'ECDH, sur des courbes P256, P384 ou Curve25519. Les méthodes d'échange de clés SSH correspondantes suivantes sont spécifiées dans [le projet d'échange de clés SSH hybride post-quantique](#).

- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- mlkem768x25519-sha256

Pourquoi ? ML-KEM

AWS s'engage à soutenir des algorithmes standardisés et interopérables. ML-KEM est le seul algorithme d'échange de clés post-quantique standardisé et approuvé par le projet de [Post-Quantumcryptographie du NIST](#). Les organismes de normalisation s'intègrent déjà ML-KEM dans les protocoles. AWS est déjà compatible avec ML-KEM le protocole TLS sur certains points de terminaison AWS d'API.

Dans le cadre de cet engagement, AWS a soumis un projet de proposition à l'IETF pour la cryptographie post-quantique qui se combine ML-KEM avec des NIST-approved courbes telles que P256 pour SSH. Afin d'améliorer la sécurité de nos clients, la AWS mise en œuvre de l'échange de clés post-quantique en SFTP et SSH suit ce projet. Nous prévoyons de soutenir ses futures mises à jour jusqu'à ce que notre proposition soit adoptée par l'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](#)) pourraient changer à mesure que le projet évolue vers la normalisation.

Note

Post-quantum le support des algorithmes est actuellement disponible pour l'échange de clés hybrides post-quantiques dans TLS pour AWS KMS (voir [Utilisation du TLS post-quantique hybride avec AWS KMS](#)) et les points de terminaison d'API AWS Certificate Manager. AWS Secrets Manager

Post-quantum échange de clés SSH hybride et exigences cryptographiques (FIPS 140)

Pour les clients qui ont besoin de se conformer à la norme FIPS, Transfer Family fournit une FIPS-approved cryptographie en SSH en utilisant la bibliothèque cryptographique open source certifiée AWS FIPS 140, -LC. AWS Les méthodes d'échange de clés hybrides post-quantiques prises en charge dans le TransferSecurityPolicy-FIPS-2025-03 in Transfer Family sont approuvées FIPS conformément à la norme [SP 800-56Cr2 du NIST](#) (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 hybrides post-quantiques dans Transfer Family

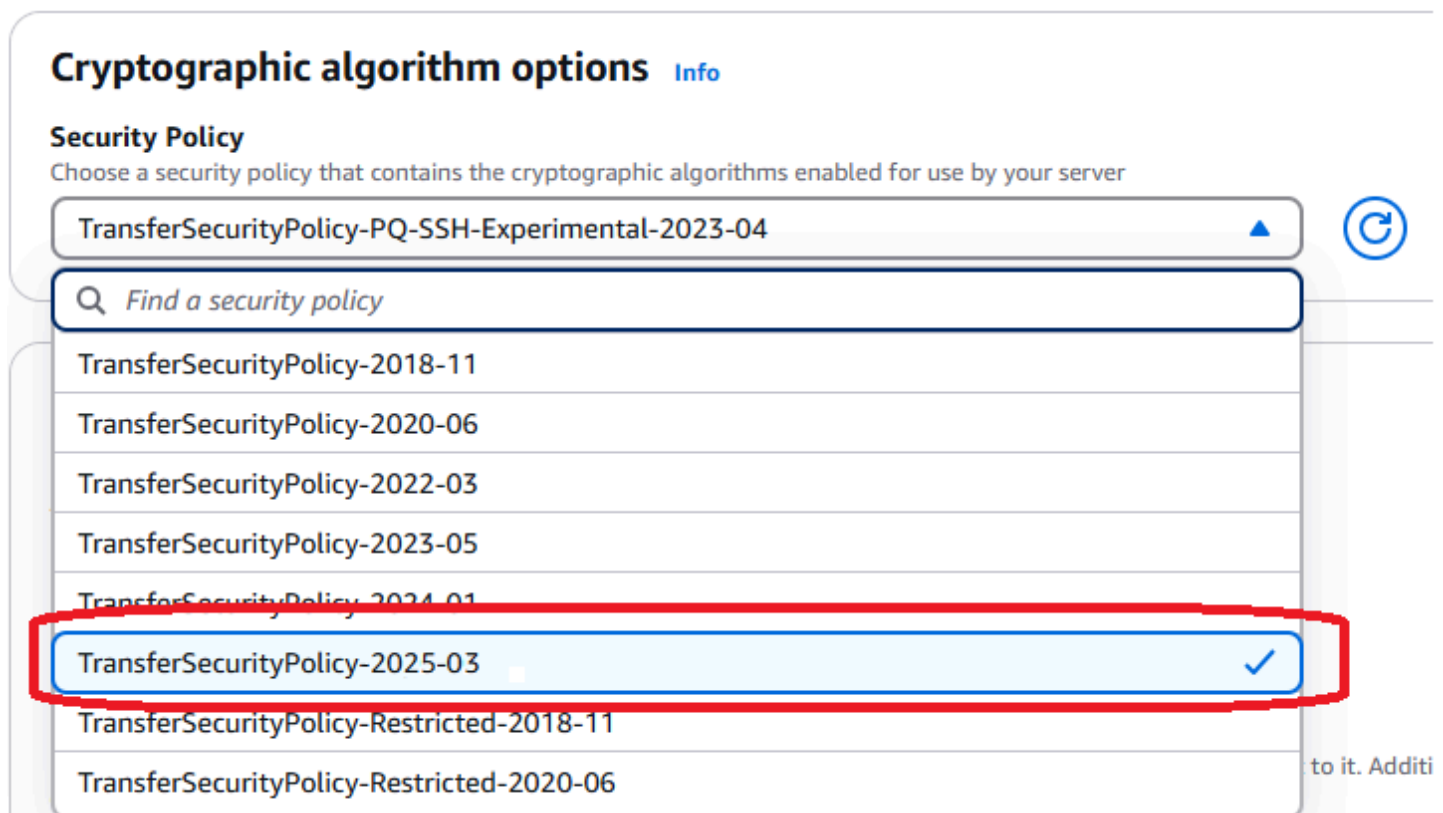
Cette section décrit les étapes à suivre pour tester l'échange de clés hybride post-quantique.

1. [Activez l'échange de clés hybrides post-quantiques sur votre point de terminaison SFTP.](#)
2. Utilisez un client SFTP (tel que [Configurer un client SFTP 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. [Confirmer l'échange de clés hybrides post-quantiques dans SFTP.](#)

Activez l'échange de clés hybrides post-quantiques sur votre point de terminaison SFTP

Vous pouvez choisir la politique SSH lorsque vous créez un nouveau point de terminaison de serveur SFTP dans Transfer Family ou en modifiant les options de l'algorithme cryptographique dans un point de terminaison SFTP existant. L'instantané suivant montre un exemple de mise à jour de la politique SSH.



Les noms des politiques SSH qui prennent en charge l'échange de clés post-quantique sont `TransferSecurityPolicy-2025-03` et `TransferSecurityPolicy-FIPS-2025-03`. Pour plus de détails sur les politiques de Transfer Family, consultez [Politiques de sécurité pour AWS Transfer Family serveurs](#).

Configurer un client SFTP qui prend en charge l'échange de clés hybrides post-quantiques

Après avoir sélectionné la bonne politique SSH post-quantique dans votre point de terminaison SFTP Transfer Family, vous pouvez expérimenter le SFTP post-quantique dans Transfer Family. Installez le dernier client OpenSSH (tel que la version 9.9) sur votre système local pour le tester.

 Note

Assurez-vous que votre client prend en charge un ou plusieurs des ML-KEM algorithmes listés précédemment. Vous pouvez consulter les algorithmes pris en charge pour votre version d'OpenSSH en exécutant cette commande : `ssh -Q kex`

Vous pouvez exécuter l'exemple de client SFTP pour vous connecter à votre point de terminaison SFTP (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 -v -o \
  KexAlgorithms=mlkem768x25519-sha256 \
  -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 :

- Remplacer *username_private_key_PEM_file* par le fichier de clé PEM-encodée privée de l'utilisateur SFTP
- Remplacez *username* par le nom d'utilisateur SFTP
- Remplacez *server-id* par l'ID du serveur Transfer Family
- Remplacez *region-id* par la région dans laquelle se trouve votre serveur Transfer Family

Confirmer 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 connexion SSH entre SFTP et Transfer Family, vérifiez la sortie du client. Vous pouvez éventuellement utiliser un programme de capture de paquets. Si vous utilisez le client OpenSSH 9.9, le résultat doit ressembler à ce qui suit (en omettant les informations non pertinentes pour des raisons de concision) :

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025
debug1: Reading configuration data /Users/username/.ssh/config
```

```
debug1: /Users/username/.ssh/config line 146: Applying options for *
debug1: Reading configuration data /Users/username/.ssh/bastions-config
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
[xxx.yyy.zzz.nnn] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_9.9
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 /Users/username/.ssh/known_hosts2: No such file or
directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: mlkem768x25519-sha256
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes128-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:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0
[...]
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 s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
([xxx.yyy.zzz.nnn]:22) using "publickey".
debug1: channel 0: new session [client-session] (inactive timeout: 0)
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

Le résultat indique que la négociation avec le client a eu lieu à l'aide de la mlkem768x25519-sha256 méthode hybride post-quantique et qu'une session SFTP a été établie avec succès.

Protection et chiffrement des données

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, veuillez consulter la [FAQ sur la confidentialité des données](#). Pour plus d'informations sur la protection des données en Europe, consultez le [modèle de responsabilité AWS partagée et le billet de blog sur le RGPD](#) sur le blog sur la AWS sécurité.

Pour des raisons 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 IAM Identity Center. Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous prenons en charge le protocole TLS 1.2.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut 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 modules cryptographiques validés FIPS 140-2 lorsque vous accédez à AWS via une CLI ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, veuillez consulter [Federal information processing standard \(FIPS\) 140-2](#) (français non garanti).

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 Name (Nom). Cela inclut lorsque vous travaillez avec Transfer Family ou d'autres AWS services à l'aide de la console, de l'API ou AWS des SDK. AWS CLI 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

une URL à un serveur externe, n'incluez pas les informations d'identification non chiffrées dans l'URL pour valider votre demande adressée au serveur.

En revanche, les données issues des opérations de chargement et de téléchargement à destination et en provenance des serveurs Transfer Family sont traitées comme totalement privées et n'existent jamais en dehors des canaux cryptés, tels qu'une connexion SFTP ou FTPS. Ces données ne sont toujours accessibles qu'aux personnes autorisées.

Chiffrement des données dans Transfer Family

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 AWS Key Management Service (AWS KMS) des clés gérées (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 crypter 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 Gestion des identités et des accès AWS (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 politique IAM qui accorde les autorisations minimales requises lors de l'utilisation AWS Transfer Family avec un compartiment Amazon S3 activé pour le AWS KMS chiffrement. Incluez cet exemple de politique à la fois dans la stratégie de rôle IAM de l'utilisateur et dans la stratégie de session, si vous en utilisez une.

```
{  
  "Sid": "Stmt1544140969635",  
  "Action": [  

```

```
"kms:Decrypt",
"kms:Encrypt",
"kms:GenerateDataKey",
"kms:GetPublicKey",
"kms:ListKeyPolicies"
],
"Effect": "Allow",
"Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

Note

L'ID de clé KMS que vous spécifiez dans cette politique doit être le même que celui spécifié pour le chiffrement par défaut à l'étape 1.

Le rôle root, ou le rôle IAM 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 dans AWS KMS](#) dans le Guide du AWS Key Management Service développeur.

AWS Transfer Family chiffrement au repos

Comme il AWS Transfer Family s'agit d'un service de transfert de fichiers, il ne gère pas vos données de stockage au repos. Les services et systèmes de stockage pris AWS Transfer Family en charge sont chargés de protéger les données dans cet état. Cependant, certaines données relatives aux services sont AWS Transfer Family gérées au repos.

Qu'est-ce qui est crypté ?

Les seules données traitées AWS Transfer Family au repos concernent les détails nécessaires au fonctionnement de vos serveurs de transfert de fichiers et au traitement des transferts. AWS Transfer Family stocke les données suivantes avec un chiffrement complet au repos dans Amazon DynamoDB :

- Configurations du serveur (par exemple, paramètres du serveur, configurations de protocole et détails du point de terminaison).
- Les données d'authentification des utilisateurs, y compris les clés publiques SSH et les métadonnées des utilisateurs.
- Détails de l'exécution du flux de travail et configurations des étapes.

- Configurations du connecteur et informations d'authentification pour les systèmes tiers. Ces informations d'identification sont chiffrées à l'aide de clés de chiffrement AWS Transfer Family gérées.

Gestion des clés

Vous ne pouvez pas gérer les clés de chiffrement AWS Transfer Family utilisées pour stocker les informations dans DynamoDB relatives à l'exécution de vos serveurs et au traitement des transferts. Ces informations incluent les configurations de votre serveur, les données d'authentification des utilisateurs, les détails du flux de travail et les informations d'identification du connecteur.

Qu'est-ce qui n'est pas crypté ?

Bien que AWS Transfer Family cela ne contrôle pas la manière dont vos données de stockage sont chiffrées au repos, nous vous recommandons tout de même de configurer vos emplacements de stockage avec le niveau de sécurité le plus élevé qu'ils prennent en charge. Par exemple, vous pouvez chiffrer des objets avec des clés de chiffrement gérées par Amazon S3 (SSE-S3) ou des AWS KMS clés (SSE-KMS).

En savoir plus sur la façon dont les services AWS de stockage cryptent les données au repos :

- [Amazon S3](#)
- [Amazon EFS](#)

Gestion des clés SSH et PGP dans Transfer Family

Dans cette section, vous trouverez des informations sur les clés SSH, 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 AWS Transfer Family and AWS Lambda](#). Pour le déploiement et la gestion automatisés des utilisateurs utilisant plusieurs clés SSH, consultez [Modules Transfer Family Terraform](#).

Note

AWS Transfer Family accepte les clés RSA, ECDSA et ED25519 pour l'authentification SSH.

Cette section explique également comment générer et gérer les clés Pretty Good Privacy (PGP).

Pour un aperçu complet de tous les algorithmes de chiffrement et de clé pris en charge, y compris des recommandations pour différents cas d'utilisation, voir [Vue d'ensemble des algorithmes de chiffrement et de clé](#).

Vue d'ensemble des algorithmes de chiffrement et de clé

AWS Transfer Family prend en charge différents types d'algorithmes à des fins différentes. Comprendre les algorithmes à utiliser pour votre cas d'utilisation spécifique permet de garantir des transferts de fichiers sécurisés et compatibles.

Référence rapide de l'algorithme

Cas d'utilisation	Algorithme recommandé	Conforme à la norme FIPS	Remarques
SSH/SFTP Authentification	RSA (rsa-sha2-256/512), ECDSA ou ED25519	RSA : Oui, ECDSA : Oui, ED25519 : Non	Compatible avec tous les clients et serveurs SSH
Génération de clés PGP	RSA ou ECC (NIST)	Oui	Pour le déchiffrement du flux de travail
Chiffrement de fichiers PGP	AES-256	Oui	Déterminé par le logiciel PGP

Algorithmes d'authentification SSH

Ces algorithmes sont utilisés pour SSH/SFTP l'authentification entre les clients et AWS Transfer Family les serveurs. Choisissez l'une de ces options lorsque vous générez des paires de clés SSH pour l'authentification des utilisateurs ou des clés d'hôte du serveur.

RSA (recommandé)

Compatible avec tous les clients et serveurs SSH, et FIPS-compliant. À utiliser avec le SHA-2 hachage pour une sécurité renforcée :

- `rsa-sha2-256`- Recommandé pour la plupart des cas d'utilisation

- `rsa-sha2-512`- Option de sécurité accrue

ED25519

Moderne et efficace. Des clés de plus petite taille avec une sécurité renforcée :

- `ssh-ed25519`- Rapide et sécurisé, mais pas FIPS-compliant

ECDSA

Option de courbe elliptique. Bon équilibre entre sécurité et performance :

- `ecdsa-sha2-nistp256`- Courbe standard
- `ecdsa-sha2-nistp384`- Courbe de sécurité plus élevée
- `ecdsa-sha2-nistp521`- Courbe de sécurité la plus élevée

Note

Nous prenons en charge `ssh-rsa` les anciennes politiques de sécurité avec SHA1. Pour en savoir plus, consultez [Algorithmes cryptographiques](#).

Choisir le bon algorithme SSH

- Pour la plupart des utilisateurs : utilisez RSA avec ou `rsa-sha2-256` `rsa-sha2-512`
- Pour la conformité à la norme FIPS : utilisez les algorithmes RSA ou ECDSA
- Pour les environnements modernes : l'ED25519 offre une sécurité et des performances excellentes

Algorithmes de chiffrement et de déchiffrement PGP

PGP (Pretty Good Privacy) utilise deux types d'algorithmes qui fonctionnent ensemble pour chiffrer et déchiffrer les fichiers dans les flux de travail :

1. Algorithmes de paires de clés : utilisés pour générer les paires de public/private clés pour le chiffrement et les signatures numériques
2. Algorithmes symétriques : utilisés pour chiffrer les données réelles du fichier (les algorithmes de paires de clés chiffrent la clé symétrique)

Algorithmes de paires de clés PGP

Choisissez l'un des algorithmes suivants lorsque vous générez des paires de clés PGP pour le déchiffrement du flux de travail :

RSA (recommandé)

Recommandé pour la plupart des utilisateurs. Largement soutenu, bien établi et. FIPS-compliant
Assure un bon équilibre entre sécurité et compatibilité.

ECC (cryptographie à courbe elliptique)

Plus efficace que RSA avec des clés de plus petite taille tout en garantissant une sécurité renforcée :

- Courbes NIST - Courbes standard largement prises en charge et FIPS-compliant
- BrainPool courbes - Courbes alternatives pour des exigences de conformité spécifiques
- Curve25519 - Courbe moderne à hautes performances offrant une sécurité renforcée avec un calcul efficace

ElGamal

Algorithme hérité. Pris en charge pour la compatibilité avec les anciens systèmes. Utilisez RSA ou ECC pour les nouvelles implémentations.

Pour obtenir des instructions détaillées sur la génération de clés PGP, consultez [Génération de clés PGP](#).

Algorithmes de chiffrement symétrique PGP

Ces algorithmes chiffrent les données réelles de vos fichiers. L'algorithme utilisé dépend de la façon dont le fichier PGP a été créé par votre logiciel PGP :

FIPS-compliant algorithmes (recommandés pour les environnements réglementés)

- AES-128, AES-192, AES-256 - Standard de cryptage avancé (recommandé)
- 3DES - Triple Data Encryption Standard (ancienne norme, utilisez AES dans la mesure du possible)

Autres algorithmes pris en charge

- IDEA, CAST5, Blowfish, DES,,, TwoFish CAMELLIA-128 CAMELLIA-192 CAMELLIA-256

Note

Vous ne choisissez pas directement l'algorithme symétrique lorsque vous utilisez des AWS Transfer Family flux de travail. Il est déterminé par le logiciel PGP utilisé pour créer le fichier crypté. Cependant, vous pouvez configurer votre logiciel PGP pour qu'il préfère des FIPS-compliant algorithmes tels que AES-256.

Pour plus d'informations sur les algorithmes symétriques pris en charge, consultez [Algorithmes de chiffrement symétriques pris en charge](#).

Génération de clés SSH 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 les clés SSH sont stockés dans le service. La clé SSH 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. Sur un même serveur, chaque utilisateur peut disposer de plusieurs clés SSH publiques sur fichier. 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 de AWS Directory Service pour Microsoft Active Directory](#).

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 clés SSH sous macOS, Linux ou Unix](#)
- [Création de clés SSH sous Microsoft Windows](#)
- [Conversion d'une clé SSH2 au format de clé publique SSH](#)

Création de clés SSH sous macOS, Linux ou Unix

Sur les systèmes d'exploitation macOS, Linux ou Unix, vous utilisez la `ssh-keygen` commande pour créer une clé publique SSH et une clé privée SSH, également appelées paire de clés.

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 créer des clés SSH 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 RSA-, ECDSA- et les clés. ED25519-formatted Choisissez la commande appropriée en fonction du type de paire de clés que vous générez.

Conseil : remplacez-le *key_name* par le nom réel de votre fichier de paire de clés SSH.

- Pour générer une paire de clés RSA 4096 bits :

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Pour générer une paire de clés ECDSA 521 bits (les tailles de bits de l'ECDSA sont de 256, 384 et 521) :

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Pour générer une paire de clés ED25519 :

```
ssh-keygen -t ed25519 -f key_name
```

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]-----+
```

Conseil : Lorsque vous exécutez la ssh-keygen commande comme indiqué ci-dessus, elle crée les clés publiques et privées sous forme de fichiers dans le répertoire en cours.

Votre paire de clés SSH est maintenant prête à être utilisée. Suivez les étapes 3 et 4 pour stocker la clé publique SSH 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 publique SSH 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.

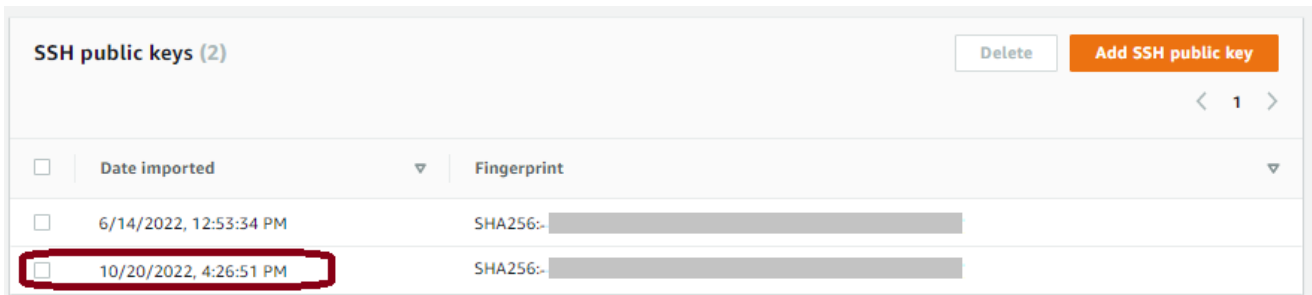
- d. Dans le volet Clés publiques SSH, choisissez Ajouter une clé publique SSH.

The screenshot shows the 'User: OneUser' configuration page in the AWS Transfer Family console. The breadcrumb trail is 'Transfer Family > Servers > s-[server icon] > User: OneUser'. At the top right are 'View logs' and 'Delete' buttons. The main section is titled 'User configuration' with an 'Edit' button. It is divided into two columns. The left column contains 'Role' (with a link to the role) and 'Posix Profile' (showing User ID: 2001, Group ID: 2001, and Secondary Group IDs: -). The right column contains 'Policy' (with a 'View' button) and 'Home directory' (set to '/fs-[path]' with 'Restricted' permissions). Below this is the 'SSH public keys (1)' section, which includes a 'Delete' button, an 'Add SSH public key' button, and a pagination control showing '1'. A table below lists the key with columns for 'Date imported' (6/14/2022, 12:53:34 PM) and 'Fingerprint' (SHA256-[fingerprint]).

- e. Collez le texte de la clé publique que vous avez générée dans la zone de texte de la clé publique SSH, puis choisissez Ajouter une clé.

The screenshot shows the 'Add key' dialog in the AWS Transfer Family console. The breadcrumb trail is 'Transfer Family > Servers > s-[server icon] > OneUser > Add key'. The dialog has a title 'Add key' and a section 'SSH public keys'. Inside this section, there is a link for 'SSH public key Info' and a prompt 'Paste the contents of SSH public key'. Below the prompt is a large text input field with the placeholder text 'Enter SSH public key'. At the bottom right of the dialog are 'Cancel' and 'Add key' buttons.

La nouvelle clé est répertoriée dans le volet des clés publiques SSH.



SSH public keys (2)			Delete	Add SSH public key
	Date imported	Fingerprint		
☐	6/14/2022, 12:53:34 PM	SHA256:-		
☐	10/20/2022, 4:26:51 PM	SHA256:-		

Création de clés SSH sous Microsoft Windows

Windows inclut OpenSSH en tant que fonctionnalité intégrée, que vous pouvez utiliser pour générer des clés SSH dans le même format que sous Linux ou macOS. Vous pouvez également utiliser des outils tiers tels que le générateur de clés de PuTTY (PuTTYgen).

Utilisation de l'OpenSSH intégré à Windows

Les versions récentes de Windows incluent OpenSSH par défaut. Vous pouvez utiliser les mêmes `ssh-keygen` commandes que celles décrites dans la macOS/Linux section :

1. Ouvrez Windows PowerShell ou une invite de commande.
2. Exécutez l'une des commandes suivantes en fonction du type de clé que vous souhaitez générer :

- Pour générer une paire de clés RSA 4096 bits :

```
ssh-keygen -t rsa -b 4096 -f key_name
```

- Pour générer une paire de clés ECDSA 521 bits :

```
ssh-keygen -t ecdsa -b 521 -f key_name
```

- Pour générer une paire de clés ED25519 :

```
ssh-keygen -t ed25519 -f key_name
```

3. Suivez les mêmes étapes que dans la macOS/Linux section pour télécharger votre clé publique sur AWS Transfer Family.

Utilisation de PuTTYgen (outil tiers)

Certains clients SSH tiers pour Windows, tels que PuTTY, utilisent différents formats de clés. PuTTY utilise le PPK format des clés privées. Si vous utilisez PuTTY ou des outils connexes tels que WinSCP, vous pouvez utiliser PuTTYgen pour créer des clés dans ce format.

Note

Si vous présentez à WinSCP un fichier de clé privée non formaté, ce client propose de convertir la clé .ppk .ppk en format pour vous.

[Pour un didacticiel sur la création de clés SSH à l'aide de PuttyGen, consultez le site Web. SSH.com](#)

Conversion d'une clé SSH2 au format de clé publique SSH

AWS Transfer Family accepte uniquement les clés SSH-formatted publiques. Si vous avez une clé publique SSH2, vous devez la convertir. Une clé publique SSH2 a le format suivant :

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAQEaiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----
```

Le format d'une clé publique SSH est le suivant :

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

Exécutez la commande suivante pour convertir une clé SSH2-formatted publique en clé SSH-formatted publique. *ssh2-key* Remplacez-le par le nom de votre clé SSH2 et *ssh-key* par le nom de votre clé SSH.

```
ssh-keygen -i -f ssh2-key.pub > ssh-key.pub
```

Faire pivoter les clés SSH

Pour des raisons de sécurité, nous recommandons la meilleure pratique qui consiste à faire pivoter vos clés SSH. 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 clés SSH peut être utilisée une seule fois. Cela élimine les risques liés au stockage des clés. Cependant, il est beaucoup plus courant de stocker les informations d'identification SSH 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.

 Note

Pour une rotation automatique des clés SSH utilisant l'infrastructure comme code, voir [Modules Transfer Family Terraform](#).

Il existe deux méthodes de rotation de clés SSH :

- Sur la console, vous pouvez télécharger une nouvelle clé publique SSH et supprimer une clé publique SSH existante.
- À l'aide de l'API, vous pouvez mettre à jour les utilisateurs existants en utilisant l'[DeleteSshPublicKey](#) API pour supprimer la clé publique Secure Shell (SSH) d'un utilisateur et l'[ImportSshPublicKey](#) API pour ajouter une nouvelle clé publique Secure Shell (SSH) au compte de l'utilisateur.

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 publique SSH, 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 publique SSH pour afficher la page Ajouter une clé.

5. Entrez la nouvelle clé publique SSH et choisissez Ajouter une clé.

 Important

Le format de la clé publique SSH dépend du type de clé que vous avez générée.

- Pour les clés RSA, le format est `ssh-rsa` *string*.
- Pour les clés ED25519, le format est `ssh-ed25519` *string*.
- Pour les clés ECDSA, la clé commence par `ecdsa-sha2-nistp256`, ou `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 publique SSH que vous venez de saisir apparaît dans la section Clés publiques SSH.

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 clés à l'aide de l'API

1. Sur les systèmes d'exploitation macOS, Linux ou Unix, ouvrez un terminal de commande.
2. Récupérez la clé SSH 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 au cours de cette procédure.

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":  
  "keyID",  
  "DateImported": 1621969331.072 } ],
```

3. Importez ensuite une nouvelle clé SSH 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 de clés PGP

Vous pouvez utiliser le décryptage Pretty Good Privacy (PGP) avec les fichiers que Transfer Family traite avec des flux de travail. Pour utiliser le déchiffrement dans une étape du flux de travail, fournissez une clé PGP. Pour des informations détaillées sur les algorithmes clés PGP, y compris les recommandations et la conformité à la norme FIPS, consultez [Algorithmes de paires de clés PGP](#)

Le blog sur le AWS stockage contient un article qui décrit comment simplement déchiffrer des fichiers sans écrire de code à l'aide des flux de travail Transfer Family Managed, [crypter et déchiffrer des fichiers avec](#) PGP et. AWS Transfer Family

L'opérateur que vous utilisez pour générer vos clés PGP 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. Selon 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 le site <https://gnupg.org/download/>.

Après avoir installé votre logiciel de génération de clés PGP, 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. Si vous choisissez ECC, vous pouvez choisir entre NIST BrainPool et Curve25519 pour la courbe elliptique.

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 clés PGP, utilisez 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 les informations de votre clé PGP. 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 clés PGP sous le nom `secretaws/transfer/server-id@pgp-default`, où se *server-id* trouve l'identifiant de votre serveur Transfer Family. Transfer Family utilise cette clé par défaut si aucune clé ne *user-name* correspond à l'utilisateur qui exécute le flux de travail.

Vous pouvez créer une clé pour un utilisateur spécifique. Dans ce cas, le format du nom du secret est `aws/transfer/server-id/user-name` le suivant : 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 privées PGP, par serveur Transfer Family, par utilisateur.

Pour configurer les clés PGP à utiliser avec le déchiffrement

1. Selon la version de GPG que vous utilisez, exécutez l'une des commandes suivantes pour générer une paire de clés PGP.
 - 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 ou l'autre **NIST**, **BrainPool** ou **Curve25519** pour la courbe elliptique. Si vous exécutez `gpg --gen-key` plutôt, vous créez une paire de clés qui utilise l'algorithme de chiffrement ECC Curve 25519.

- Pour les versions **GnuPG** antérieures à 2.3.0, vous pouvez utiliser la commande suivante, car RSA est le 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 stocker votre clé PGP.
 - 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 panneau 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 des Key/value paires, choisissez l'onglet Key/value.
 - 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 des Key/value paires, choisissez l'Key/value onglet.

- 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 lorsque vous avez généré votre paire de clés PGP.

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

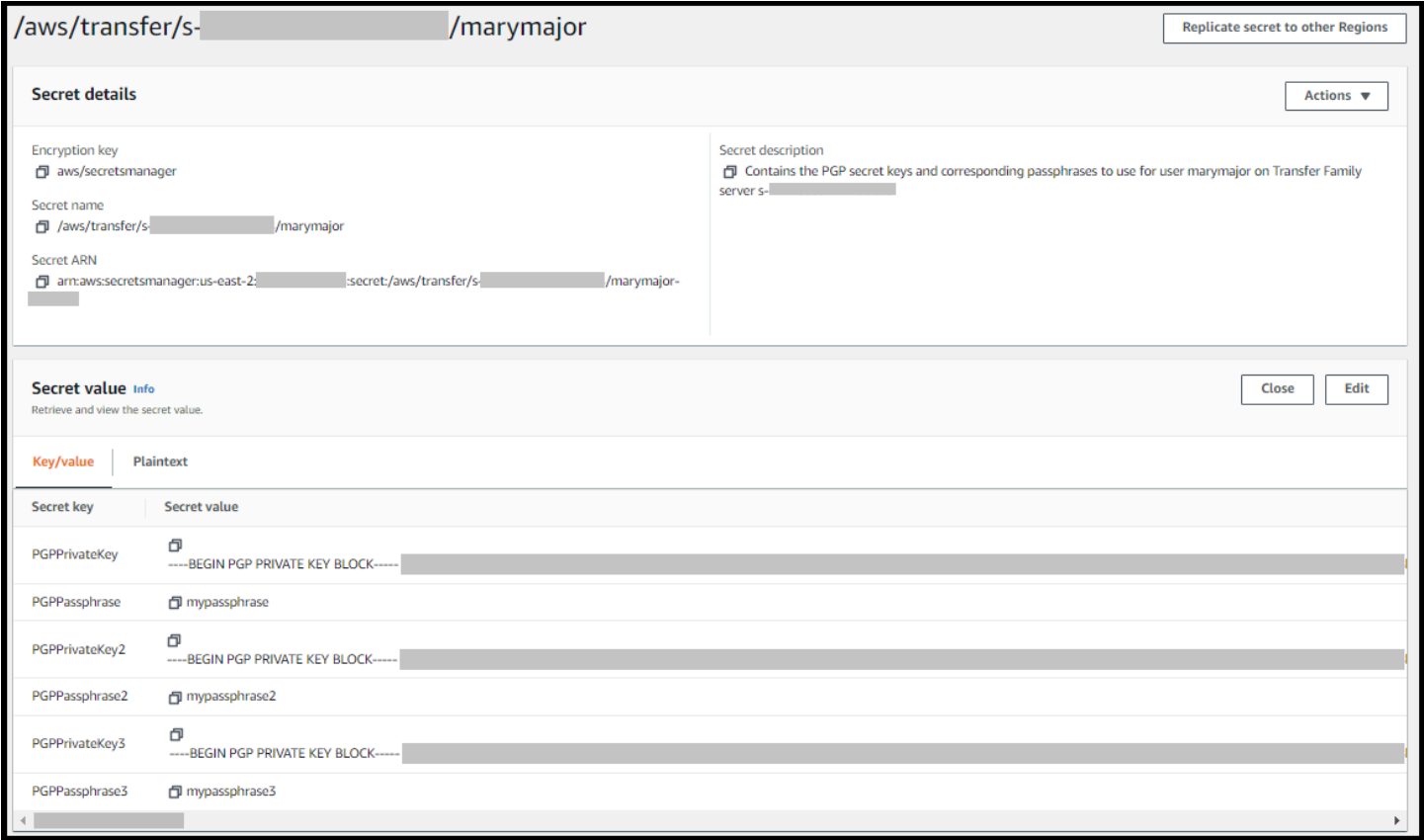
Vous pouvez ajouter jusqu'à 3 jeux de clés et de phrases de passe. Pour ajouter un deuxième ensemble, ajoutez deux nouvelles lignes, entrez **PGPPrivateKey2** et **PGPPassphrase2** pour les clés, puis collez une autre clé privée et une autre phrase secrète. Pour ajouter un troisième ensemble, les valeurs 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 par

user-name 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.



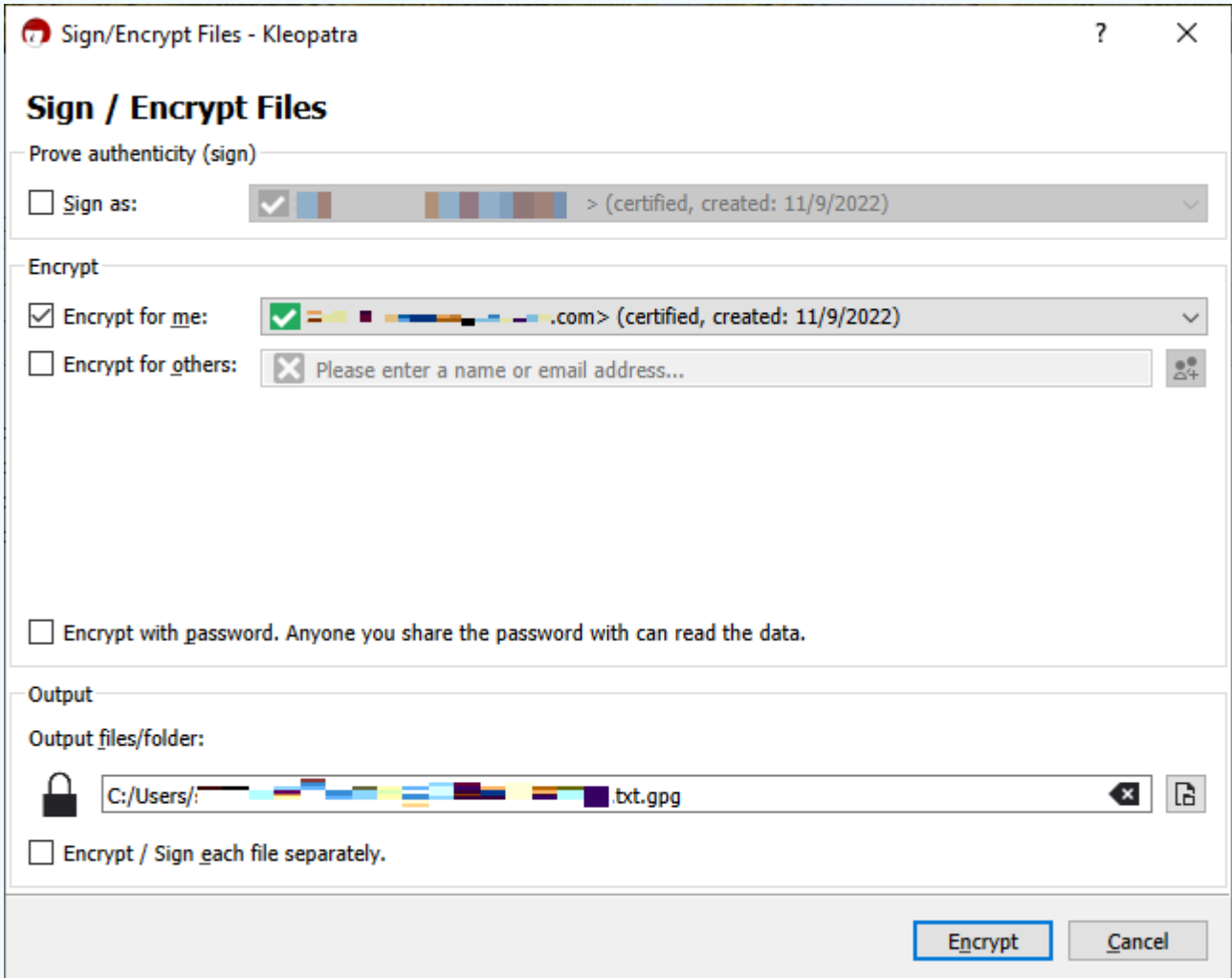
Clients PGP pris en charge

Les clients suivants ont été testés avec Transfer Family et peuvent être utilisés pour générer des clés PGP et pour chiffrer les 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.



Si vous signez le fichier chiffré et tentez de le télécharger sur un serveur Transfer Family avec un flux de déchiffrement, le message d'erreur suivant s'affiche :

Encrypted file with signed message unsupported

- Principales versions de GnuPG : 2.4, 2.3, 2.2, 2.0 et 1.4.

Notez que d'autres clients PGP 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

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS Transfer Family les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion de l'accès à l'aide de politiques](#)
- [Comment ? 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 identité et accès](#)
- [Clés de condition IAM pour la gouvernance organisationnelle](#)

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir [Résolution des problèmes AWS Transfer Family identité et accès](#))
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir [Comment ? AWS Transfer Family fonctionne avec IAM](#))
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir [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 en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez [Connexion à votre Compte AWS](#) dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez [Signature AWS Version 4 pour les demandes d'API](#) dans le Guide de l'utilisateur IAM.

Utilisateur racine d'un compte AWS

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez [Tâches qui requièrent les informations d'identification de l'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez [Qu'est-ce que IAM Identity Center ?](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un [utilisateur IAM](#) est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir [Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires](#) dans le guide de l'utilisateur IAM.

[Les groupes IAM](#) spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez [Cas d'utilisation pour les utilisateurs IAM](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en [passant d'un rôle utilisateur à un rôle IAM \(console\)](#) ou en appelant une opération AWS CLI ou AWS API. Pour plus d'informations, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez [Choix entre les politiques gérées et les politiques en ligne](#) dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques intégrées qui se trouvent dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez [Vue d'ensemble des listes de contrôle d'accès \(ACL\)](#) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez [Politiques de contrôle de service](#) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez [Politiques de contrôle des ressources \(RCP\)](#) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez [Politiques de session](#) dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section [Logique d'évaluation des politiques](#) dans le guide de l'utilisateur IAM.

Comment ? AWS Transfer Family fonctionne avec IAM

Avant d'utiliser Gestion des identités et des accès AWS (IAM) pour gérer l'accès à AWS Transfer Family, vous devez connaître les fonctionnalités IAM disponibles. AWS Transfer Family Pour obtenir une vue d'ensemble de la façon dont AWS Transfer Family les autres AWS services fonctionnent avec IAM, consultez la section [AWS Services compatibles avec IAM](#) dans le Guide de l'utilisateur d'IAM.

Rubriques

- [AWS Transfer Family politiques basées sur l'identité](#)
- [AWS Transfer Family stratégies basées sur les ressources](#)
- [Autorisation basée sur AWS Transfer Family tags](#)
- [AWS Transfer Family Rôles IAM](#)

AWS Transfer Family politiques basées sur l'identité

Avec les politiques basées sur l'identité IAM, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. AWS Transfer Family prend en charge des actions, ressources et clés de condition spécifiques. Pour en savoir plus sur tous les éléments que vous utilisez dans une politique JSON, consultez la [référence des éléments de stratégie JSON IAM](#) dans le guide de l'Gestion des identités et des accès AWS utilisateur.

Actions

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

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, vous devez inclure l'`transfer:CreateServer` action dans sa politique à l'aide de l'opération d'`CreateServerAPI` Transfer Family. 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 les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": ""
```

La ressource du serveur Transfer Family possède l'ARN suivant.

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

Par exemple, pour spécifier le serveur `s-01234567890abcdef` Transfer Family dans votre relevé, utilisez l'ARN suivant.

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

Pour plus d'informations sur le format des ARN, consultez [Amazon Resource Names \(ARN\)](#) dans le Service Authorization Reference ou [IAM ARN dans le guide de l'utilisateur IAM](#).

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 les politiques IAM. 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 autorisant l'accès aux serveurs et aux utilisateurs de Transfer Family. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN 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 les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément Condition indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

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, voir [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](#) Pour les politiques IAM spécifiques aux points de terminaison VPC, consultez. [Limiter l'accès aux points de terminaison VPC pour les serveurs Transfer Family](#)

AWS Transfer Family stratégies basées sur les ressources

Resource-based les politiques sont des documents de politique JSON 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* Resource-based les politiques 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 permettre un accès comptes multiples , vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que [principal dans une stratégie basée sur les ressources](#). L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource 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 les rôles IAM diffèrent des politiques basées sur les ressources](#) dans le Guide de l'Gestion des identités et des accès AWS utilisateur.

Le service Amazon S3 ne prend en charge qu'un seul type de politique basée sur les ressources, appelée *bucket* stratégie, 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 AWS Transfer Family tags

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 Rôles IAM

Un [rôle IAM](#) est une entité de votre AWS compte qui possède des autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec AWS Transfer Family

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous obtenez des

informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API 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, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou modifier les ressources AWS Transfer Family . Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour savoir comment créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez la section [Création de politiques dans l'onglet JSON du guide](#) de l'Gestion des identités et des accès AWS utilisateur.

Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Utilisation de AWS Transfer Family console](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)

Bonnes pratiques en matière de politiques

Identity-based les politiques 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 [politiques gérées par AWS](#) ou [politiques gérées par AWS pour les activités professionnelles](#) dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez [politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez [Conditions pour éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez [Validation de politiques avec IAM Access Analyzer](#) dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez [Sécurisation de l'accès aux API avec MFA](#) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez [Bonnes pratiques de sécurité dans IAM](#) dans le Guide de l'utilisateur IAM.

Utilisation de AWS Transfer Family console

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 (utilisateurs et rôles IAM) tributaires de cette politique.

Pour plus d'informations, consultez la section [Ajouter des autorisations à un utilisateur](#) dans le Guide de Gestion des identités et des accès AWS l'utilisateur.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API que vous tentez d'effectuer.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 à AWS Transfer Family ressources

Les conditions des politiques IAM 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 stratégie IAM, vous pouvez utiliser des clés de condition de balise 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 niveau de l'API. Vous pouvez également appliquer un contrôle plus dynamique qu'en utilisant le contrôle d'accès basé sur les ressources. Vous pouvez créer des politiques IAM qui autorisent ou refusent une opération en fonction des balises fournies dans la demande (balises de demande). Vous pouvez également créer des politiques IAM 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, consultez la section [Contrôle de l'accès aux AWS ressources à l'aide des balises de ressources](#) dans le guide

de l'utilisateur IAM. Pour plus de détails sur la spécification des politiques IAM avec API Gateway, consultez la section [Contrôler l'accès à une API avec des autorisations IAM](#) dans le guide du développeur d'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`, `UntagResource`, `StartServer`, `StopServer`, `DescribeServer`, et si la ressource utilisateur ou serveur est étiquetée avec la clé `stage` et la valeur `prod`.

```
{
  "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 identité et 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 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 pour accéder à mon AWS Transfer Family resources](#)

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 IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées concernant un élément `widget` mais ne dispose pas des autorisations `transfer:GetWidget` nécessaires.

```
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, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS Transfer Family. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

L'exemple de politique suivant contient l'autorisation de transmettre un rôle à AWS Transfer Family. **123456789012** Remplacez-le par votre identifiant de compte AWS et **MyTransferRole** par le nom de votre rôle IAM réel.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
      "Effect": "Allow"
    }
  ]
}
```

Je souhaite autoriser des personnes extérieures à mon AWS compte pour accéder à mon 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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises en charge par AWS Transfer Family, consultez [Comment ? AWS Transfer Family fonctionne avec IAM](#).
- Pour savoir comment fournir l'accès à vos ressources sur celles des Comptes AWS que vous possédez, consultez la section [Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez](#) dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section [Fournir un accès à des ressources Comptes AWS détenues par des tiers](#) dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez [Fournir un accès à des utilisateurs authentifiés en externe \(fédération d'identité\)](#) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Clés de condition IAM pour la gouvernance organisationnelle

AWS Transfer Family fournit des clés de condition IAM qui vous permettent de restreindre les configurations de ressources dans n'importe quelle politique IAM. Ces clés de condition peuvent être utilisées dans les politiques basées sur l'identité associées aux utilisateurs ou aux rôles, ou dans les politiques de contrôle des services (SCP) pour la gouvernance organisationnelle.

Les politiques de contrôle des services sont des politiques IAM qui s'appliquent à AWS l'ensemble d'une organisation et fournissent des garanties préventives sur plusieurs comptes. Lorsqu'elles sont utilisées dans les SCP, ces clés de condition permettent de faire respecter les exigences de sécurité et de conformité à l'échelle de l'organisation.

Voir aussi

- [Actions, ressources et clés de condition pour Transfer Family](#)
- [Politiques de contrôle de service \(SCP\)](#)
- Regardez [cette vidéo](#) qui explique comment appliquer des garde-fous préventifs à l'aide de politiques de contrôle des services

Clés de condition disponibles

AWS Transfer Family prend en charge les clés de condition suivantes à utiliser dans les politiques IAM :

`transfer:RequestServerEndpointType`

Limite la création et les mises à jour de serveurs en fonction du type de point de terminaison (PUBLIC, VPC, VPC_ENDPOINT). Couramment utilisé pour empêcher les terminaux destinés au public.

`transfer:RequestServerProtocols`

Limite la création et les mises à jour de serveurs en fonction des protocoles pris en charge (SFTP, FTPS, FTP, AS2).

`transfer:RequestServerDomain`

Limite la création de serveurs en fonction du type de domaine (S3, EFS).

`transfer:RequestConnectorProtocol`

Limite la création de connecteurs en fonction du protocole (AS2, SFTP).

Actions prises en charge

Les clés de condition peuvent être appliquées aux AWS Transfer Family actions suivantes :

- `CreateServer`: Supports `RequestServerEndpointType` `RequestServerProtocols` et clés de `RequestServerDomain` condition
- `UpdateServer`: Supports `RequestServerEndpointType` et clés de `RequestServerProtocols` condition
- `CreateConnector`: Supporte la clé de `RequestConnectorProtocol` condition

Exemple de politique SCP

L'exemple de SCP suivant empêche la création de AWS Transfer Family serveurs publics au sein de votre organisation :

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "DenyPublicTransferServers",
    "Effect": "Deny",
    "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
    "Resource": "*",
```

```
    "Condition": {
      "StringEquals": {
        "transfer:RequestServerEndpointType": "PUBLIC"
      }
    }
  }
}
```

Validation de conformité pour AWS Transfer Family

Third-party les auditeurs évaluent la sécurité et la conformité dans AWS Transfer Family le cadre de multiples programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, HIPAA. 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 pour la sécurité et la conformité HIPAA — Ce livre blanc](#) décrit comment les entreprises peuvent créer des applications AWS HIPAA-compliant
- [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 CSPM](#)— 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.

Pour tous les points de terminaison Transfer Family :

- La Zone-level redondance de disponibilité est intégrée au service.
- Il existe des flottes redondantes pour chaque AZ.
- Cette redondance est fournie automatiquement.

Note

Pour les points de terminaison d'un Virtual Private Cloud (VPC), il est possible de fournir un sous-réseau unique. Toutefois, nous vous recommandons de créer des points de terminaison dans plusieurs zones de disponibilité au sein de votre VPC, afin de réduire le risque d'interruptions de service en cas de panne de zone de disponibilité.

Voir aussi

- Pour plus de détails sur la création de serveurs Transfer Family dans un VPC, consultez [Création d'un serveur dans un cloud privé virtuel](#)
- Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section [Infrastructure AWS globale](#).
- Pour un exemple sur la manière de renforcer la redondance et de minimiser la latence du réseau en utilisant le Latency-based routage, consultez le billet de blog [Minimisez la latence du réseau avec vos AWS Transfer Family serveurs](#).

Créez une connexion privée entre un VPC et AWS Transfer Family API

Vous pouvez établir une connexion privée entre votre VPC et les AWS Transfer Family API en créant un point de terminaison VPC d'interface, alimenté par. [AWS PrivateLink](#) Vous pouvez accéder aux AWS Transfer Family API comme si elles se trouvaient dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou de connexion Direct AWS Connect. Les instances de votre VPC ne requièrent pas d'adresses IP publiques pour communiquer avec les API AWS Transfer Family .

Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface. Pour plus d'informations, consultez la section [Accès aux AWS services AWS PrivateLink](#) dans le AWS PrivateLink Guide. Avant de configurer un point de terminaison VPC d'interface pour les AWS Transfer Family API, consultez les [considérations](#) du AWS PrivateLink guide.

Contrôle de l'accès à l'aide des politiques de point de terminaison VPC

Par défaut, l'accès complet aux AWS Transfer Family API est autorisé via le point de terminaison. Vous pouvez contrôler l'accès au point de terminaison de l'interface à l'aide des politiques de point de terminaison VPC. Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès aux AWS Transfer Family API. La politique spécifie les informations suivantes :

- Le principal qui peut effectuer des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être effectuées.

Pour plus d'informations, consultez [Contrôle de l'accès aux services avec points de terminaison d'un VPC](#) dans le Guide de l'utilisateur Amazon VPC.

Voici un exemple de politique de point de terminaison pour les AWS Transfer Family API. Lorsqu'elle est attachée à un point de terminaison, cette politique accorde l'accès à toutes les actions de l' AWS Transfer Family API sur toutes les ressources, à l'exception de celles qui sont étiquetées avec une clé Environment et une valeurTest.

```
{
```

```
"Statement": [{
  "Effect": "Deny",
  "Action": "transfer:StartFileTransfer",
  "Principal": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:ResourceTag/Environment": "Test"
    }
  }
}, {
  "Effect": "Allow",
  "Action": "transfer:*",
  "Principal": "*",
  "Resource": "*"
}]
}
```

Créez un point de terminaison VPC d'interface pour AWS Transfer Family API

Vous pouvez créer un point de terminaison VPC pour les AWS Transfer Family API à l'aide de la console Amazon VPC ou de l'interface de ligne de commande (CLI) AWS. Pour plus d'informations, consultez [Créer un point de terminaison d'un VPC](#) dans le Guide AWS PrivateLink.

Créez un point de terminaison VPC pour les AWS Transfer Family API en utilisant l'un des noms de service suivants :

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips`— Pour créer un point de terminaison VPC d'interface conforme à la publication 140-3 du Federal Information Processing Standard (FIPS), norme gouvernementale américaine.

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d' AWS Transfer Family API aux API en utilisant son nom DNS par défaut pour la région, par exemple, `transfer.us-east-1.amazonaws.com`.

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 des appels d'API AWS publiés pour accéder AWS Transfer Family via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Des suites de chiffrement dotées d'un secret de transmission parfait (PFS), telles que DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

Évitez de placer les NLB et les NAT devant AWS Transfer Family serveurs

Note

Les serveurs configurés avec les protocoles FTP et FTPS autorisent uniquement une configuration avec un VPC : aucun point de terminaison public n'est disponible pour. FTP/FTPS

De nombreux clients configurent un Network Load Balancer (NLB) pour acheminer le trafic vers leur serveur. AWS Transfer Family Ils le font généralement soit parce qu'ils ont créé leur serveur AWS avant de pouvoir y accéder à la fois depuis leur VPC et depuis Internet, soit pour prendre en charge le protocole FTP sur Internet. Cette configuration augmente non seulement les coûts pour les clients, mais peut également entraîner d'autres problèmes, décrits dans cette section.

Les passerelles NAT sont un composant obligatoire lorsque les clients se connectent à partir d'un réseau privé protégé par un pare-feu d'entreprise. Sachez toutefois que lorsque de nombreux clients se trouvent derrière la même passerelle NAT, cela peut avoir un impact sur les performances et les limites de connexion. S'il existe un NLB ou un NAT dans le chemin de communication entre le client et le serveur FTP ou FTPS, le serveur ne peut pas reconnaître avec précision l'adresse IP du client, car AWS Transfer Family il ne voit que l'adresse IP du NLB ou du NAT.

Si vous utilisez la configuration d'un serveur Transfer Family derrière un NLB, nous vous recommandons de passer à un point de terminaison VPC et d'utiliser une adresse IP Elastic au lieu d'utiliser un NLB. Lorsque vous utilisez des passerelles NAT, tenez compte des limites de connexion décrites ci-dessous.

Si vous utilisez le protocole FTPS, cette configuration réduit non seulement votre capacité à vérifier qui accède à votre serveur, mais elle peut également avoir un impact sur les performances. AWS Transfer Family utilise l'adresse IP source pour partager vos connexions sur notre plan de données. Pour le FTPS, cela signifie qu'au lieu d'avoir 10 000 connexions simultanées, les serveurs Transfer Family avec des passerelles NLB ou NAT sur la route de communication sont limités à seulement 300 connexions simultanées.

Bien que nous vous recommandions d'éviter les équilibreurs de charge réseau placés devant AWS Transfer Family les serveurs, si votre implémentation FTP ou FTPS nécessite un NLB ou un NAT dans la route de communication en provenance du client, suivez les recommandations suivantes :

- Pour un NLB, utilisez le port 21 pour les contrôles de santé, au lieu des ports 8192-8200.
- Pour le AWS Transfer Family serveur, activez la reprise de session TLS en `TlsSessionResumptionMode = ENFORCED` configurant.

 Note

Il s'agit du mode recommandé, car il offre une sécurité renforcée :

- Exige que les clients utilisent la reprise de session TLS pour les connexions suivantes.
 - Fournit des garanties de sécurité renforcées en garantissant des paramètres de chiffrement cohérents.
 - Aide à prévenir les attaques de rétrogradation potentielles.
 - Maintient la conformité aux normes de sécurité tout en optimisant les performances.
- Si possible, évitez d'utiliser un NLB pour tirer pleinement parti des limites de AWS Transfer Family performances et de connexion.

Pour obtenir des conseils supplémentaires sur les alternatives NLB, contactez l'équipe de gestion des AWS Transfer Family produits via le AWS Support. Pour plus d'informations sur l'amélioration de votre niveau de sécurité, consultez le billet de blog [Six conseils pour améliorer la sécurité de votre AWS Transfer Family serveur](#).

Sécurité de l'infrastructure de connectivité VPC

Les connecteurs SFTP avec sortie VPC améliorent la sécurité de l'infrastructure grâce à l'isolation du réseau et à la connectivité privée :

Avantages de l'isolation du réseau

- **Trafic réseau privé** : tout le trafic du connecteur vers les serveurs SFTP privés reste dans votre VPC et ne transite jamais par l'Internet public.
- **Sortie contrôlée** : pour les points de terminaison publics accessibles via VPC, le trafic passe par vos passerelles NAT, ce qui vous permet de contrôler les adresses IP de sortie et les politiques réseau.
- **Contrôles de sécurité VPC** : exploitez les groupes de sécurité VPC, les ACL réseau et les tables de routage existants pour contrôler l'accès au réseau des connecteurs.
- **Connectivité hybride** : accédez aux serveurs SFTP sur site via des connexions VPN ou Direct Connect établies sans exposition supplémentaire à Internet.

Considérations de sécurité relatives à Resource Gateway

Les passerelles de ressources fournissent des points d'entrée sécurisés pour l'accès aux Cross-VPC ressources :

- **Multi-AZ déploiement** : les passerelles de ressources nécessitent des sous-réseaux situés dans au moins deux zones de disponibilité pour garantir une haute disponibilité et une tolérance aux pannes.
- **Contrôles des groupes de sécurité** : configurez les groupes de sécurité pour restreindre l'accès aux ports SFTP (généralement le port 22) aux seules sources autorisées.
- **Emplacement des sous-réseaux privés** : déployez des passerelles de ressources dans des sous-réseaux privés lors de la connexion à des serveurs SFTP privés afin de maintenir l'isolation du réseau.
- **Limites de connexion** : chaque passerelle de ressources prend en charge jusqu'à 350 connexions simultanées avec un délai d'inactivité de 350 secondes pour les connexions TCP.

Ajouter un pare-feu pour applications Web

AWS WAF est un pare-feu d'applications Web qui aide à protéger les applications Web et les API contre les attaques. Vous pouvez l'utiliser pour configurer un ensemble de règles appelé liste de contrôle d'accès Web (ACL Web) 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 vos API](#).

Pour ajouter AWS WAF

1. Ouvrez la console API Gateway à l'adresse <https://console.aws.amazon.com/apigateway/>.
2. Dans le volet de navigation des API, 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 l'ACL Web que vous souhaitez associer à cette étape.
 - Si l'ACL Web dont vous avez besoin n'existe pas, vous devez en créer une en procédant comme suit :
 1. Choisissez Create Web ACL.
 2. Sur la page d'accueil du service AWS WAF, choisissez Create web ACL.
 3. Dans Détails de l'ACL Web, dans Nom, tapez le nom de l'ACL Web.
 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, reportez-vous à la section [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'action ACL Web par défaut pour les demandes qui ne correspondent 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 Create web ACL.
7. Choisissez Save Changes (Enregistrer les modifications).
 8. Sélectionnez Ressources.
 9. Pour Actions, choisissez Deploy API.

Pour plus d'informations sur le niveau de sécurité de Transfer Family avec un pare-feu d'application AWS Web, consultez la section [Securing Transfer Family with AWS application firewall et Amazon API Gateway](#) sur le blog AWS consacré au stockage.

Cross-service prévention confuse 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. Cross-service l'usurpation d'identité 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 l'utilisateur IAM.

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 l'adjoint confus consiste à utiliser l'Amazon Resource Name (ARN) exact 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 de l'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 ARN utilisateur de Transfer Family.
- **Rôle d'accès** — Permet d'accéder uniquement aux fichiers Amazon S3 en cours de transfert. Pour les transferts AS2 entrants, le rôle d'accès utilise l'Amazon Resource Name (ARN) pour l'accord. Pour les transferts AS2 sortants, le rôle d'accès utilise l'ARN du 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 ARN de serveur Transfer Family.
- **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 ARN de serveur Transfer Family. Pour les transferts AS2 sortants, le rôle de journalisation utilise l'ARN du connecteur.
- **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 (ARN) Transfer Family.

Pour plus d'informations, consultez [Politiques et autorisations dans IAM](#) dans le Guide de l'utilisateur IAM.

 Note

Dans les exemples suivants, remplacez chacune *user input placeholder* par 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": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012: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": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012: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:us-
east-1:123456789012:user/server-id/user-name"
        }
    }
}
]
}

```

AWS Transfer Family : flux de travail, 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": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333: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:us-
west-2:111122223333:workflow/workflow-id"
        }
      }
    }
  ]
}
```

AWS Transfer Family Connector : rôle, interservices, prévention des adjoints confus

L'exemple de politique suivant permet à n'importe quel connecteur 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": "123456789012"
        },
        "ArnLike": {
```

```

        "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:connector/*"
      }
    }
  ]
}

```

L'exemple de politique suivant permet à un connecteur 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:us-east-1:123456789012:connector/connector-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 détails de l'ARN d'un flux de travail si aucun flux de travail n'est associé à votre serveur.

L'exemple de logging/invoction politique 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": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:transfer:us-west-2:111122223333:server/*",
            "arn:aws:transfer:us-west-2:111122223333:workflow/*"
          ]
        }
      }
    }
  ]
}
```

L'exemple de logging/invoction politique 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": "111122223333"
        },
        "ArnEquals": {
            "aws:SourceArn": [
                "arn:aws:transfer:us-west-2:111122223333:server/server-id",
                "arn:aws:transfer:us-west-2:111122223333: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 des politiques Gestion des identités et des accès AWS \(IAM\) 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 gérées par AWS, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM. 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 la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page [politiques gérées par AWS pour les fonctions de tâche](#) dans le Guide de l'utilisateur IAM.

AWS politique gérée : `AWSTransferConsoleFullAccess`

La `AWSTransferConsoleFullAccess` politique fournit un accès complet à Transfer Family via la console AWS de gestion. Pour plus d'informations, voir [Service-linked le rôle de AWS Transfer Family](#).

AWS politique gérée : `AWSTransferFullAccess`

La `AWSTransferFullAccess` politique fournit un accès complet aux services Transfer Family. Pour plus d'informations, voir [Service-linked le rôle de AWS Transfer Family](#).

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. Pour plus d'informations, voir [Service-linked le rôle de AWS Transfer Family](#).

AWS politique gérée : `AWSTransferReadOnlyAccess`

La `AWSTransferReadOnlyAccess` politique fournit un accès en lecture seule aux services Transfer Family. Pour plus d'informations, voir [Service-linked le rôle de AWS Transfer Family](#).

AWS Mises à jour de Transfer Family vers AWS stratégies 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 obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page [Historique du document pour AWS Transfer Family](#).

Modifier	Description	Date
Mise à jour de la documentation	Des sections ont été ajoutées pour chacune des politiques gérées par Transfer Family.	27 janvier 2022
AWSTransferReadOnlyAccess : 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

Modules Transfer Family Terraform

[HashiCorpTerraform](#) est un moteur d'infrastructure en tant que code (IaC) open source développé à l'aide du langage de HashiCorp configuration (HCL). Terraform fournit un flux de travail d'interface de ligne de commande (CLI) cohérent qui, associé à AWS Transfer Family pour l'infrastructure principale, peut gérer des centaines de services cloud et codifier les API cloud dans des fichiers de configuration déclaratifs.

Vous pouvez utiliser Terraform pour déployer en toute sécurité les serveurs et connecteurs SFTP AWS Transfer Family, ainsi que les dépendances et personnalisations associées. Pour le référentiel contenant le code Terraform permettant de créer les ressources nécessaires à l'exécution de AWS Transfer Family, consultez le code source du module [Terraform Transfer Family](#) sur GitHub.

Note

Les modules AWS Transfer Family pour Terraform sont le fruit d'un effort soutenu par la communauté. Ils ne font partie d'aucun AWS service. Best-effort le support est fourni par la communauté AWS Storage.

Serveurs SFTP

Cette automatisation vous fournit un module Terraform personnalisable et des exemples de bout en bout pour créer un point de terminaison SFTP (PUBLIC ou des types de points de VPC terminaison), intégrer Amazon CloudWatch pour la journalisation et la surveillance, gérer les identités des utilisateurs pour l'accès aux points de terminaison et configurer les rôles IAM pour l'accès aux compartiments Amazon S3 où les fichiers sont stockés. Le module prend en charge plusieurs clés publiques SSH par utilisateur (jusqu'à 50 clés) pour une sécurité améliorée et des capacités de rotation des clés.

Connecteurs SFTP

AWS Le module Transfer Family Terraform prend désormais en charge le déploiement de connecteurs SFTP pour transférer des fichiers entre Amazon S3 et des serveurs SFTP distants. Les connecteurs SFTP fournissent une fonctionnalité entièrement gérée et à faible code pour copier des fichiers entre Amazon S3 et des serveurs SFTP distants.

Vous pouvez désormais utiliser Terraform pour provisionner par programmation vos connecteurs SFTP, les dépendances associées et les personnalisations en un seul déploiement. Le module fournit également des exemples de bout en bout pour automatiser les flux de travail de transfert de fichiers en fonction d'un calendrier ou de déclencheurs d'événements. L'utilisation de Terraform pour le déploiement élimine le besoin de configurations manuelles fastidieuses et sujettes aux erreurs, et vous offre une option de déploiement rapide, reproductible et sécurisée qui peut évoluer.

AS2

Pour montrer la prise en charge des modèles AS2 Terraform, ajoutez une réaction positive (#) à la demande de fonctionnalité des modèles Transfer [Family Terraform](#). Vous pouvez également ajouter un commentaire décrivant votre cas d'utilisation.

Échange de données B2B

AWS B2B Échange de données automatise la transformation, la validation et la génération de documents d'échange de données informatisé (EDI) vers et depuis les formats de données JSON et XML. [Pour montrer la prise en charge des modèles Terraform pour l'échange de données B2B, ajoutez une réaction positive \(#\) à la demande de fonctionnalité.](#) Vous pouvez également ajouter un commentaire décrivant votre cas d'utilisation.

Résolution des problèmes AWS Transfer Family

Ce chapitre fournit des informations de résolution des problèmes courants que vous pouvez rencontrer lors de l'utilisation AWS Transfer Family. Chaque section se concentre sur un domaine de fonctionnalité spécifique pour vous aider à trouver rapidement des solutions à vos problèmes.

- Pour les problèmes liés à l'IAM dans Transfer Family, consultez [Résolution des problèmes AWS Transfer Family identité et accès](#).
- Pour les problèmes liés à vos applications Web Transfer Family, consultez [Résolution des problèmes liés à vos applications Web](#).

Rubriques

- [Résoudre les problèmes d'authentification](#)
- [Résoudre les problèmes liés au connecteur SFTP](#)
- [Résoudre les problèmes de connectivité et de transfert SFTP](#)
- [Résoudre les problèmes liés au fournisseur d'identité personnalisé](#)
- [Résoudre les problèmes liés au flux de travail](#)
- [Résoudre les problèmes liés à l'EFS](#)
- [Résoudre les problèmes de stockage et de chiffrement](#)
- [Résoudre les problèmes de surveillance et d'alerte](#)
- [Résoudre les problèmes de transfert entre régions](#)
- [Résoudre les problèmes de déploiement de Terraform](#)
- [Résoudre les problèmes d'intégration du Web Application Firewall](#)
- [Résoudre les problèmes des utilisateurs gérés par les services](#)
- [Résoudre les problèmes liés à l'AS2](#)

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](#)

- [Limites de groupe Active Directory dépassées](#)
- [Problèmes d'authentification divers](#)
- [Résoudre les problèmes liés à Amazon API Gateway](#)
- [Résoudre les problèmes liés au test de votre fournisseur d'identité](#)
- [Dupliquer des compartiments Amazon S3 dans une application Web](#)

Défaillances d'authentification : SSH/SFTP

Description

Lorsque vous essayez de vous connecter à votre serveur à l'aide du protocole de transfert de fichiers (SFTP) Secure Shell (SSH), 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 Gateway et que vous recevez cette erreur, consultez [Trop d'échecs d'authentification](#).

Cause

Vous n'avez pas ajouté de paire de clés RSA pour votre utilisateur. Vous devez donc vous authentifier à l'aide d'un mot de passe.

Solution

Lorsque vous exécutez la `sftp` commande, spécifiez `-o 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).

Limites de groupe Active Directory dépassées

Description

Lorsque vous tentez d'ajouter d'autres groupes Active Directory à votre AWS Transfer Family serveur, vous recevez un message d'erreur indiquant que vous avez atteint le nombre maximum de groupes autorisés.

Cause

AWS Transfer Family a une limite par défaut de 100 groupes Active Directory par serveur.

Solution

Voici deux solutions possibles :

- Consolidez vos groupes Active Directory pour réduire le nombre total nécessaire.
- Si votre cas d'utilisation nécessite plus de 100 groupes, envisagez d'utiliser une solution de fournisseur d'identité personnalisée, comme décrit dans [Simplifier l'authentification Active Directory avec un fournisseur d'identité personnalisé pour AWS Transfer Family](#).

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, /amzn-s3-demo-bucket/images c'est acceptable, mais /amzn-s3-demo-bucket/images/ ne amzn-s3-demo-bucket/images l'est pas.

Résoudre les problèmes liés à Amazon API Gateway

Cette section décrit les solutions possibles aux problèmes d'API Gateway 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 SFTP (Secure Shell), 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, l'ARN du rôle n'est qu'un espace réservé, comme l'indique la valeur d'ID de rôle de tous les zéros :

```
{
```



```
"Response": "{\n  \"Role\": \"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",\n  \"HomeDirectory\": \"\\\"/\\\"\",\n  \"StatusCode\": 200,\n  \"Message\": \"\",\n  \"Url\": \"https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/servers/transfer-server-ID/users/myuser/config\"\n}
```

Solution

Remplacez l'ARN du rôle fictif par un rôle réel autorisé à accéder au serveur.

Pour mettre à jour le rôle

1. Ouvrez la 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 ARN de rôle 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. Sur la *stack* page de révision, sélectionnez Je reconnais que cela AWS CloudFormation pourrait créer des ressources IAM, puis choisissez Update stack.

Connexion fermée

Description

Lorsque vous essayez de vous connecter à votre serveur à l'aide du protocole SFTP (Secure Shell), le message d'erreur suivant s'affiche :

Connection closed

Cause

Ce problème peut être dû au fait 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 au test de votre fournisseur d'identité

Description

Si vous testez votre fournisseur d'identité à l'aide de la console ou de l'opération `TestIdentityProvider` API, 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.

Dupliquer des compartiments Amazon S3 dans une application Web

Description

Le même bucket Amazon S3 apparaît plusieurs fois dans l'interface de l'application Web Transfer Family.

Cause

Cela se produit lorsqu'un utilisateur appartient à plusieurs groupes Active Directory qui ont des autorisations pour le même compartiment Amazon S3. L'application Web répertorie toutes les autorisations de haut niveau associées à l'UID ou au GID de l'utilisateur, y compris les autorisations dupliquées pour le même emplacement de compartiment.

Solution

Pour éviter les doublons dans les offres, consolidez les autorisations afin que chaque utilisateur ne dispose que d'une seule subvention par site Amazon S3. Passez en revue la configuration de vos subventions d'accès Amazon S3 et supprimez les autorisations redondantes pour le même compartiment dans différents groupes Active Directory.

Résoudre les problèmes liés au connecteur SFTP

Cette section décrit les solutions possibles aux problèmes liés aux connecteurs SFTP.

Rubriques

- [Résoudre les problèmes liés à l'ajout de clés d'hôte fiables pour votre connecteur SFTP](#)
- [Échec d'une négociation clé](#)
- [Régulation du connecteur SFTP](#)
- [Optimisation des performances du connecteur SFTP](#)
- [Résoudre les problèmes de connectivité VPC](#)
- [Problèmes divers liés au connecteur SFTP](#)

Résoudre les problèmes liés à l'ajout de clés d'hôte fiables pour votre connecteur SFTP

Description

Lorsque vous créez ou modifiez un connecteur SFTP 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...==
```

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 [Politiques de sécurité pour AWS Transfer Family Connecteurs SFTP](#).

Régulation du connecteur SFTP

Description

Lorsque vous utilisez des connecteurs SFTP pour les transferts de fichiers, vous rencontrez des erreurs telles que :

```
{"type":"ExecutionThrottled","details":{},"connectorId":"c-1234567890abcdef0"}
```

Ou vous remarquez que les transferts de fichiers sont retardés ou échouent par intermittence lors d'opérations à volume élevé.

Cause

Les connecteurs SFTP ont des quotas de service qui limitent le nombre de transferts de fichiers et d'opérations d'API simultanés. Lorsque ces limites sont dépassées, des restrictions ont lieu pour protéger le service et garantir une utilisation équitable par tous les clients.

Solution

Pour résoudre les problèmes liés au connecteur SFTP, essayez les solutions suivantes :

1. Implémentez une logique de ralentissement exponentiel et de nouvelle tentative dans vos applications. Par exemple, créez une fonction qui réessaie automatiquement les opérations ayant échoué en augmentant les temps d'attente entre les tentatives.
2. Implémentez la limitation de débit dans votre application :
 - Limitez le nombre de transferts simultanés.
 - Ajoutez des délais entre les lots de transferts.
3. Surveillez votre utilisation par rapport aux quotas de service :
 - Utilisez CloudWatch des métriques pour suivre l'utilisation de l'API.
 - Configurez des alarmes pour vous avertir lorsque vous approchez des limites de quota.
4. Pour connaître les options permettant de dimensionner vos connecteurs SFTP, consultez [Dimensionnement de vos connecteurs SFTP](#).
5. Si le ralentissement persiste et a un impact sur vos activités commerciales, demandez une augmentation de quota via la console Service Quotas.

Optimisation des performances du connecteur SFTP

Description

Les transferts de votre connecteur SFTP sont plus lents que prévu ou vous constatez des performances irrégulières.

Cause

Les performances du connecteur SFTP peuvent être affectées par divers facteurs, notamment les conditions du réseau, la taille des fichiers, la configuration du serveur distant et les limites de transfert simultané.

Solution

Pour optimiser les performances du connecteur SFTP :

- Configurez votre serveur SFTP distant pour des performances optimales :
 - Augmenter le nombre maximum de sessions et de transferts par session
 - Optimisez la taille des fenêtres TCP pour les connexions à latence élevée
 - Utilisez la compression si elle est prise en charge par les deux extrémités
- Envisagez d'optimiser le réseau en plaçant votre connecteur Transfer Family dans une région proche de votre serveur SFTP distant.
- Mettez en œuvre une stratégie de surveillance pour identifier les goulots d'étranglement liés aux performances :
 - Surveillez le débit et la latence du réseau
 - Analyser les journaux pour détecter les modèles de lenteur des transferts

Résoudre les problèmes de connectivité VPC

Cette section décrit les solutions aux problèmes courants liés aux connecteurs LATTICE-enabled VPC_SFTP.

Connecteur bloqué dans le statut EN ATTENTE

Description

Votre connecteur VPC_ LATTICE-enabled SFTP reste en PENDING état pendant une période prolongée (plus de 10 minutes).

Cause

Cela peut être dû à des retards de résolution DNS, à des problèmes de configuration de Resource Gateway ou à des problèmes d'association au réseau du service VPC Lattice.

Solution

[Contactez AWS Support](#)[AWS Contact.pour](#) nous aider à analyser la cause première du problème. Vous pouvez également essayer la solution suivante.

1. Vérifiez que le statut de votre passerelle de ressources est en ACTIVE bon état :

```
aws vpc-lattice get-resource-gateway --resource-gateway-  
identifiant rgw-1234567890abcdef0
```

2. Vérifiez que votre configuration de ressources est correctement configurée et active :

```
aws vpc-lattice get-resource-configuration --resource-configuration-  
identifiant rcfg-1234567890abcdef0
```

3. Assurez-vous que votre passerelle de ressources possède des sous-réseaux dans au moins deux zones de disponibilité qui prennent en charge le VPC Lattice.
4. Si le problème persiste, supprimez et recréez le connecteur avec la même configuration.

Connecteur en état ERROED

Description

Votre connecteur VPC_ LATTICE-enabled SFTP affiche l'ERRORÉtat avec les détails de l'erreur.

Cause

Les causes courantes incluent un ARN de configuration des ressources non valide, des adresses IP insuffisantes dans les sous-réseaux VPC ou des tentatives de partage de ressources entre régions.

Solution

1. Vérifiez les détails de l'erreur à l'aide de `describe-connector` :

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. Vérifiez que l'ARN de configuration des ressources est correct et qu'il se trouve dans la même région que votre connecteur.
3. Assurez-vous que vos sous-réseaux VPC disposent de suffisamment d'adresses IP disponibles pour la passerelle de ressources.

4. Vérifiez que votre cible de configuration des ressources (adresse IP ou nom DNS) est accessible depuis votre VPC.

Erreur d'adresse IP publique non prise en charge

Description

Vous recevez un message d'erreur lorsque vous essayez de créer une configuration de ressources avec une adresse IP publique : `ValidationException: IP address x.x.x.x is not in allowed ranges.`

Cause

Les configurations de ressources pour les points de terminaison publics doivent utiliser des noms DNS et non des adresses IP.

Solution

Utilisez le nom DNS public de votre serveur SFTP au lieu de son adresse IP lors de la création de la configuration des ressources :

```
aws vpc-lattice create-resource-configuration \  
  --name my-public-server-config \  
  --resource-gateway-identifier rgw-1234567890abcdef0 \  
  --resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \  
  --port-ranges 22
```

Erreur relative à la zone de disponibilité non prise en charge

Description

Vous recevez un message d'erreur lors de la création d'une passerelle de ressources : `Subnet subnet-xxx is not valid because it is not in a supported Availability Zone.`

Cause

Toutes les zones de disponibilité ne prennent pas en charge l'accès aux ressources en réseau Cross-VPC VPC. Le message d'erreur répertorie les AZ prises en charge pour votre région.

Solution

1. Créez des sous-réseaux dans les zones de disponibilité prises en charge répertoriées dans le message d'erreur.
2. Mettez à jour votre passerelle de ressources pour utiliser uniquement les sous-réseaux des zones de disponibilité prises en charge.
3. Assurez-vous d'avoir au moins deux sous-réseaux dans différentes zones de disponibilité prises en charge.

Délais de connexion avec les connecteurs VPC_LATTICE

Description

Les transferts de fichiers via les connecteurs VPC expirent ou échouent par intermittence.

Cause

VPC Lattice a des limites de connexion (350 connexions par ressource) et des délais d'inactivité (350 secondes pour TCP).

Solution

1. Surveillez les connexions simultanées pour respecter la limite de 350 connexions par ressource.
2. Implémentez le regroupement et la réutilisation des connexions dans vos applications.
3. Configurez les valeurs de délai d'expiration appropriées dans vos applications clientes SFTP (moins de 350 secondes).
4. Envisagez de créer plusieurs configurations de ressources pour la même cible afin de répartir la charge.

Problèmes divers liés au connecteur SFTP

Description

Vous recevez une erreur après l'exécution `StartFileTransfer`, mais vous ne connaissez pas la cause du problème, et seul l'ID du connecteur est renvoyé après l'appel d'API.

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 connecteur SFTP](#). 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 de la commande [TestConnection](#) API.
- Afficher CloudWatch les journaux de votre connecteur : voir [Exemples d'entrées de journal pour les connecteurs SFTP](#). Cette rubrique fournit des exemples d'entrées de journal du connecteur SFTP, ainsi que la convention de dénomination pour vous aider à trouver les journaux appropriés.

Résoudre les problèmes de connectivité et de transfert SFTP

Cette section décrit les solutions possibles aux problèmes de connectivité SFTP et de transfert de fichiers.

Rubriques

- [Résoudre les problèmes de connectivité SFTP](#)
- [Résoudre les problèmes liés au client SFTP](#)
- [Résoudre les problèmes de téléchargement de fichiers](#)
- [Résoudre les problèmes de connecteur SFTP de type VPC de sortie](#)

Résoudre les problèmes de connectivité SFTP

Description

Votre client SFTP ne parvient pas à établir la connexion. Ce problème peut se produire de façon continue ou intermittente. Par exemple, vous pouvez voir la séquence d'événements suivante dans les journaux de débogage de votre client SFTP :

```
sftp -vvv username@1.1.1.1
.....
debug1: Local version string .....
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

Cause

Il existe un cas limite où le TCP ACK (ACK sans données) à zéro octet, également connu sous le nom de poignée de main à trois, est soit supprimé, soit retardé.

Solution

Pour contourner ce problème, Transfer Family propose une solution qui utilise une configuration différente pour résoudre ce problème, mais qui peut entraîner des problèmes de compatibilité avec les anciens clients. C'est pourquoi cette solution n'est disponible que sur le port 2223.

Dans la procédure de création d'un serveur Transfer Family dans un VPC ([Création d'un serveur dans un cloud privé virtuel](#)), lorsque vous spécifiez un groupe de sécurité, configurez le trafic SSH pour qu'il utilise le port 2223.

Résoudre les problèmes liés au client SFTP

Les messages côté client SFTP sont décrits dans. [Messages SFTP](#) La meilleure façon de résoudre les problèmes liés aux clients SFTP est de consulter les journaux des clients SFTP et, si nécessaire, de contacter votre administrateur réseau.

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 télécharger 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 des fichiers que vous avez téléchargés. Les utilisateurs rencontrent parfois des problèmes avec les transferts FTP et SFTP qui déforment certains caractères des noms de fichiers, tels que les trémas, les lettres accentuées ou certains scripts, tels que le chinois ou l'arabe.

Cause

Bien que les protocoles FTP et SFTP puissent permettre aux clients de négocier le codage des caractères des noms de fichiers, ce n'est pas le cas d'Amazon S3 et Amazon EFS. 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.

Résoudre les problèmes de connecteur SFTP de type VPC de sortie

Si vous rencontrez des problèmes avec les connecteurs SFTP de type sortie VPC, vérifiez les points suivants :

L'état du connecteur est EN ATTENTE

Description

Votre connecteur de type sortie VPC reste en attente pendant plusieurs minutes après sa création et TestConnection renvoie le message « Connecteur non disponible ».

Cause

La résolution DNS pour les connecteurs VPC peut prendre plusieurs minutes après la création.

Solution

Attendez que l'état du connecteur devienne **ACTIF** avant de tenter de transférer des fichiers. Il s'agit d'un comportement normal pour les connecteurs de type sortie VPC.

Délai d'expiration de connexion

Description

Votre connecteur de type sortie VPC expire lorsque vous essayez de vous connecter au serveur SFTP.

Cause

Les groupes de sécurité peuvent ne pas autoriser le trafic sur le port 22 entre vos sous-réseaux Resource Gateway et le serveur SFTP cible.

Solution

Vérifiez que les groupes de sécurité autorisent le trafic sur le port 22 entre vos sous-réseaux Resource Gateway et le serveur SFTP cible.

Erreurs de configuration des ressources

Description

Votre connecteur de type sortie VPC ne parvient pas à se connecter en raison de problèmes de configuration des ressources.

Cause

La configuration des ressources peut indiquer une adresse IP ou un nom DNS incorrects, ou la passerelle de ressources peut ne pas se trouver dans le même VPC que votre serveur SFTP (pour les points de terminaison privés).

Solution

Assurez-vous que votre configuration de ressources pointe vers la bonne adresse IP ou le bon nom DNS, et que la passerelle de ressources se trouve dans le même VPC que votre serveur SFTP (pour les points de terminaison privés). Pour plus d'informations, consultez [Configurations de ressources](#) dans le Guide de l'utilisateur Amazon VPC Lattice.

Problèmes liés aux terminaux publics

Description

Votre connecteur de type sortie VPC ne peut pas se connecter aux points de terminaison SFTP publics.

Cause

Pour les points de terminaison publics, vous devez utiliser un nom DNS (et non une adresse IP) dans votre configuration de ressources, et votre VPC doit disposer d'une passerelle NAT pour l'accès Internet sortant.

Solution

Assurez-vous d'utiliser un nom DNS, et non une adresse IP, dans la configuration de vos ressources. Vérifiez que votre VPC dispose d'une passerelle NAT pour l'accès Internet sortant.

Problèmes liés à la zone de disponibilité

Description

Vous ne pouvez pas créer de passerelle de ressources en raison des limites de la zone de disponibilité.

Cause

Les passerelles de ressources nécessitent des sous-réseaux dans au moins 2 zones de disponibilité, et toutes les AZ ne prennent pas en charge le VPC Lattice.

Solution

Vérifiez les zones de disponibilité prises en charge pour VPC Lattice dans votre région et assurez-vous que vous disposez de sous-réseaux dans au moins 2 zones de disponibilité prises en charge.

Résoudre les problèmes liés au fournisseur d'identité personnalisé

Cette section décrit les solutions possibles aux problèmes liés aux fournisseurs d'identité personnalisés avec Transfer Family.

Rubriques

- [Résoudre les erreurs d'intégration d'API Gateway](#)
- [Résoudre les problèmes de temporisation des fonctions Lambda](#)
- [Résoudre les problèmes de temporisation Lambda constants](#)

- [Résoudre les problèmes liés aux exceptions KeyError](#)

Résoudre les erreurs d'intégration d'API Gateway

Description

Les utilisateurs ne peuvent pas s'authentifier auprès de votre serveur Transfer Family, et lorsque vous testez votre fournisseur d'identité, vous constatez des erreurs telles que :

```
{
  "Response": "",
  "StatusCode": 500,
  "Message": "Internal server error"
}
```

Cause

Des erreurs d'intégration d'API Gateway peuvent survenir pour les raisons suivantes :

- Configuration incorrecte de l'API Gateway
- Les erreurs liées à la fonction Lambda ne sont pas correctement gérées
- Problèmes d'autorisation entre API Gateway et Lambda
- Réponses mal formées de la fonction Lambda

Solution

Pour résoudre les erreurs d'intégration d'API Gateway :

1. Consultez les journaux de vos fonctions Lambda pour obtenir des informations détaillées sur les erreurs :
 - Dans la CloudWatch console, accédez à Groupes de journaux >/aws/lambda/your-function-name
 - Recherchez les messages d'erreur ou empilez les traces indiquant la cause première
2. Vérifiez que votre fonction Lambda renvoie des réponses correctement formatées :

```
{
  "Role": "arn:aws:iam::123456789012:role/TransferUserRole",
```

```
"HomeDirectory": "/mybucket/home/username"
}
```

3. Activez la CloudWatch journalisation détaillée pour API Gateway :

- Dans la console API Gateway, sélectionnez votre API et choisissez Stages
- Sélectionnez votre étape et sous Logs/Tracing, activez CloudWatch Logs
- Définissez le niveau du journal sur ERROR ou INFO

4. Testez directement votre point de terminaison API Gateway :

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-  
server-id/users/username/config \  
-H "Content-Type: application/json" \  
-d '{"Password": "password"}'
```

5. Vérifiez les autorisations entre API Gateway et Lambda :

- Assurez-vous qu'API Gateway est autorisé à appeler votre fonction Lambda
- Vérifiez que le rôle d'exécution de votre fonction Lambda dispose des autorisations nécessaires

Résoudre les problèmes de temporisation des fonctions Lambda

Description

Lorsque les utilisateurs tentent de s'authentifier auprès de votre serveur Transfer Family à l'aide d'un fournisseur d'identité personnalisé, ils rencontrent de longs délais suivis d'échecs d'authentification. Dans vos journaux Lambda, vous voyez des erreurs de temporisation.

Cause

Les fonctions Lambda utilisées pour les fournisseurs d'identité personnalisés ont un délai d'expiration par défaut de 3 secondes. Si votre logique d'authentification prend plus de temps que ce délai (par exemple, lorsque vous interrogez des bases de données externes ou que vous effectuez des appels d'API à des fournisseurs d'identité tiers), la fonction expirera et l'authentification échouera.

Solution

Pour résoudre les problèmes de temporisation Lambda :

1. Augmentez le délai d'expiration de la fonction Lambda :

- Dans la console Lambda, accédez à votre fonction et sélectionnez l'onglet Configuration

- Sous Configuration générale, cliquez sur Modifier
 - Augmenter la valeur du délai d'attente (jusqu'à 15 secondes sont recommandés pour les fonctions d'authentification)
2. Optimisez le code de votre fonction Lambda :
 - Utiliser le pool de connexions pour les requêtes de base de données
 - Implémenter la mise en cache pour les données fréquemment consultées
 - Minimiser les appels d'API externes lors de l'authentification
 3. Envisagez d'utiliser Lambda Provisioned Concurrency pour éliminer les démarrages à froid :

```
aws lambda put-provisioned-concurrency-config \
  --function-name my-authentication-function \
  --qualifier prod \
  --provisioned-concurrent-executions 5
```

4. Surveillez les performances Lambda à l'aide de CloudWatch métriques et configurez des alarmes pour les seuils de durée

Résoudre les problèmes de temporisation Lambda constants

Description

Les utilisateurs rencontrent des délais d'attente constants lorsqu'ils utilisent une fonction Lambda pour l'authentification.

Cause

Lambda ne parvient pas à accéder au AWS service correspondant utilisé pour l'authentification (tel que DynamoDB, Secrets Manager ou un autre fournisseur d'identité).

Solution

Vérifiez que les sous-réseaux peuvent accéder AWS aux services. Ou, si vous vous connectez à un fournisseur d'identité Internet (tel qu'Okta), vérifiez que le sous-réseau de la fonction Lambda peut accéder à Internet via une passerelle NAT

Résoudre les problèmes liés aux exceptions **KeyError**

Description

Dans les entrées de votre journal Transfer Family, vous remarquez des KeyError « » exceptions.

Cause

La cause la plus probable est que l'utilisateur ou l'`identity_provider` enregistrement est mal formé ou qu'il manque des champs obligatoires.

Solution

Consultez le ERRORS journal, situé dans le groupe de `/aws/transfer/your-server-id` journaux, pour trouver des indices.

Résoudre les problèmes liés au flux de travail

Cette section décrit les solutions possibles aux problèmes liés aux flux de travail gérés.

Rubriques

- [Résoudre les problèmes liés aux flux de travail gérés](#)
- [Résoudre les problèmes de déchiffrement du flux de travail](#)

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 [Real-time sections Traitement 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 sessions SFTP 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

Cette section décrit les solutions possibles aux problèmes suivants liés aux flux de travail chiffrés.

Rubriques

- [Résoudre les problèmes de chiffrement des destinataires anonymes](#)
- [Résolution d'une erreur liée au fichier de chiffrement signé](#)
- [Résolution d'une erreur liée à un algorithme FIPS](#)

Résoudre les problèmes de chiffrement des destinataires anonymes

Description

Votre flux de déchiffrement échoue lors du traitement de certains fichiers chiffrés, mais fonctionne avec d'autres.

Cause

Les fichiers peuvent avoir été chiffrés sans spécifier de destinataire (chiffrement anonyme), ce qui complique la tâche du flux de travail lorsqu'il s'agit de déterminer la clé à utiliser pour le déchiffrement.

Solution

Chiffrez toujours les fichiers dont le destinataire n'est pas anonyme à l'aide de ce `-r` paramètre. Par exemple :

```
gpg -e -r user@example.com --openpgp file.txt
```

Pour vérifier si un fichier a été crypté auprès d'un destinataire spécifique ou de manière anonyme, utilisez la `--list-packets` commande suivante :

```
gpg --list-packets file.txt.gpg
```

Cette commande affiche la structure des paquets du GPG-encrypted fichier sans déchiffrer son contenu. Recherchez une sortie qui inclut des informations sur le destinataire, telles que :

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

Si vous voyez des informations d'identification de clé, le fichier a été crypté pour un destinataire spécifique. Si ces informations sont manquantes, le fichier a peut-être été chiffré de manière anonyme, ce qui peut entraîner des échecs de déchiffrement dans les flux de travail de Transfer Family.

Vous pouvez également utiliser cette commande pour vérifier :

- Quels algorithmes de chiffrement ont été utilisés
- Méthodes de compression (le cas échéant)
- Horodatages de création

Pour consulter la liste des algorithmes de chiffrement pris en charge pour votre installation GPG, utilisez :

```
gpg --version
```

Ces informations peuvent vous aider à vous assurer que vous utilisez des algorithmes de chiffrement compatibles avec les flux de travail Transfer Family, en particulier lorsque la conformité à la norme FIPS est requise.

Résolution d'une erreur liée au fichier de chiffrement signé

Description

Votre flux de déchiffrement échoue et le message d'erreur suivant s'affiche :

```
"Encrypted file with signed message unsupported"
```

Cause

Transfer Family ne prend actuellement pas en charge la signature de fichiers chiffrés.

Solution

Dans votre client PGP, s'il existe une option permettant de signer le fichier chiffré, assurez-vous de désactiver cette option, car Transfer Family ne prend actuellement pas en charge la signature pour les fichiers chiffrés.

Résolution d'une erreur liée à un algorithme FIPS

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 mode FIPS 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 approuvés par la norme FIPS. 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 utilise l'OCB (un mode de chiffrement par blocs non FIPS) pour chiffrer des fichiers : cela entraîne l'échec du flux de travail.

Solution

Vous devez modifier la clé GPG que vous avez utilisée pour chiffrer vos fichiers, puis les rechiffrer. La procédure suivante décrit les étapes à suivre.

Pour modifier vos clés PGP

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]
      wJalrXUtnFEMI/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 l'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 l'EFS

Cette section décrit les solutions possibles aux problèmes liés au stockage Amazon EFS.

Rubriques

- [Résoudre les problèmes liés à Amazon EFS](#)

Résoudre les problèmes liés à Amazon EFS

Cette section décrit les solutions possibles pour les problèmes Amazon EFS suivants.

Rubriques

- [Résoudre les problèmes des utilisateurs gérés par le service Amazon EFS](#)
- [Résoudre les problèmes liés au profil POSIX manquant](#)
- [Résoudre les problèmes liés aux annuaires logiques avec Amazon EFS](#)

Résoudre les problèmes des utilisateurs gérés par le service Amazon EFS

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 utilisateur Gestion des identités et des accès AWS (IAM) n'est pas autorisé à accéder à Amazon Elastic File System (Amazon EFS).

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 au profil POSIX manquant

Description

Si vous utilisez le stockage Amazon EFS pour votre serveur et que vous utilisez un fournisseur d'identité personnalisé, vous devez fournir un profil POSIX à votre AWS Lambda fonction.

Cause

L'une des causes possibles est que les modèles que nous fournissons pour créer une AWS Lambda méthode Amazon API Gateway basée sur des données ne contiennent actuellement pas d'informations POSIX.

Si vous avez fourni des informations POSIX, le format que vous avez utilisé pour fournir les informations POSIX n'est peut-être pas correctement analysé par Transfer Family.

Solution

Assurez-vous de fournir un élément JSON 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'objet JSON 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 et l'UID.

```
{"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 Amazon EFS, 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 de stockage et de chiffrement

Cette section décrit les solutions possibles aux problèmes de stockage et de chiffrement.

Rubriques

- [Résoudre les problèmes liés aux compartiments Amazon S3 chiffrés](#)
- [Résolution des problèmes d'exception ResourceNotFound](#)

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 utilisateur IAM 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 en savoir plus, consultez [Protection et chiffrement des données](#).

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 commande d'API 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 commande d'API pour spécifier explicitement où trouver une ressource particulière.

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

Résoudre les problèmes de surveillance et d'alerte

Cette section fournit des informations sur la résolution des problèmes de surveillance et d'alerte liés AWS Transfer Family, notamment aux CloudWatch mesures manquantes ou incomplètes et aux EventBridge événements manquants.

Rubriques

- [Résoudre les problèmes liés aux métriques manquantes ou incomplètes CloudWatch](#)

- [Résoudre les problèmes liés aux événements manquants EventBridge](#)

Résoudre les problèmes liés aux métriques manquantes ou incomplètes CloudWatch

Description

CloudWatch les statistiques de vos serveurs Transfer Family sont manquantes, incomplètes ou ne sont pas mises à jour comme prévu.

Cause

Les indicateurs manquants ou incomplets peuvent être dus à plusieurs facteurs :

- Problèmes de configuration de journalisation
- Faibles niveaux d'activité qui ne génèrent pas de statistiques dans les délais prévus
- Afficher les métriques dont les dimensions ou les plages de temps sont incorrectes

Solution

Pour résoudre les problèmes liés à des CloudWatch métriques manquantes ou incomplètes, procédez comme suit :

1. Assurez-vous que la journalisation est correctement configurée pour votre serveur Transfer Familyserver :
 - Dans la console Transfer Family, vérifiez que la journalisation est activée sous Détails du serveur > Détails supplémentaires > Rôle de journalisation.
 - Assurez-vous que le rôle de journalisation dispose des autorisations et des relations de confiance nécessaires.
2. Lorsque vous consultez les métriques dans la CloudWatch console :
 - Utilisez les bonnes dimensions, par exemple ServerId pour les métriques au niveau du serveur
 - Ajustez la plage de temps pour vous assurer qu'elle couvre les périodes d'activité
 - Vérifiez que vous êtes dans le bon Région AWS
3. Générez une activité de test sur votre serveur Transfer Family pour vous assurer que les métriques sont produites.

Résoudre les problèmes liés aux événements manquants EventBridge

Description

Vous avez configuré EventBridge les règles Amazon pour capturer les événements Transfer Family, mais les événements ne sont pas diffusés vers vos destinations cibles et ne déclenchent pas les actions attendues.

Cause

EventBridge Les événements manquants peuvent être causés par :

- Modèles d'événements mal configurés
- Problèmes d'autorisation liés aux cibles des événements
- Limites de service ou régulation
- Événements non générés en raison de la configuration du serveur

Solution

Pour résoudre les problèmes liés aux EventBridge événements manquants, procédez comme suit :

1. Vérifiez que votre modèle d'événement est correctement formaté pour correspondre aux événements Transfer Family :

```
{
  "source": ["aws.transfer"],
  "detail-type": ["Transfer State Change"],
  "detail": {
    "serverId": ["s-1234567890abcdef0"]
  }
}
```

2. Vérifiez que la cible de votre événement dispose des autorisations nécessaires :

- Pour les cibles Lambda, assurez-vous que la politique de ressources de la fonction Lambda permet de l'invoquer EventBridge
- Pour les cibles SQS, vérifiez que la politique de file d'attente autorise EventBridge l'envoi de messages
- Pour les cibles SNS, confirmez que la politique du sujet autorise EventBridge la publication sur ces cibles

3. Testez votre règle en générant des exemples d'événements :

- Utilisez la EventBridge console pour créer un événement de test correspondant à votre modèle
- Effectuez des actions sur votre serveur Transfer Family qui devraient générer des événements

4. Activez les métriques des EventBridge règles pour surveiller les invocations et les échecs des règles :

```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state  
ENABLED --metrics-enabled
```

5. Consultez les CloudWatch journaux pour détecter tout message d'erreur lié à des échecs de livraison d'événements

Résoudre les problèmes de transfert entre régions

Cette section décrit les solutions possibles aux problèmes liés au transfert de fichiers Régions AWS.

Rubriques

- [Résoudre les problèmes d'autorisation de transfert entre régions](#)
- [Résoudre les problèmes de performances de transfert entre régions](#)

Résoudre les problèmes d'autorisation de transfert entre régions

Description

Lorsque vous tentez de transférer des fichiers entre des compartiments Amazon S3 situés dans différentes régions à l'aide des flux de travail Transfer Family, vous rencontrez des erreurs telles que :

```
{  
  "type": "StepErrored",  
  "details": {  
    "errorType": "BAD_REQUEST",  
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code:  
AccessDenied)",  
    "stepType": "COPY",  
    "stepName": "cross_region_copy"  
  }  
}
```


Cause

Cross-region les transferts nécessitent des autorisations IAM spécifiques pour les compartiments source et de destination. Le rôle IAM utilisé par votre serveur ou votre flux de travail Transfer Family ne dispose peut-être pas des autorisations suffisantes pour accéder aux buckets dans d'autres régions.

Solution

Pour résoudre les problèmes d'autorisation de transfert entre régions :

1. Assurez-vous que votre rôle IAM dispose d'autorisations pour les compartiments source et de destination :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::source-bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::destination-bucket-name/*"
    }
  ]
}
```

2. Si vous utilisez le chiffrement KMS, ajoutez des autorisations pour les clés KMS source et de destination :

```
{
  "Effect": "Allow",
  "Action": [
```

```
"kms:Decrypt",
"kms:GenerateDataKey"
],
"Resource": [
  "arn:aws:kms:source-region:account-id:key/source-key-id",
  "arn:aws:kms:destination-region:account-id:key/destination-key-id"
]
}
```

3. Vérifiez que les politiques relatives aux compartiments dans les deux régions autorisent l'accès depuis le rôle IAM de votre serveur Transfer Family
4. Pour les transferts entre comptes, assurez-vous que les autorisations entre comptes appropriées sont configurées

Résoudre les problèmes de performances de transfert entre régions

Description

Cross-region les transferts sont nettement plus lents que prévu ou expirent lors des transferts de fichiers volumineux.

Cause

Cross-region les transferts impliquent par nature une latence plus importante et peuvent être affectés par les conditions du réseau, la taille des fichiers et les limites de service. Les fichiers volumineux ou les volumes élevés de petits fichiers peuvent entraîner une dégradation des performances.

Solution

Pour améliorer les performances de transfert entre régions :

- Pour les fichiers volumineux, pensez à utiliser Amazon S3 Transfer Acceleration :

```
aws s3 cp --source-region us-east-1 --region us-west-2 \  
s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \  
--acl bucket-owner-full-control --s3-accelerate
```

- Pour plusieurs petits fichiers, regroupez-les avant le transfert :
 - Utiliser la compression pour combiner plusieurs fichiers
 - Utilisez les opérations par lots Amazon S3 pour les transferts à grande échelle

- Envisagez d'utiliser des connecteurs SFTP Transfer Family avec des paramètres de délai d'expiration appropriés pour les transferts importants
- Pour les transferts récurrents, pensez à répliquer les données à l'aide d'Amazon S3 Cross-Region Replication (CRR) au lieu de transferts ad hoc
- Surveillez les performances des transferts à l'aide CloudWatch des métriques Amazon pour identifier les goulots d'étranglement

Résoudre les problèmes de déploiement de Terraform

Cette section décrit les solutions possibles aux problèmes liés au déploiement des ressources Transfer Family à l'aide de Terraform. Pour des informations générales sur les modules Terraform pour Transfer Family, consultez. [Modules Transfer Family Terraform](#)

Rubriques

- [Résoudre les problèmes de création de ressources Terraform](#)
- [Résoudre les problèmes de gestion de l'état de Terraform](#)

Résoudre les problèmes de création de ressources Terraform

Description

Lorsque vous tentez de créer des ressources Transfer Family à l'aide de Terraform, vous rencontrez des erreurs telles que :

```
Error: error creating Transfer Server: InvalidRequestException: The request is not valid.  
Error: error creating Transfer User: InvalidRequestException: Unable to create the user because the server endpoint type is incompatible with the home directory type.
```

Cause

Ces erreurs se produisent généralement en raison de paramètres de configuration incompatibles ou de dépendances manquantes dans votre configuration Terraform. Les causes courantes incluent :

- Type de terminal et configurations de stockage incompatibles
- Rôles ou politiques IAM requis manquants
- Spécifications de politique de sécurité incorrectes

- Problèmes de configuration des points de terminaison VPC

Solution

Pour résoudre les problèmes de déploiement de Terraform :

- Assurez-vous que votre configuration Terraform utilise des combinaisons de paramètres compatibles :
 - Pour les points de terminaison publics, assurez-vous d'utiliser Amazon S3 pour le stockage.
 - Pour les points de terminaison VPC, vérifiez que le VPC et le groupe de sécurité sont correctement configurés.
- Utilisez des dépendances explicites avec l'attribut `depends_on` pour vous assurer que les ressources sont créées dans le bon ordre.
- Vérifiez que tous les rôles IAM disposent des relations de confiance et des autorisations nécessaires.
- Utilisez la dernière version du AWS fournisseur pour Terraform afin de garantir la compatibilité avec toutes les fonctionnalités de Transfer Family.
- Pour les déploiements complexes et les cas d'utilisation simples, pensez à utiliser les modules officiels Transfer Family Terraform disponibles sur le site. GitHub <https://github.com/aws-ia/terraform-aws-transfer-family> Ces modules fournissent de nombreux exemples couvrant des cas d'utilisation simples et complexes pour les clients, suivent les AWS meilleures pratiques et peuvent simplifier le déploiement pour les clients qui ont besoin d'aide pour la configuration de l'infrastructure en tant que code (IaC).

Résoudre les problèmes de gestion de l'état de Terraform

Description

Après avoir modifié vos ressources Transfer Family en dehors de Terraform (via console ou AWS CLI), vous rencontrez une dérive d'état ou des erreurs lors de l'exécution `terraform plan` ou `terraform apply`.

Cause

Terraform gère un fichier d'état qui suit les ressources qu'il gère. Lorsque des modifications sont apportées en dehors de Terraform, le fichier d'état se désynchronise avec les ressources réelles, ce qui entraîne des erreurs ou un comportement inattendu lors des opérations Terraform suivantes.

Solution

Pour résoudre les problèmes de gestion de l'état de Terraform avec les ressources Transfer Family :

1. `terraform import` À utiliser pour placer les ressources existantes sous la gestion de Terraform :

```
terraform import <transfer_family_server.example> s-<server-id>
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. `terraform refresh` À utiliser pour mettre à jour le fichier d'état avec l'infrastructure réelle actuelle
3. Pour les ressources qui ne peuvent pas être importées ou qui présentent des problèmes d'état complexes, envisagez de les `terraform state rm` supprimer du fichier d'état, puis de les recréer avec Terraform
4. Mettre en œuvre une politique visant à gérer les ressources de Transfer Family exclusivement via Terraform afin d'éviter une future dérive de l'État
5. Utilisez le stockage d'état à distance avec verrouillage pour empêcher les modifications simultanées lorsque vous travaillez en équipe

Résoudre les problèmes d'intégration du Web Application Firewall

Cette section décrit les solutions possibles aux problèmes liés à l'intégration AWS WAF à Transfer Family.

Rubriques

- [Résoudre les problèmes liés au blocage du trafic légitime par le WAF](#)
- [Résoudre les problèmes d'intégration du WAF avec les fournisseurs d'identité personnalisés](#)

Résoudre les problèmes liés au blocage du trafic légitime par le WAF

Description

Après la configuration AWS WAF avec votre point de terminaison Transfer Family, les utilisateurs légitimes ne peuvent pas se connecter ou rencontrent des défaillances de connexion intermittentes. Vous pouvez voir des réponses HTTP 403 (Interdit) dans vos journaux.

Cause

Vos AWS WAF règles sont peut-être trop restrictives ou mal configurées, ce qui entraîne des faux positifs qui bloquent le trafic légitime. Les causes courantes incluent :

- IP-based règles qui bloquent par inadvertance les réseaux d'entreprise ou les VPN
- Rate-based règles avec des seuils trop bas pour vos modèles de trafic habituels
- Groupes de règles gérés trop agressifs pour votre cas d'utilisation

Solution

Pour résoudre les problèmes de faux positifs :

1. Activez la AWS WAF journalisation pour identifier les règles qui déclenchent les blocages. Pour obtenir des instructions, consultez la section [Journalisation du trafic ACL AWS WAF Web](#).
2. Consultez vos journaux pour identifier les tendances des demandes bloquées.
3. Ajustez vos règles en :
 - Ajouter des adresses ou des plages IP à une liste d'autorisation
 - Augmenter les limites tarifaires pour les règles basées sur les taux
 - Configuration de règles spécifiques en mode Comptage au lieu du mode Bloc pour surveiller sans bloquer
 - Création d'exceptions pour des règles spécifiques à l'aide d'exclusions de groupes de règles
4. Testez la configuration mise à jour avec un échantillon représentatif du trafic légitime avant le déploiement complet.

Résoudre les problèmes d'intégration du WAF avec les fournisseurs d'identité personnalisés

Description

Après la configuration AWS WAF avec votre serveur Transfer Family qui utilise un fournisseur d'identité personnalisé, l'authentification échoue ou les utilisateurs rencontrent des problèmes d'authentification intermittents.

Cause

Lorsque vous utilisez un fournisseur d'identité personnalisé avec API Gateway, AWS WAF les règles peuvent interférer avec les appels d'API entre Transfer Family et votre fournisseur d'identité. Cela

peut se produire parce que le trafic de l'API AWS WAF est inspecté et potentiellement bloqué en fonction de ses ensembles de règles.

Solution

Pour résoudre les problèmes liés aux fournisseurs d'identité personnalisés AWS WAF et aux fournisseurs d'identité :

- Assurez-vous que votre AWS WAF configuration inclut des exceptions pour les points de terminaison API Gateway utilisés par votre fournisseur d'identité personnalisé.
- Ajoutez le principal du service Transfer Family (transfer.amazonaws.com) à une liste d'autorisation dans vos règles. AWS WAF
- Si vous utilisez des groupes de règles gérés, examinez-les pour détecter les règles susceptibles d'affecter les flux d'authentification des API et envisagez de désactiver ces règles spécifiques.
- Testez votre fournisseur d'identité directement à l'aide de l'opération `TestIdentityProvider` API pour vérifier qu'il fonctionne correctement sans AWS WAF interférence.

Résoudre les problèmes des utilisateurs gérés par les services

Cette section décrit les solutions possibles aux problèmes liés aux utilisateurs gérés par des services.

Rubriques

- [Résoudre les problèmes des utilisateurs gérés par des services](#)

Résoudre les problèmes des utilisateurs gérés par des services

Cette section décrit les solutions possibles aux problèmes suivants.

Rubriques

- [Résoudre les problèmes liés à un corps de clé publique trop long](#)
- [Le dépannage n'a pas réussi à ajouter la clé publique SSH](#)

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 clé PGP pour le corps de la clé publique et les clés PGP AWS Transfer Family ne sont pas prises en charge pour les utilisateurs gérés par des services.

Solution

Si la clé PGP l'est RSA-based, vous pouvez la convertir au format PEM. Par exemple, Ubuntu fournit un outil de conversion ici : <https://manpages.ubuntu.com/manpages/jammy/en/man1/openpgp2ssh.1.html>

Le dépannage n'a pas réussi à ajouter la clé publique SSH

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, mais les clés SSH2-formatted publiques AWS Transfer Family ne sont pas prises en charge SSH2-formatted pour les utilisateurs gérés par des services.

Solution

Vous devez convertir la clé au format OpenSSH. Ce processus est décrit dans [Conversion d'une clé SSH2 au format de clé publique SSH](#).

Résoudre les problèmes liés à l'AS2

Cette section décrit les solutions possibles aux problèmes liés aux transferts AS2.

Rubriques

- [Résoudre les problèmes liés à l'AS2](#)
- [Problèmes liés aux certificats AS2](#)
- [Problèmes de réception AS2 MDN](#)
- [Problèmes de surveillance de l'expiration des certificats](#)

Résoudre les problèmes liés à l'AS2

[Codes d'erreur AS2](#), les messages et les conseils de dépannage relatifs aux serveurs compatibles avec la déclaration d'applicabilité 2 (AS2) sont décrits dans la section codes de défaillance AS2 de ce guide.

Problèmes liés aux certificats AS2

Description

Vous rencontrez des erreurs liées aux certificats lors des transferts AS2.

Cause

Les causes courantes incluent les certificats expirés, les formats de certificats incorrects ou les chaînes de certificats incompatibles.

Solution

Essayez les solutions suivantes :

- Vérifiez que vos certificats ne sont pas expirés
- Assurez-vous que les certificats sont au bon format (PEM pour AWS Transfer Family)
- Vérifiez que la chaîne de certificats est complète et valide
- Vérifiez que les certificats de signature et de chiffrement correspondent à ceux des partenaires commerciaux
- Faites pivoter les certificats bien avant leur expiration pour éviter les interruptions

Problèmes de réception AS2 MDN

Description

Vous ne recevez pas les notifications de disposition des messages (mDNS) attendues pour les transferts AS2.

Cause

Des problèmes MDN peuvent survenir en raison de problèmes de connectivité réseau, de configurations de point de terminaison incorrectes ou de différences de format MDN.

Solution

Envisagez les solutions suivantes :

- Vérifiez que l'URL MDN est correctement configurée et accessible
- Vérifiez la connectivité réseau entre le serveur AS2 et le point de terminaison MDN
- Assurez-vous que les deux partenaires commerciaux sont configurés pour le même type de MDN (synchrone ou asynchrone)
- Consultez les journaux AS2 pour détecter toute erreur liée au traitement MDN
- Si vous utilisez un mDNS synchrone, vérifiez que les délais d'expiration sont définis de manière appropriée

Problèmes de surveillance de l'expiration des certificats

Cette section fournit des solutions aux problèmes courants liés à la surveillance de l'expiration des certificats et à la DaysUntilExpiry métrique.

DaysUntilExpiry métrique n'apparaissant pas

Problème : La DaysUntilExpiry métrique n'est pas visible sur Amazon CloudWatch après l'importation d'un certificat.

Solution :

- Patientez jusqu'à 24 heures après l'importation du certificat. Transfer Family peut prendre jusqu'à une journée pour émettre la métrique sur votre compte.
- Assurez-vous que vous recherchez dans la bonne AWS région et sous l'espace de AWS/Transfer noms dans CloudWatch.

Les alarmes d'expiration des certificats ne se déclenchent

Problème : les CloudWatch alarmes relatives à l'expiration des certificats ne se déclenchent pas comme prévu.

Solution :

- Vérifiez que l'alarme est configurée avec les `Maximum` statistiques et une période d'un jour.
- Vérifiez que la comparaison des seuils est définie `Less than or equal to` sur le nombre de jours souhaité.
- Assurez-vous que cette option `Treat missing data as good (not breaching)` est sélectionnée dans la configuration de l'alarme.
- Vérifiez que les dimensions de l'alarme correspondent à celles de votre certificat `CertificateId` et à la description (si fournies).
- Vérifiez que les actions d'alarme (rubriques SNS, notifications par e-mail) sont correctement configurées et actives.

AWS Transfer Family Référence d'API

Le guide de référence API complet pour Transfer Family est disponible sur [AWS Transfer Family API Reference](#).

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

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, à des 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, les ARN prennent la forme `arn:aws:transfer:region:account-id:server/server-id`.

Voici un exemple d'ARN de serveur : `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

- Pour les utilisateurs, les ARN se présentent sous la forme `arn:aws:transfer:region:account-id:user/server-id/username`.

Par exemple : `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

Les entrées DNS (points de terminaison) utilisées sont les suivantes :

- Les points de terminaison d'API se présentent sous la forme `transfer.region.amazonaws.com`.
- Les points de terminaison de serveur se présentent sous la forme `server-id.server.transfer.region.amazonaws.com`.

Cette référence d'interface d'API 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 actions d'API, voir [Actions](#).
- Pour la liste alphabétique des types de données, voir [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 appel d'API 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](#).

Effectuer 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 AWS Transfer Family opérations, la signature des demandes d'authentification et le traitement 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](#).

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 demande, y compris l'opération que vous souhaitez appeler, la date de la demande et les informations correspondant à votre autorisation en tant qu'expéditeur de la demande. 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.

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 charge utile de Transfer Family request/response 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' AWS API](#).

Réponses d'erreur

Lorsqu'il y a une erreur, les informations de l'en-tête de réponse contiennent :

- Content-Type: `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](#).

Fournisseurs d'identité

AWS Transfer Family prend en charge plusieurs types de fournisseurs d'identité pour authentifier et gérer les utilisateurs. Chaque serveur ne peut utiliser qu'une seule méthode d'authentification, qui doit être sélectionnée lors de la création du serveur.

Service géré

Avec la méthode `SERVICE_MANAGED` d'authentification, les informations d'identification des utilisateurs sont stockées et gérées au sein de celle-ci AWS Transfer Family. Les utilisateurs sont authentifiés à l'aide de clés publiques SSH associées à leur nom d'utilisateur sur le serveur.

Chaque utilisateur peut avoir une ou plusieurs clés publiques SSH stockées dans le service. Lorsqu'un client demande une opération sur un fichier, il fournit le nom d'utilisateur et la clé privée SSH, qui sont authentifiés par rapport à la clé publique enregistrée.

Directory Service

La méthode `AWS_DIRECTORY_SERVICE` d'authentification vous permet d'intégrer AWS Directory Service for Microsoft Active Directory (AWS Directory Service for Microsoft Active Directory).

Cette option vous permet de gérer l'authentification et l'accès des utilisateurs par le biais de vos groupes Active Directory existants. Les utilisateurs peuvent s'authentifier à l'aide de leurs informations d'identification Active Directory.

Il existe une limite par défaut de 100 groupes Active Directory par serveur, qui peut être portée à un maximum de 150 groupes par le biais d'une augmentation de la limite de service.

Lambda

La méthode `AWS_LAMBDA` d'authentification vous permet de vous connecter à un fournisseur d'identité personnalisé à l'aide de AWS Lambda.

Cette option offre la flexibilité nécessaire pour s'intégrer à vos systèmes de gestion des identités existants. La fonction Lambda est chargée d'authentifier les utilisateurs et de renvoyer les politiques d'accès appropriées.

Personnalisé (API Gateway)

La méthode `API_GATEWAY` d'authentification (affichée sous la forme Personnalisée dans la console) vous permet d'utiliser une méthode d'authentification personnalisée qui fournit à la fois l'authentification des utilisateurs et le contrôle d'accès.

Cette méthode repose sur Amazon API Gateway pour utiliser votre appel d'API provenant de votre fournisseur d'identité afin de valider les demandes des utilisateurs. Vous pouvez utiliser cette méthode personnalisée pour authentifier les utilisateurs auprès d'un service d'annuaire, d'une name/password paire de bases de données ou d'un autre mécanisme.

Pour toutes les méthodes d'authentification, les utilisateurs se voient attribuer des politiques qui définissent leur accès aux buckets Amazon S3 ou aux systèmes de fichiers Amazon Elastic File System. Le serveur hérite de la relation de confiance de l'utilisateur par le biais d'un rôle IAM assorti d'une AssumeRole action, ce qui lui permet d'effectuer des opérations sur les fichiers pour le compte de l'utilisateur.

Conventions de dénomination

AWS Transfer Family utilise des formats standardisés pour les identifiants de ressources et les Amazon Resource Names (ARN). Il est important de comprendre ces conventions lorsque vous travaillez avec l' AWS Transfer Family API.

Formats d'identification

Les conventions suivantes sont respectées dans les formats AWS Transfer Family d'identification :

Identifiants de serveur

Les valeurs ServerId se présentent sous la forme s-01234567890abcdef.

Identifiants de clé publique SSH

Les valeurs SshPublicKeyId se présentent sous la forme key-01234567890abcdef.

Identifiants du connecteur

Les valeurs ConnectorId se présentent sous la forme c-01234567890abcdef.

ID de flux de travail

Les valeurs WorkflowId se présentent sous la forme w-01234567890abcdef.

Identifiants de profil

Les valeurs ProfileId se présentent sous la forme p-01234567890abcdef.

WebApp Identifiants

Les valeurs WebAppId se présentent sous la forme webapp-01234567890abcdef.

Formats ARN

Les formats Amazon Resource Name (ARN) se présentent sous la forme suivante :

ARN du serveur

Pour les serveurs, les ARN prennent la forme `arn:aws:transfer:region:account-id:server/server-id`.

Exemple: `arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`.

ARN des utilisateurs

Pour les utilisateurs, les ARN se présentent sous la forme `arn:aws:transfer:region:account-id:user/server-id/username`.

Exemple: `arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`.

ARN du connecteur

Pour les connecteurs, les ARN prennent la forme `arn:aws:transfer:region:account-id:connector/connector-id`.

Exemple: `arn:aws:transfer:us-east-1:123456789012:connector/c-01234567890abcdef`.

ARN du flux de travail

Pour les flux de travail, les ARN prennent la forme `arn:aws:transfer:region:account-id:workflow/workflow-id`.

Exemple: `arn:aws:transfer:us-east-1:123456789012:workflow/w-01234567890abcdef`.

WebApp ARN

Pour les applications Web, les ARN prennent la forme `arn:aws:transfer:region:account-id:webapp/webapp-id`.

Exemple: `arn:aws:transfer:us-east-1:123456789012:webapp/webapp-01234567890abcdef`.

Vous pouvez attribuer des balises, qui sont des paires clé-valeur, à des 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.

DNS et points de terminaison

AWS Transfer Family utilise des conventions de dénomination DNS standardisées pour les points de terminaison d'API et les points de terminaison de serveur. Il est essentiel de comprendre ces points de terminaison pour configurer les clients et effectuer des appels d'API.

Points de terminaison d'API

Les points de terminaison d'API sont utilisés pour effectuer des appels d'API afin de gérer les AWS Transfer Family ressources. Ces points de terminaison prennent les formes suivantes :

Points de terminaison d'API standard

Les points de terminaison d'API standard prennent la forme `formetransfer.region.amazonaws.com`.

Exemple : `transfer.us-east-1.amazonaws.com`

Dual-Stack Points de terminaison de l'API

AWS Transfer Family propose des points de terminaison d'API à double pile accessibles via des requêtes IPv4 ou IPv6 :

- `https://transfer.region-code.api.aws`
- `https://transfer-fips.region-code.api.aws`

Points de terminaison du serveur

Les points de terminaison du serveur sont utilisés par les clients de transfert de fichiers pour se connecter aux AWS Transfer Family serveurs. Ces points de terminaison prennent les formes suivantes :

Points de terminaison de serveur standard

Les points de terminaison de serveur standard prennent la forme `server-id.server.transfer.region.amazonaws.com`.

Exemple : `s-01234567890abcdef.server.transfer.us-east-1.amazonaws.com`

Noms d'hôtes personnalisés

Vous pouvez également configurer des noms d'hôte personnalisés pour vos AWS Transfer Family serveurs. Les noms d'hôte personnalisés peuvent être utilisés pour offrir une expérience plus conviviale ou personnalisée à vos utilisateurs.

Pour utiliser un nom d'hôte personnalisé, vous devez :

1. Posséder le nom de domaine
2. Fournir un certificat valide
3. Configurer les enregistrements DNS pour qu'ils pointent vers votre AWS Transfer Family serveur

Pour une liste complète des AWS Transfer Family points de terminaison par AWS région, consultez les [AWS Transfer Family points de terminaison et les quotas](#) dans le. Références générales AWS

Historique du document pour AWS Transfer Family

Le tableau suivant décrit la documentation de cette version de AWS Transfer Family.

- Version d'API : transfer-2018-11-05
- Dernière mise à jour de la documentation : 19 novembre 2025

Modifier	Description	Date
Support des terminaux VPC pour les applications Web Transfer Family	AWS Transfer Family les applications Web prennent désormais en charge les points de terminaison hébergés par VPC, ce qui vous permet d'héberger votre point de terminaison d'application Web dans un cloud privé virtuel pour les transferts de données privées vers et depuis Amazon S3 sans passer par l'Internet public. Pour en savoir plus, consultez Création d'une application Web Transfer Family dans un VPC .	19 novembre 2025
Prise en charge d'IPv6	AWS Transfer Family prend désormais en charge les points de terminaison à double pile (IPv4 et IPv6) pour les points de terminaison publics SFTP, les points de terminaison pour les connecteurs SFTP et AS2 et les VPC-internal SFTP/FTPS/FTP/AS2 points de terminaison	30 juin 2025

Modifier	Description	Date
	d'API. Pour en savoir plus, consultez Support IPv6 pour les serveurs Transfer Family .	
Améliorations apportées à l'expérience utilisateur des connecteurs SFTP	• Possibilité de paramétrer les connexions simultanées en libre-service pour vos connecteurs • Possibilité de fournir une clé privée SSH au format OpenSSH utilisée pour authentifier les connexions • Possibilité de découvrir la clé d'hôte publique des serveurs distants à l'aide de leurs connecteurs SFTP Pour en savoir plus, consultez Création d'un connecteur SFTP avec sortie gérée par service.	9 avril 2025

Modifier	Description	Date
Possibilité pour les connecteurs SFTP de supprimer, renommer et déplacer des fichiers sur le serveur SFTP distant	Vous pouvez désormais organiser vos fichiers stockés sur des serveurs SFTP distants en supprimant, renommant ou déplaçant les fichiers source vers des emplacements d'archivage une fois qu'ils ont été copiés depuis le serveur distant. Pour en savoir plus, consultez Déplacer ou renommer des fichiers ou des répertoires sur le serveur SFTP distant.	7 avril 2025
Support pour les applications AWS Transfer Family Web	AWS Transfer Family les applications Web sont une nouvelle ressource que les clients peuvent utiliser pour créer une interface simple permettant d'accéder à leurs données dans Amazon S3 via un navigateur Web. Pour en savoir plus, consultez Applications Web Transfer Family .	1er décembre 2024
Référence d'API déplacée dans un guide distinct	Pour améliorer l'expérience client, la référence d'API est désormais publiée séparément du guide de l'utilisateur. Pour la référence séparée sur l'API, voir Bienvenue dans l' AWS Transfer Family API .	31 juillet 2024

Modifier	Description	Date
Possibilité pour les connecteurs SFTP de répertorier les fichiers et répertoires distants	Transfer Family a ajouté la possibilité à ses clients d'utiliser des connecteurs SFTP pour répertorier les fichiers stockés sur des serveurs SFTP distants. Pour plus d'informations, consultez Lister le contenu d'un répertoire distant .	23 avril 2024
Possibilité d'utiliser le certificat TLS autosigné d'un partenaire commercial avec échange de messages AS2	AWS Transfer Family a ajouté la possibilité d'importer et d'utiliser le certificat TLS public autosigné d'un partenaire commercial pour envoyer des messages de déclaration d'applicabilité 2 (AS2) à son serveur via HTTPS.	12 avril 2024
Ajout de politiques de sécurité pour les connecteurs SFTP	AWS Transfer Family a ajouté des politiques de sécurité à utiliser avec les connecteurs SFTP. Pour en savoir plus, consultez Politiques de sécurité pour AWS Transfer Family Connecteurs SFTP .	5 avril 2024

Modifier	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 en savoir plus, consultez Gestion Transfer Family événements utilisant Amazon EventBridge .	8 février 2024
Ajout de nouvelles politiques de sécurité	AWS Transfer Family a ajouté de nouvelles politiques de sécurité FIPS et non FIPS. En outre, la politique de sécurité par défaut attribuée aux serveurs est toujours la plus récente. Pour en savoir plus, consultez Politiques de sécurité pour AWS Transfer Family serveurs .	5 février 2024
Support des adresses IP statiques pour les connecteurs SFTP et AS2	Transfer Family fournit désormais des adresses IP statiques pour les connecteurs SFTP et AS2. Cela permet de se connecter à des serveurs SFTP distants sécurisés par des contrôles de liste d'adresses IP autorisées. Pour AS2, nous introduisons des adresses IP statiques pour les réponses MDN asynchrones des serveurs AS2.	16 janvier 2024

Modifier	Description	Date
Le guide de l'utilisateur a été réorganisé pour 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
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 de terminaison de serveur SFTP, FTPS ou FTP.	17 novembre 2023

Modifier	Description	Date
Port alternatif pour les serveurs SFTP 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 terminaison VPC. Pour de plus amples informations, veuillez consulter Création d'un serveur dans un cloud privé virtuel .	17 novembre 2023
Support pour les connecteurs SFTP	Les connecteurs SFTP 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 Utilisation de connecteurs SFTP .	25 juillet 2023
Support de l'authentification AS2 Basic	Transfer Family prend désormais en charge l'utilisation de l'authentification de base pour les serveurs qui utilisent le protocole Applicability Statement 2 (AS2). Pour de plus amples informations, veuillez consulter Authentification de base pour les connecteurs AS2 .	30 juin 2023

Modifier	Description	Date
Support pour la journalisation JSON structurée	Transfer Family prend désormais en charge la fourniture de journaux JSON 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 les AWS Transfer Family serveurs .	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 public/private clés ou des deux. Ceci est disponible pour les serveurs qui utilisent le protocole SFTP et un fournisseur d'identité personnalisé. Pour de plus amples informations, veuillez consulter Création d'un SFTP-enabled serveur .	17 mai 2023

Modifier	Description	Date
Support pour le déchiffrement de Pretty Good Privacy (PGP) avec des fichiers traités par Transfer Family avec des flux de travail	Transfer Family dispose d'un support intégré pour le déchiffrement Pretty Good Privacy (PGP). Vous pouvez utiliser le déchiffrement PGP sur les fichiers chargés via SFTP, FTPS ou FTP vers Amazon Simple Storage Service (Amazon S3) ou Amazon Elastic File System (Amazon EFS). Pour plus d'informations, consultez Génération de clés PGP et Utilisez le déchiffrement PGP 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	Vous pouvez créer des serveurs qui utilisent le protocole AS2 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 d'AS2 .	25 juillet 2022

Modifier	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 les serveurs FTP et FTPS). Pour plus d'informations, consultez Création d'un SFTP-enabled serveur, Création d'un FTPS-enabled serveur ou Création d'un FTP-enabled serveur.	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 une 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

Modifier	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 de AWS Directory Service pour Microsoft Active Directory .	24 mai 2021

Modifier	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 (Amazon EFS). Amazon EFS est un système de fichiers NFS élastique simple, évolutif et entièrement géré. Pour de plus amples informations, veuillez consulter Configuration d'un système de fichiers Amazon EFS .	6 janvier 2021

Modifier	Description	Date
Support pour AWS WAF	Transfer Family prend désormais en charge AWS WAF un pare-feu d'applications Web qui aide à protéger les applications Web et les opérations d'API 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

Modifier	Description	Date
Nouveau Régions AWS	Transfer Family est désormais disponible dans les AWS GovCloud (US) régions. Pour plus d'informations sur les points de terminaison 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'utilisateur.	30 septembre 2020
Une politique de sécurité avec des algorithmes cryptographiques 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 serveurs.	12 août 2020

Modifier	Description	Date
Prise en charge des points de terminaison FIPS (Federal Information Processing Standard)	FIPS-enabled les points de terminaison sont désormais disponibles en Amérique Régions AWS du Nord. Pour les régions disponibles, consultez les AWS Transfer Family points de terminaison et les quotas dans le Références générales AWS. Pour activer le protocole FIPS pour un point de terminaison de SFTP-enabled serveur, consultez Création d'un SFTP-enabled serveur . Pour activer le protocole FIPS pour un point de terminaison de FTPS-enabled serveur, consultez Création d'un FTPS-enabled serveur . Pour activer le protocole FIPS pour un point de terminaison de FTP-enabled serveur, consultez Création d'un FTP-enabled serveur .	12 août 2020
Augmentation de la longueur des caractères du nom d'utilisateur et caractères supplémentaires 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

Modifier	Description	Date
Support pour la création automatique de rôles de CloudWatch journalisation Amazon Gestion des identités et des accès AWS (IAM)	Transfer Family prend désormais en charge la création automatique d'un rôle IAM de CloudWatch journalisation pour visualiser l'activité de l'utilisateur final. Pour plus d'informations, consultez Création d'un SFTP-enabled serveur , Création d'un FTPS-enabled serveur ou Création d'un FTP-enabled serveur .	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 lors de l'autorisation d'accès via le protocole SFTP (Secure File Transfer Protocol), le protocole de transfert de fichiers via SSL (FTPS) ou le protocole FTP (File Transfer Protocol). Pour de plus amples informations, veuillez consulter Travailler avec des fournisseurs d'identité personnalisés .	9 juin 2020

Modifier	Description	Date
AWS Le transfert pour SFTP est désormais disponible AWS Transfer Family et ajoute le support pour FTP et FTPS.	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 le protocole FTP sur SSL (FTPS) et les flux de travail basés sur le protocole FTP en texte brut AWS, en plus de la prise en charge existante du protocole SFTP (Secure File Transfer Protocol).	23 avril 2020

Modifier	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

Modifier	Description	Date
Première version de AWS Transfer Family 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

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.