



Guide de l'utilisateur

AWSStorage Gateway



Version de l'API 2013-06-30

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

AWSStorage Gateway: Guide de l'utilisateur

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

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

Table of Contents

Qu'est-ce qu'Amazon S3 File Gateway ?	1
Amazon S3 File Gateway	1
Fonctionnement de Storage Gateway	3
Amazon S3 File Gateway	3
Configuration	6
S'inscrire à Amazon Web Services	6
Créer un utilisateur IAM	6
Prérequis	8
Prérequis requis	9
Exigences en matière de matériel et de stockage	9
Exigences pour le réseau et le pare-feu	11
Hyperviseurs pris en charge et exigences pour l'hôte	25
Clients NFS pris en charge pour une passerelle de fichiers	26
Clients SMB pris en charge pour une passerelle de fichiers	27
Opérations de système de fichiers prises en charge	27
Accès à AWS Storage Gateway	28
Régions AWS prises en charge	28
Utilisation de l'appliance matérielle	29
Régions AWS prises en charge	30
Configuration de votre appliance matérielle	30
Montage sur rack et connexion de l'appliance matérielle au secteur	32
Dimensions de l'appliance matérielle	32
Configuration des paramètres réseau	37
Activation de votre appliance matérielle	40
Lancement d'une passerelle	42
Configuration d'une adresse IP pour la passerelle	43
Configuration de votre passerelle	45
Suppression d'une passerelle	45
Suppression de votre appliance matérielle	46
Commencer	47
Créer une passerelle de fichiers S3	47
Configuration d'une passerelle de fichiers Amazon S3	47
Connect votre passerelle de fichiers Amazon S3 àAWS	48
Vérifiez les paramètres et activez votre passerelle de fichiers Amazon S3	50

Configurer votre passerelle de fichiers Amazon S3	50
Création d'un partage de fichiers	53
Création d'un partage de fichiers NFS	56
Création d'un partage de fichiers SMB	63
Création d'un partage de fichiers SMB	65
Montez et utilisez votre partage de fichiers	74
Montez votre partage de fichiers NFS sur votre client	74
Montez votre partage de fichiers SMB sur votre client	76
Utilisation de partages de fichiers sur un compartiment avec des objets préexistants	81
Testez votre passerelle de fichiers S3	82
Comment procéder ensuite ?	83
Nettoyez les ressources dont vous n'avez pas besoin	83
Activer une passerelle dans un VPC	84
Création d'un point de terminaison de VPC pour Storage Gateway	85
Configuration et configuration d'un proxy HTTP	86
Autorisation du trafic vers les ports requis dans votre proxy HTTP	89
Gestion de votre passerelle Amazon S3 File Gateway	91
Ajout d'un partage de fichiers	91
Octroi d'accès à un compartiment S3	92
Prévention du député confus entre services	94
Utilisation d'un partage de fichiers pour l'accès entre comptes	95
Suppression d'un partage de fichiers	97
Modification des paramètres de votre partage de fichiers NFS	99
Modification des métadonnées par défaut pour votre partage de fichiers NFS	102
Modification des paramètres d'accès de votre partage de fichiers NFS	104
Modification des paramètres SMB pour une passerelle	105
Définition d'un niveau de sécurité pour votre passerelle	105
Utilisation d'Active Directory pour authentifier les utilisateurs	106
Fourniture d'un accès invité à votre partage de fichiers	109
Configurez les groupes locaux pour votre passerelle	109
Définition de la visibilité du partage de fichiers	110
Modification des paramètres de votre partage de fichiers SMB	111
Actualisation des objets dans votre compartiment Amazon S3	115
Utilisation de la fonctionnalité de verrouillage des objets S3 avec une passerelle de fichiers Amazon S3	119
Comprendre l'état du partage de fichiers	120

Bonnes pratiques de partage de fichiers	121
Empêcher l'écriture de plusieurs partages de fichiers dans votre compartiment Amazon S3	122
Autoriser des clients NFS spécifiques à monter votre partage de fichiers	122
Surveillance de la passerelle de fichiers	124
Obtention des journaux de santé de passerelle de fichiers	124
Configuration d'un groupe de journaux CloudWatch pour votre passerelle	126
Utilisation des métriques Amazon CloudWatch	127
Réception de notifications sur les opérations de fichiers	129
Obtenir une notification de téléchargement de fichiers	130
Obtention d'une notification de téléchargement de jeux de fichiers	132
Recevoir une notification de cache d'actualisation	135
Présentation des métriques de la passerelle	137
Comprendre les mesures de partage de fichiers	143
Comprendre les journaux d'audit de passerelle de fichiers	145
Maintenance de votre passerelle	151
Arrêt de la machine virtuelle de la passerelle	151
Gestion des disques locaux	152
Décider de la quantité de stockage sur disque local	152
Taille du stockage de cache	153
Configuration du stockage de cache	153
Utilisation du stockage éphémère avec des passerelles EC2	154
Gestion de bande passante	156
Modifier le calendrier limite de bande passante	157
Utilisation de la AWS SDK for Java	158
Utilisation de la AWS SDK for .NET	161
Utilisation de la AWS Tools for Windows PowerShell	163
Gestion des mises à jour de la passerelle	164
Exécution des tâches de maintenance sur la console locale	166
Exécution de tâches sur la console locale de la machine virtuelle (passerelle de fichiers)	166
Exécution de tâches sur la console locale EC2 (passerelle de fichiers)	188
Accès à la console locale de la passerelle	198
Configuration des cartes réseau pour la passerelle	204
Suppression de votre passerelle et suppression des ressources	210
Suppression de votre passerelle à l'aide de la console Storage Gateway	211
Suppression de ressources à partir d'une passerelle déployée sur site	212

Suppression de ressources à partir d'une passerelle déployée sur une instance Amazon EC2	213
Remplacement de votre passerelle de fichiers existante par une nouvelle instance	214
Méthode 1 : Migrer le disque cache et l'ID de passerelle vers une instance de remplacement ..	215
Méthode 2 : Instance de remplacement avec disque cache vide et nouvel ID de passerelle	218
Performances	221
Conseils sur les performances des passerelles de fichiers	221
Performances de passerelle de fichiers S3 sur les clients Linux	222
Performances de passerelle de fichiers sur les clients	224
Optimisation des performances de la passerelle	225
Ajouter des ressources à la passerelle	226
Ajouter des ressources à votre environnement d'application	228
Utilisation de VMware High Availability avec Storage Gateway	229
Configurer votre cluster vSphere VMware HA	229
Télécharger l'image .ova pour votre type de passerelle	231
Déployer la passerelle	231
(Facultatif) Ajouter des options de remplacement pour d'autres machines virtuelles de votre cluster	232
Activer votre passerelle	232
Tester votre configuration de VMware High Availability	233
Sécurité	234
Protection des données	235
Chiffrement des données	236
Authentification et contrôle d'accès	237
Authentification	237
Contrôle d'accès	239
Présentation de la gestion des accès	241
Utilisation des politiques basées sur une identité (politiques IAM)	247
Utilisation de balises pour contrôler l'accès aux ressources	257
Utilisation des listes ACL pour l'accès au partage de fichiers SMB	259
Référence des autorisations Storage Gateway	263
Utilisation des rôles liés à un service	271
Journalisation et surveillance	275
Informations Storage Gateway dans CloudTrail	276
Présentation des entrées des fichiers journaux Storage Gateway	277
Validation de la conformité	279

Résilience	280
Sécurité de l'infrastructure	280
Bonnes pratiques de sécurité	281
Dépannage des problèmes de passerelle	282
Dépannage des problèmes de passerelle sur site	282
Activation deAWS Supportpour résoudre les problèmes de votre passerelle	287
Résolution des problèmes d'installation de Microsoft Hyper-V	289
Dépannage des problèmes liés à la passerelle Amazon EC2	294
L'activation de la passerelle n'a pas eu lieu après quelques instants	294
Impossible de trouver l'instance de passerelle EC2 dans la liste des instances	295
Activation deAWS Supportpour résoudre les problèmes de la passerelle	295
Dépannage des problèmes d'appliance matérielle	297
Comment déterminer l'adresse IP du service	297
Comment effectuer une réinitialisation d'usine	298
Comment obtenir le support Dell iDRAC	298
Comment trouver le numéro de série de l'appliance matérielle	298
Comment obtenir la prise en charge de l'appliance matérielle	298
Dépannage des problèmes de passerelle de fichiers	299
Erreur: InaccessibleStorageClass	300
Erreur: Accès S3 refusé	300
Erreur: InvalidObjectState	301
Erreur: ObjectMissing	302
: Notification Redémarrer	302
: Notification HardReboot	302
: Notification HealthCheckFailure	303
: Notification AvailabilityMonitorTest	303
Erreur: RoleTrustRelationshipInvalid	303
Dépannage des métriques CloudWatch	304
Dépannage des problèmes de partage de fichiers	307
Le partage de fichiers est bloqué dans l'état CREATION	307
Impossible de créer un partage de fichiers	308
Les partages de fichiers SMB n'autorisent pas plusieurs méthodes d'accès différentes	308
Plusieurs partages de fichiers ne peuvent pas écrire dans le compartiment S3 mappé	309
Impossible de télécharger des fichiers dans le compartiment S3	309
Impossible de modifier le chiffrement par défaut en SSE-KMS	309

Les modifications apportées directement dans un compartiment S3 avec le versionnement d'objet activé peuvent affecter ce que vous voyez dans votre partage de fichiers	310
Lorsque vous écrivez dans un compartiment S3 avec le versionnement d'objet activé, la passerelle de fichiers peut créer plusieurs versions d'un objet S3	311
Les modifications apportées à un compartiment S3 ne sont pas reflétées dans Storage Gateway	313
Les autorisations ACL ne fonctionnent pas comme prévu	313
Les performances de la passerelle ont diminué après une opération récursive	314
Notifications d'intégrité relatives à la haute disponibilité	314
Dépannage des problèmes de haute disponibilité	314
Notification d'Health	314
Métriques	316
Récupération de vos données : bonnes pratiques	316
Récupération après un arrêt inattendu de la machine virtuelle	317
Récupération de données à partir d'un disque cache défectueux	317
Récupération de données depuis un centre de données inaccessible	318
Ressources supplémentaires	319
Configuration de l'hôte	319
Configuration de VMware for Storage Gateway	319
Synchronisation de l'heure de l'ordinateur virtuel de la passerelle	325
Passerelle de fichiers sur un hôte EC2	327
Obtention de la clé d'activation	331
AWS CLI	331
Linux (bash/zsh)	332
Microsoft Windows PowerShell	332
Utilisation d'AWS Direct Connect avec Storage Gateway	333
Exigences de ports	333
Connexion à votre passerelle	343
Obtention d'une adresse IP auprès d'un hôte Amazon EC2	343
Présentation des ressources et des ID de ressource	344
Utilisation des ID de ressource	345
Balisage de vos ressources	346
Utilisation des balises	347
Voir aussi	348
Composants open source	349
Composants open source pour Storage Gateway	349

Composants open source pour Amazon S3 File Gateway	349
Quotas	350
Quotas pour partages de fichiers	350
Tailles de disques locales recommandées pour votre passerelle	351
Utilisation des classes de stockage	351
Utilisation de classes de stockage avec une passerelle de fichiers	352
Utilisation de la classe de stockage GLACIER avec une passerelle de fichiers	358
Référence API	359
En-têtes de requête obligatoires	359
Signature des requêtes	362
Exemple de calcul de signature	363
Réponses d'erreur	364
Exceptions	365
Codes d'erreur d'opération	367
Réponses d'erreur	387
Opérations	389
Historique de document	390
Mises à jour antérieures	404
.....	cdix

Qu'est-ce qu'Amazon S3 File Gateway ?

AWSStorage Gateway connecte une application logicielle sur site à une unité de stockage basée sur le cloud afin de fournir une intégration continue avec les fonctionnalités de sécurité des données entre l'environnement informatique sur site et l'AWS infrastructure de stockage. Vous pouvez utiliser le service pour stocker des données dans le AWS Cloud pour un stockage évolutif et économique qui vous aide à garantir la sécurité des données. AWS Storage Gateway vous propose des solutions de stockage basées sur les volumes, les bandes et les fichiers.

Rubriques

- [Amazon S3 File Gateway](#)

Amazon S3 File Gateway

Amazon S3 File Gateway—Amazon S3 File Gateway prend en charge une interface de fichiers dans [Amazon Simple Storage Service \(Amazon S3\)](#) et combine un service et une application logicielle virtuelle. Cette combinaison vous permet de stocker et de récupérer des objets dans Amazon S3 à l'aide de protocoles de fichier standard tels que NFS (Network File System) et SMB (Server Message Block). L'appliance logicielle, ou passerelle, est déployée dans votre environnement sur site en tant que machine virtuelle (VM) s'exécutant sur l'hyperviseur VMware ESXi, Microsoft Hyper-V ou KVM (machine virtuelle basée sur le noyau Linux). La passerelle permet d'accéder aux objets dans S3 sous forme de fichiers ou de points de montage de partage de fichiers. Une passerelle de fichiers S3 vous permet d'effectuer les actions suivantes :

- Vous pouvez stocker et récupérer des fichiers directement à l'aide du protocole NFS version 3 ou 4.1.
- Vous pouvez stocker et récupérer des fichiers directement à l'aide du protocole de système de fichiers SMB versions 2 et 3.
- Vous pouvez accéder à vos données directement dans Amazon S3 à partir de n'importe quel AWS Application ou service cloud.
- Vous pouvez gérer vos données S3 à l'aide des stratégies de cycle de vie, de la réplication entre régions et de la gestion des versions. Vous pouvez combiner une passerelle de fichiers S3 à un montage de système de fichiers NFS sur Amazon S3.

Une passerelle de fichiers S3 simplifie le stockage de fichiers dans Amazon S3, s'intègre aux applications existantes par le biais de protocoles de système de fichiers standard du secteur et fournit une alternative rentable au stockage sur site. Elle offre également un accès à faible latence aux données, grâce à la mise en cache locale transparente. Une passerelle de fichiers S3 gère le transfert de données depuis et vers AWS, met en tampon des applications en cas de surcharge du réseau, optimise et diffuse des données en parallèle et gère la consommation de bande passante. S3 File Gateway intègre avec AWS services, par exemple avec les éléments suivants :

- Gestion de l'accès courant à l'aide d'AWS Identity and Access Management (IAM)
- Chiffrement à l'aide d'AWS Key Management Service (AWS KMS)
- Surveillance à l'aide d'Amazon CloudWatch (CloudWatch)
- Audit avec AWS CloudTrail (CloudTrail)
- Opérations à l'aide d'AWS Management Console et AWS Command Line Interface (AWS CLI)
- Gestion des coûts et facturation

Dans la documentation suivante, vous trouverez une section de mise en route qui couvre les informations de configuration communes à toutes les passerelles, ainsi que des sections de configuration propres à certaines passerelles. La section de mise en route vous explique comment déployer, activer et configurer le stockage pour une passerelle. La section relative à la gestion vous montre comment gérer votre passerelle et vos ressources :

- fournit des instructions sur la façon de créer et d'utiliser une passerelle de fichiers S3. Cette section explique comment créer un partage de fichiers, mapper votre lecteur à un compartiment Amazon S3 et charger des fichiers et dossiers dans Amazon S3.
- décrit comment exécuter des tâches de gestion pour tous les types et ressources de passerelles.

Dans ce manuel, vous trouverez principalement comment mener des opérations de passerelle à l'aide de l'AWS Management Console. Pour réaliser ces opérations par programmation, consultez le manuel [AWS Référence d'API Storage Gateway](#).

Fonctionnement de Storage Gateway (architecture)

Vous trouverez ci-après une présentation de l'architecture des solutions Storage Gateway disponibles.

Rubriques

- [Amazon S3 File Gateway](#)

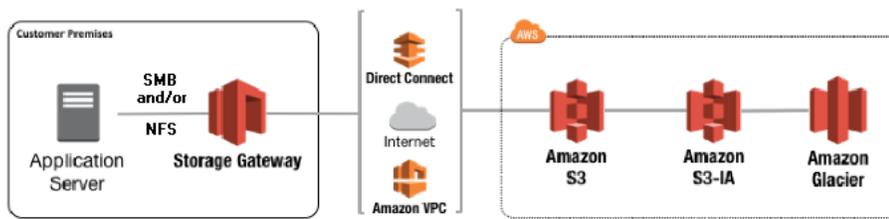
Amazon S3 File Gateway

Pour utiliser une passerelle de fichiers S3, commencez par télécharger une image de machine virtuelle pour la passerelle. Vous activez ensuite la passerelle depuis leAWS Management Consoleou via l'API Storage Gateway. Vous pouvez également créer une passerelle de fichiers S3 à l'aide d'une image Amazon EC2.

Une fois que la passerelle de fichiers S3 est activée, vous créez et configurez votre partage de fichiers, puis associez ce partage à votre compartiment Simple Storage Service (Amazon S3). Les clients peuvent ainsi accéder au partage à l'aide du protocole Network File System (NFS) ou Server Message Block (SMB). Les fichiers écrits sur un partage de fichiers deviennent des objets dans Amazon S3, le chemin d'accès constituant la clé. Les fichiers et les objets sont liés par un mappage un à un, et la passerelle met à jour de façon asynchrone les objets dans Amazon S3 à mesure que vous modifiez les fichiers. Les objets existants dans le compartiment Amazon S3 apparaissent comme des fichiers dans le système de fichiers, et la clé devient le chemin d'accès. Les objets sont chiffrés avec des clés de chiffrement côté serveur Amazon S3 (SSE-S3). L'ensemble du transfert de données est effectué via HTTPS.

Le service optimise le transfert de données entre la passerelle etAWSen utilisant des téléchargements parallèles en plusieurs parties ou des téléchargements par plage d'octets, afin de mieux utiliser la bande passante disponible. Le cache local est conservé pour offrir un accès à faible latence aux données récemment consultées et réduire les frais liés à la sortie de données. Les métriques CloudWatch fournissent des informations sur l'utilisation des ressources sur la machine virtuelle et le transfert de données vers ou depuisAWS. CloudTrail suit tous les appels d'API.

Le stockage de fichiers S3 File Gateway vous permet de réaliser des tâches d'intégration de charges de travail cloud dans Amazon S3, de sauvegarde et archivage, de hiérarchisation et de migration des données du stockage vers laAWSCloud. Le diagramme suivant offre une présentation du déploiement du stockage de fichiers pour Storage Gateway.



S3 File Gateway convertit les fichiers en objets S3 lors du chargement de fichiers sur Amazon S3. L'interaction entre les opérations de fichiers effectuées sur des partages de fichiers sur des objets S3 File Gateway et S3 nécessite que certaines opérations soient soigneusement prises en compte lors de la conversion entre fichiers et objets.

Les opérations courantes sur les fichiers modifient les métadonnées des fichiers, ce qui entraîne la suppression de l'objet S3 actuel et la création d'un nouvel objet S3. Le tableau suivant présente des exemples d'opérations sur les fichiers et de l'impact sur les objets S3.

Opération des fichiers	Impact sur l'objet S3	Implication pour les classes
Renommer un fichier	Remplace l'objet S3 existant et crée un nouvel objet S3 pour chaque fichier	Des frais de suppression anticipée et de récupération peuvent s'appliquer
Renommer un dossier	Remplace tous les objets S3 existants et crée de nouveaux objets S3 pour chaque dossier et fichiers de la structure de dossiers	Des frais de suppression anticipée et de récupération peuvent s'appliquer
Modifier les autorisations de fichiers/dossiers	Remplace l'objet S3 existant et crée un nouvel objet S3 pour chaque fichier ou dossier	Des frais de suppression anticipée et de récupération peuvent s'appliquer
Modifier la propriété des fichiers/dossiers	Remplace l'objet S3 existant et crée un nouvel objet S3 pour chaque fichier ou dossier	Des frais de suppression anticipée et de récupération peuvent s'appliquer
Ajouter à un fichier	Remplace l'objet S3 existant et crée un nouvel objet S3 pour chaque fichier	Des frais de suppression anticipée et de récupération peuvent s'appliquer

Lorsqu'un fichier est écrit sur la passerelle de fichiers S3 par un client NFS ou SMB, la passerelle de fichiers télécharge les données du fichier vers Amazon S3 suivies de ses métadonnées (propriétaires, horodatages, etc.). Le téléchargement des données du fichier crée un objet S3, et le téléchargement des métadonnées du fichier met à jour les métadonnées de l'objet S3. Ce processus crée une autre version de l'objet, entraînant deux versions d'un objet. Si la gestion des versions S3 est activée, les deux versions seront stockées.

Lorsqu'un fichier est modifié dans la passerelle de fichiers S3 par un client NFS ou SMB après son téléchargement sur Amazon S3, la passerelle de fichiers S3 télécharge les données nouvelles ou modifiées au lieu de charger le fichier entier. La modification du fichier entraîne la création d'une nouvelle version de l'objet S3.

Lorsque la passerelle de fichiers S3 télécharge des fichiers plus volumineux, il peut être nécessaire de charger des morceaux plus petits du fichier avant que le client n'ait fini d'écrire sur la passerelle de fichiers S3. Cela s'explique notamment par la libération de l'espace cache ou un taux d'écriture élevé dans un partage de fichiers. Il peut en résulter plusieurs versions d'un objet dans le compartiment S3.

Vous devez surveiller votre compartiment S3 pour déterminer le nombre de versions d'un objet existant avant de configurer des stratégies de cycle de vie pour déplacer des objets vers différentes classes de stockage. Vous devez configurer l'expiration du cycle de vie pour les versions précédentes afin de minimiser le nombre de versions dont vous disposez pour un objet dans votre compartiment S3. L'utilisation de la réplication de même région (SRR) ou de la réplication entre régions (CRR) entre compartiments S3 augmentera le stockage utilisé.

Configuration pour Amazon S3 File Gateway

Cette section fournit des instructions sur la mise en route sur Amazon S3 File Gateway. Pour commencer, vous devez créer un compte AWS. Si vous utilisez pour la première fois, nous vous recommandons de lire la page [Régions](#) et [Prérequis](#) sections.

Rubriques

- [S'inscrire à Amazon Web Services](#)
- [Créer un utilisateur IAM](#)
- [Configuration requise de la passerelle de fichiers](#)
- [Accès à AWS Storage Gateway](#)
- [Régions AWS prises en charge](#)

S'inscrire à Amazon Web Services

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

Pour s'inscrire à un Compte AWS

1. Ouvrez <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 et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Créer un utilisateur IAM

Après avoir créé votre AWS Effectuez les étapes suivantes pour créer un compte AWS Identity and Access Management (IAM) pour vous-même. Ensuite, vous ajoutez cet utilisateur à un groupe disposant d'autorisations d'administration.

Pour créer un administrateur pour vous-même et ajouter l'utilisateur à un groupe d'administrateurs (console)

1. Connectez-vous à la [console IAM](#) en tant que propriétaire du compte en choisissant Root user (Utilisateur racine) et en saisissant votre adresse e-mail Compte AWS. Sur la page suivante, saisissez votre mot de passe.

Note

Nous vous recommandons vivement de respecter la bonne pratique qui consiste à avoir recours à l'utilisateur IAM **Administrator** suivant et protéger les informations d'identification de l'utilisateur racine. Connectez-vous en tant qu'utilisateur racine pour effectuer certaines [tâches de gestion des comptes et des services](#).

2. Dans le panneau de navigation, choisissez Utilisateurs, puis Add user (Ajouter un utilisateur).
3. Dans Nom d'utilisateur, saisissez **Administrator**.
4. Cochez la case à côté de accès à la AWS Management Console. Ensuite, sélectionnez Mot de passe personnalisé, puis saisissez votre nouveau mot de passe dans la zone de texte.
5. (Facultatif) Par défaut, AWS oblige le nouvel utilisateur à créer un nouveau mot de passe lors de sa première connexion. Décochez la case en regard de L'utilisateur doit créer un nouveau mot de passe à sa prochaine connexion pour autoriser le nouvel utilisateur à réinitialiser son mot de passe une fois qu'il s'est connecté.
6. Choisissez Next (Suivant) Permissions (Autorisations).
7. Sous Définir des autorisations, choisissez Ajouter un utilisateur au groupe.
8. Choisissez Créer un groupe.
9. Dans la boîte de dialogue Créer un groupe, pour Nom du groupe, saisissez **Administrators**.
10. Choisissez Filtrer les polices, puis sélectionnez fonction de tâche gérée par AWS pour filtrer le contenu du tableau.
11. Dans la liste des politiques, cochez la case AdministratorAccess. Choisissez ensuite Créer un groupe.

Note

Avant de pouvoir utiliser les autorisations AdministratorAccess pour accéder à la console AWS Billing and Cost Management, vous devez activer l'accès du rôle et de

l'utilisateur IAM à la facturation. Pour ce faire, suivez les instructions de [l'étape 1 du didacticiel sur la délégation de l'accès à la console de facturation](#).

12. De retour dans la liste des groupes, activez la case à cocher du nouveau groupe. Choisissez Actualiser si nécessaire pour afficher le groupe dans la liste.
13. Choisissez Next (Suivant) Tags (Balises).
14. (Facultatif) Ajoutez des métadonnées à l'utilisateur en associant les balises sous forme de paires clé-valeur. Pour en savoir plus sur l'utilisation des étiquettes dans IAM, consultez [Étiqueter des entités IAM](#) dans le guide de l'utilisateur IAM.
15. Choisissez Next (Suivant) Vérification pour afficher la liste des membres du groupe à ajouter au nouvel utilisateur. Une fois que vous êtes prêt à continuer, choisissez Créer un utilisateur.

Vous pouvez utiliser ce même processus pour créer d'autres groupes et utilisateurs et pour accorder à vos utilisateurs l'accès aux ressources de votre Compte AWS. Pour savoir comment utiliser des stratégies qui limitent les autorisations d'accès des utilisateurs à des ressources AWS spécifiques, veuillez consulter [Gestion des accès](#) et [Exemples de stratégies](#).

Configuration requise de la passerelle de fichiers

Sauf mention contraire, les exigences suivantes sont communes à tous les types de passerelle de fichiers dans AWS Storage Gateway. Votre configuration doit répondre aux exigences de cette section. Vérifiez les exigences qui s'appliquent à la configuration de votre passerelle avant de déployer votre passerelle.

Rubriques

- [Prérequis requis](#)
- [Exigences en matière de matériel et de stockage](#)
- [Exigences pour le réseau et le pare-feu](#)
- [Hyperviseurs pris en charge et exigences pour l'hôte](#)
- [Clients NFS pris en charge pour une passerelle de fichiers](#)
- [Clients SMB pris en charge pour une passerelle de fichiers](#)
- [Opérations de système de fichiers prises en charge pour une passerelle de fichiers](#)

Prérequis requis

Avant d'utiliser une passerelle de fichiers Amazon FSx (FSx File Gateway), vous devez répondre aux exigences suivantes :

- Créez et configurez un système de fichiers FSx for Windows File Server. Pour obtenir des instructions, consultez [Étape 1 : Créer votre système de fichiers](#) dans le Guide de l'utilisateur Amazon FSx for Windows File Server.
- Configurez Microsoft Active Directory (AD).
- Assurez-vous que la bande passante réseau est suffisante entre la passerelle et AWS. Un minimum de 100 Mbps est requis pour télécharger, activer et mettre à jour correctement la passerelle.
- Configurez votre réseau privé, votre VPN ou AWS Direct Connect entre votre Amazon Virtual Private Cloud (Amazon VPC) et l'environnement sur site où vous déployez votre passerelle de fichiers FSx.
- Assurez-vous que votre passerelle peut résoudre le nom de votre contrôleur de domaine Active Directory. Vous pouvez utiliser DHCP dans votre domaine Active Directory pour gérer la résolution ou spécifier manuellement un serveur DNS à partir du menu des paramètres de configuration réseau de la console locale de la passerelle.

Exigences en matière de matériel et de stockage

Les sections suivantes fournissent des informations sur les exigences matérielles minimales et les paramètres pour votre passerelle, et la quantité minimale d'espace disque à allouer pour le stockage requis.

Pour obtenir des informations sur les bonnes pratiques permettant d'optimiser les performances des passerelles de fichiers, consultez [Conseils sur les performances des passerelles de fichiers](#).

Exigences en matière de matériel pour les machines virtuelles sur site

Lors du déploiement de votre passerelle sur site, vous devez veiller à ce que le matériel sous-jacent sur lequel vous déployez la machine virtuelle de la passerelle (machine virtuelle) soit en mesure de dédier au minimum les ressources suivantes :

- Quatre processeurs virtuels attribués à la VM
- 16 GiB de mémoire RAM réservée pour les passerelles de fichiers
- 80 GiB d'espace disque pour l'installation de l'image de l'ordinateur virtuel et les données système

Pour plus d'informations, consultez [Optimisation des performances de la passerelle](#). Pour plus d'informations sur la façon dont votre matériel affecte les performances de l'ordinateur virtuel de la passerelle, consultez [Quotas pour partages de fichiers](#).

Configuration requise pour les types d'instances Amazon EC2

Lors du déploiement de votre passerelle sur Amazon Elastic Compute Cloud (Amazon EC2), la taille d'instance doit être au moins **xlarge** pour que votre passerelle fonctionne. Toutefois, pour la famille d'instances optimisées pour le calcul, la taille doit être au moins **2xlarge**. Utilisez l'un des types d'instance suivants recommandés pour votre type de passerelle.

Recommandé pour les types de passerelle de fichiers

- Famille d'instances à visée générale — type d'instance m4 ou m5.
- Famille d'instances optimisées pour le calcul — types d'instance c4 ou c5. Sélectionnez la taille d'instance 2xlarge ou une taille supérieure pour répondre aux exigences de RAM.
- Famille d'instances optimisées pour la mémoire : types d'instance r3.
- Famille d'instances optimisées pour le stockage : types d'instance i3.

Note

Lorsque vous lancez votre passerelle dans Amazon EC2 et que le type d'instance que vous avez choisi prend en charge le stockage éphémère, les disques sont répertoriés automatiquement. Pour en savoir plus sur le stockage d'instance Amazon EC2, consultez [Stockage d'instance](#) dans le Guide de l'utilisateur Amazon EC2.

Les écritures d'application sont stockées dans le cache de manière synchrone, puis chargées de manière asynchrone vers un stockage durable dans Amazon S3. Si le stockage éphémère est perdu suite à l'arrêt d'une instance avant la fin du chargement, les données résidant encore dans le cache et qui n'ont pas encore été écrites dans Amazon Simple Storage Service (Amazon S3) risquent d'être perdues. Avant d'arrêter l'instance qui héberge la passerelle, assurez-vous que le `CachePercentDirty` Métrique CloudWatch est 0. Pour de plus amples informations sur le stockage éphémère, veuillez consulter [Utilisation du stockage éphémère avec des passerelles EC2](#). Pour plus d'informations sur la surveillance des métriques pour votre passerelle de stockage, consultez [Surveillance de la passerelle de fichiers](#).

Si le compartiment S3 contient plus de 5 millions d'objets et que vous utilisez un volume SSD à usage général, un volume EBS racine d'au moins 350 GiB est nécessaire pour que la passerelle présente des performances acceptables au démarrage. Pour savoir comment

accroître la taille du volume, consultez [Modification d'un volume EBS à l'aide d'Elastic Volumes \(console\)](#).

Besoins de stockage

Outre les 80 GiB d'espace disque pour la machine virtuelle, vous avez également besoin de disques supplémentaires pour la passerelle.

Type de passerelle	Cache (minimum)	Cache (maximum)			
Passerelle de fichiers	150 GiB	64 Tio			

Note

Vous pouvez configurer un ou plusieurs disques locaux pour votre cache, jusqu'à la capacité maximale.

Lorsque vous ajoutez un cache à une passerelle existante, il est important de créer des disques sur votre hôte (hyperviseur ou instance Amazon EC2). Ne modifiez pas la taille des disques existants si les disques ont été alloués antérieurement en tant que cache.

Pour plus d'informations sur les quotas de passerelle, consultez [Quotas pour partages de fichiers](#).

Exigences pour le réseau et le pare-feu

Votre passerelle nécessite un accès à Internet, aux réseaux locaux, aux serveurs DNS, aux pare-feu, aux routeurs, etc.

Les besoins en bande passante réseau varient en fonction de la quantité de données chargées et téléchargées par la passerelle. Un minimum de 100 Mbps est requis pour télécharger, activer et mettre à jour correctement la passerelle. Vos modèles de transfert de données détermineront la bande passante nécessaire pour prendre en charge votre charge de travail.

Vous trouverez ci-après des informations sur les ports obligatoires et sur l'autorisation d'accès via les pare-feu et les routeurs.

Note

Dans certains cas, vous pouvez déployer FSx File Gateway sur Amazon EC2 ou utiliser d'autres types de déploiement (y compris sur site) avec des stratégies de sécurité réseau restreignant les plages d'adresses IP. Dans ces cas, votre passerelle peut connaître des problèmes de connectivité de service lorsque les valeurs de plage IP changent. Les valeurs de la plage d'adresses IP que vous devez utiliser se trouvent dans le sous-ensemble de services Amazon pour la Région dans laquelle vous activez votre passerelle. Pour consulter les valeurs des plages d'adresses IP actuelles, consultez [AWS Plages d'adresses IP](#) dans la Référence générale.

Rubriques

- [Exigences pour les ports](#)
- [Exigences en matière de mise en réseau et de pare-feu pour l'appliance matérielle Storage Gateway](#)
- [Accorder l'accès à AWS Storage Gateway via les pare-feu et les routeurs](#)
- [Configuration des groupes de sécurité pour votre instance de passerelle Amazon EC2](#)

Exigences pour les ports

Storage Gateway nécessite que certains ports soient autorisés pour son fonctionnement. L'illustration suivante montre les ports requis que vous devez autoriser pour chaque type de passerelle. Certains ports sont requis par tous les types de passerelle, d'autres sont nécessaires uniquement pour des types de passerelle spécifiques. Pour plus d'informations sur les exigences de port, consultez [Exigences de ports](#).

Ports communs à tous les types de passerelles

Les ports suivants sont communs à tous les types de passerelles et sont requis par tous les types de passerelles.

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
TCP	443 (HTTPS)	Sortant	Storage Gateway	AWS	Pour la communication

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
					tion entre Storage Gateway et leAWSpoint de terminaison du service. Pour plus d'informations sur les points de terminaison de service, consultez Accorder l'accès à AWS Storage Gateway via les pare-feu et les routeurs.

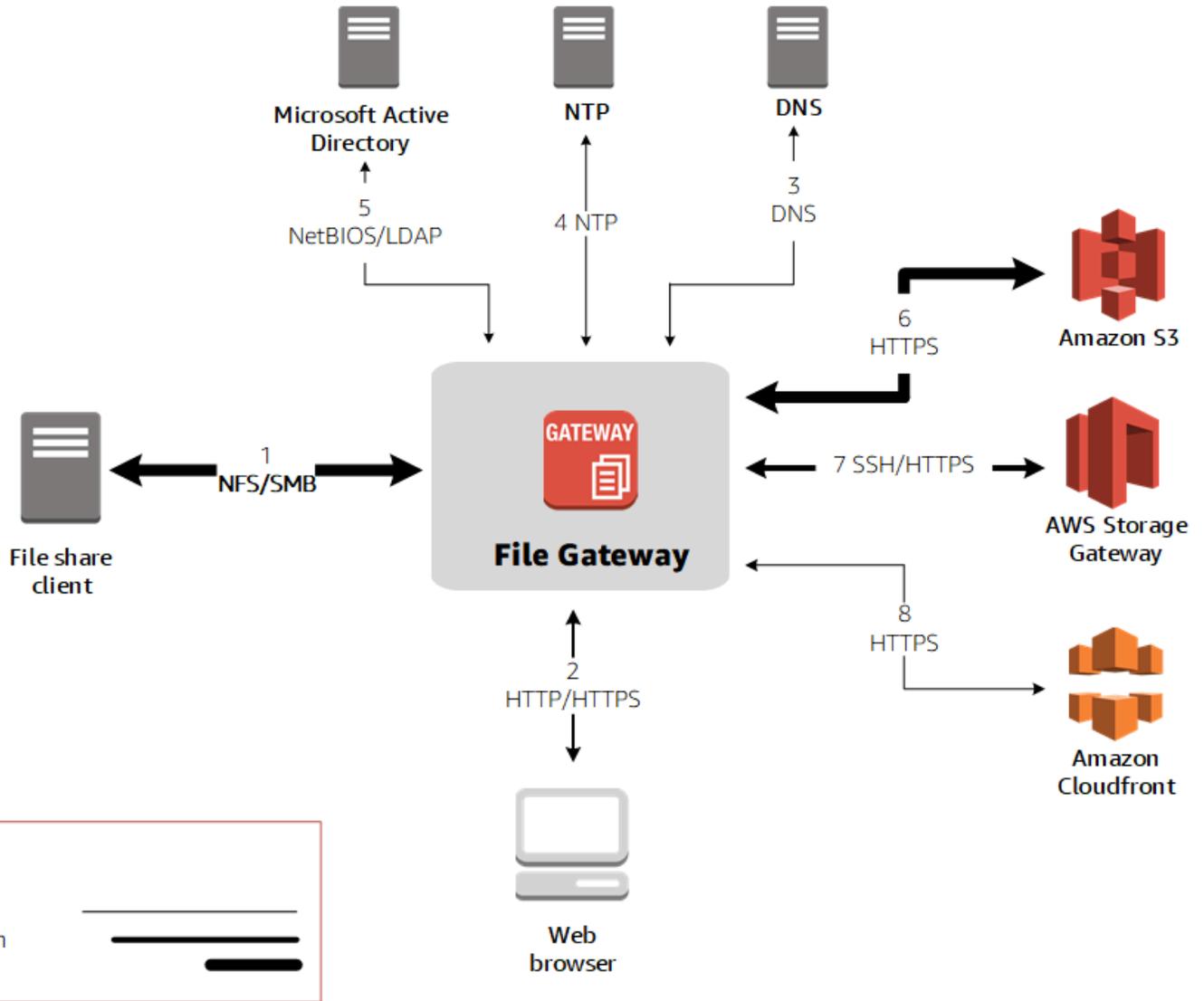
Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
TCP	80 (HTTP)	Entrant	L'hôte à partir duquel vous vous connectez auAWS Management Console.	Storage Gateway	<p>Par les systèmes locaux pour obtenir la clé d'activation Storage Gateway. Le port 80 est utilisé uniquement lors de l'activation de l'application Storage Gateway.</p> <p>Storage Gateway ne nécessite pas de port 80 pour être accessible publiquement. Le niveau requis de l'accès au port 80 dépend de la configuration de votre réseau. Si vous activez votre passerelle</p>

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
					à partir de la console Storage Gateway, l'hôte à partir duquel vous vous connectez à la console doit avoir accès au port 80 de votre passerelle.
UDP/UDP	53 (DNS)	Sortant	Storage Gateway	Serveur DNS	Pour toute communication entre Storage Gateway et le serveur DNS.

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
TCP	22 (canal de support)	Sortant	Storage Gateway	AWS Support	AutoriseAWS Supportpour accéder à votre passerelle afin de vous aider à résoudre les problèmes de passerelle. Ce port ne doit pas être ouvert pour que votre passerelle fonctionne normalement, mais il doit l'être pour résoudre les problèmes.
UDP	123 (NTP)	Sortant	Client NTP	Serveur NTP	Utilisé par les systèmes locaux pour synchroniser l'heure de l'ordinateur virtuel et celle de l'hôte.

Ports pour les passerelles de fichiers

L'illustration suivante montre les ports à ouvrir pour une passerelle de fichiers S3.



Note
 Pour consulter les exigences de port spécifiques, consultez [Exigences de ports](#).

Pour S3 File Gateway, il vous suffit d'utiliser Microsoft Active Directory pour autoriser les utilisateurs de domaine à accéder à un partage de fichiers SMB (Server Message Block). Vous pouvez joindre votre passerelle de fichiers à un domaine Microsoft Windows valide (résolu par DNS).

Vous pouvez également utiliser l'AWS Directory Service pour créer un [AWS Managed Microsoft AD](#) dans Amazon Web Services Cloud. Pour la plupart des déploiements AWS Managed Microsoft AD, vous devez configurer le protocole DHCP (Dynamic Host Configuration Protocol) pour votre VPC.

Pour plus d'informations sur la création d'un jeu d'options DHCP, consultez [Créer un jeu d'options DHCP](#) dans le [AWS Directory Service Guide d'administration](#).

Outre les ports communs, Amazon S3 File Gateway nécessite les ports suivants.

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
TCP/UDP	2049 (NFS)	Entrant	Clients NFS	Storage Gateway	Pour que les systèmes locaux se connectent aux partages NFS exposés par la passerelle.
TCP/UDP	111 (NFSv3)	Entrant	Client NFSv3	Storage Gateway	Pour que les systèmes locaux se connectent à l'outil de mappage de port exposé par la passerelle.

 **Note**
Ce port n'est nécessaire que pour NFSv3.

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
TCP/UDP	20048 (NFSv3)	Entrant	Client NFSv3	Storage Gateway	Pour que les systèmes locaux se connectent aux supports exposés par la passerelle.

 **Note**

Ce port n'est nécessaire que pour NFSv3.

Exigences en matière de mise en réseau et de pare-feu pour l'appliance matérielle Storage

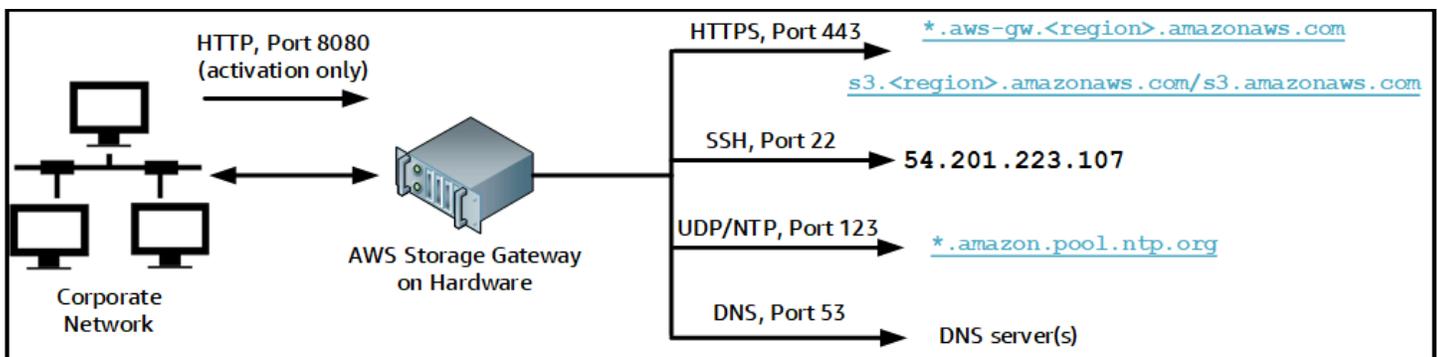
Chaque appliance matérielle Storage Gateway nécessite les services réseau suivants :

- Accès Internet— connexion réseau permanente à Internet via une interface réseau sur le serveur.
- Services DNS— Services DNS pour toute communication entre l'appliance matérielle et le serveur DNS.
- Synchronisation du temps— Un service de temps Amazon NTP doit être accessible.
- Adresse IP— Une adresse DHCP ou IPv4 statique attribuée. Vous ne pouvez pas affecter d'adresse IPv6.

Le serveur Dell PowerEdge R640 comporte cinq ports réseau physiques à l'arrière. L'arrière du serveur comporte les ports suivants de gauche à droite :

1. iDRAC
2. em1
3. em2
4. em3
5. em4

Vous pouvez utiliser le port iDRAC pour la gestion du serveur à distance.



Une appliance matérielle requiert les ports ci-dessous pour fonctionner.

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
SSH	22	Sortant	Appliance matérielle	54.201.223.107	canal de support
DNS	53	Sortant	Appliance matérielle	Serveurs DNS	Résolution de noms
UDP/NTP	123	Sortant	Appliance matérielle	*.amazon.pool.ntp.org	Synchronisation du temps

Protocole	Port	Direction	Source	Destination (Destination)	Utilisation
HTTPS	443	Sortant	Appliance matérielle	* .amazonaws.com	Transfert de données
HTTP	8080	Entrant	AWS	Appliance matérielle	Activation (brève)

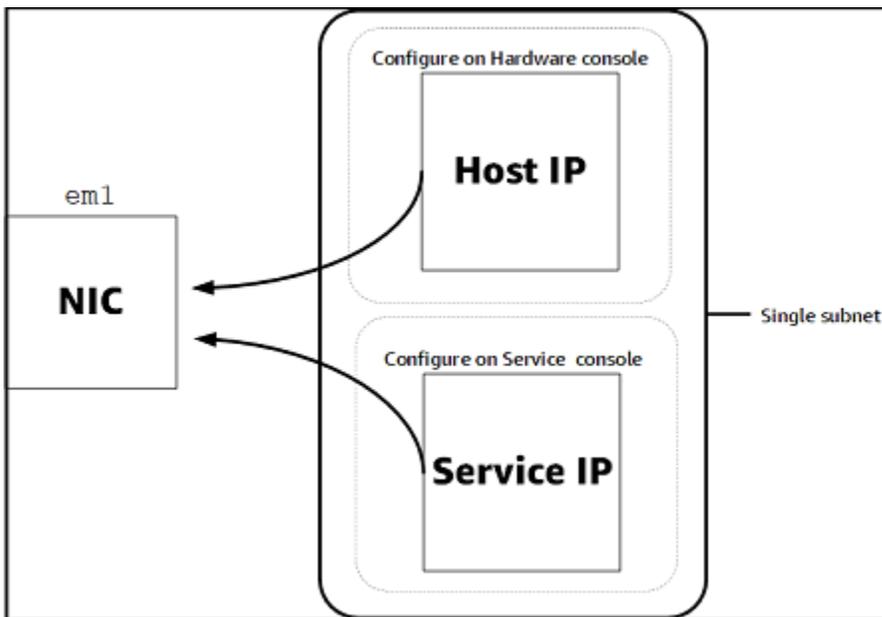
Pour fonctionner comme prévu, une appliance matérielle nécessite que les paramètres de réseau et de pare-feu soient paramétrés comme suit :

- Configurez toutes les interfaces réseau connectées dans la console du matériel.
- Vérifiez que chaque interface réseau se trouve sur un sous-réseau spécifique.
- Fournissez à toutes les interfaces réseau connectées un accès Internet sortant à tous les points de terminaison énumérés dans le diagramme précédent.
- Configurez au moins une interface réseau pour qu'elle prenne en charge l'appliance matérielle. Pour plus d'informations, consultez [Configuration des paramètres réseau](#).

 Note

Pour accéder à une illustration de l'arrière du serveur avec ses ports, veuillez consulter [Montage en rack de votre appliance matérielle et connexion à l'alimentation](#).

Toutes les adresses IP situées sur la même interface réseau (NIC), qu'elles concernent une passerelle ou un hôte, doivent se trouver sur le même sous-réseau. L'illustration suivante est le schéma d'adressage.



Pour en savoir plus sur l'activation et la configuration d'une appliance matérielle, consultez [Utilisation de l'appliance matérielle Storage Gateway](#).

Accorder l'accès à AWS Storage Gateway via les pare-feu et les routeurs

Votre passerelle a besoin d'accéder aux points de terminaison de service suivants afin de communiquer avec AWS. Si vous utilisez un pare-feu ou un routeur pour filtrer ou limiter le trafic réseau, vous devez les configurer afin de permettre les communications sortantes à ces points de terminaison de service AWS.

⚠ Important

En fonction de votre passerelle AWS Région, remplacer *région* dans le point de terminaison du service avec la chaîne Region correcte.

Le point de terminaison de service suivant est requis par toutes les passerelles pour les opérations de compartiment de tête.

```
s3.amazonaws.com:443
```

Les points de terminaison de service suivants sont requis par toutes les passerelles pour le chemin de contrôle (anon-cp, client-cp, proxy-app) et le chemin de données (dp-1) opérations.

```
anon-cp.storagegateway.region.amazonaws.com:443  
client-cp.storagegateway.region.amazonaws.com:443  
proxy-app.storagegateway.region.amazonaws.com:443  
dp-1.storagegateway.region.amazonaws.com:443
```

Le point de terminaison de service de passerelle suivant est requis pour effectuer des appels d'API.

```
storagegateway.region.amazonaws.com:443
```

L'exemple suivant est un point de terminaison de service de passerelle dans la région USA Ouest (Oregon) (us-west-2).

```
storagegateway.us-west-2.amazonaws.com:443
```

Les points de terminaison de service Amazon S3 ci-dessous sont utilisés uniquement par les passerelles de fichiers. Une passerelle de fichiers nécessite que ce point de terminaison accède au compartiment Amazon S3 sur lequel un partage de fichiers est mappé.

```
s3.region.amazonaws.com
```

L'exemple suivant est un point de terminaison de service Amazon S3 dans la région USA Est (Ohio) (us-east-2).

```
s3.us-east-2.amazonaws.com
```

Note

Si votre passerelle ne parvient pas à déterminer la région AWS où se trouve le compartiment S3, ce point de terminaison de service est par défaut `s3.us-east-1.amazonaws.com`. Nous vous recommandons d'autoriser l'accès à la région US East (N. Virginia) (us-east-1) en plus des régions où est activée la passerelle et où se trouve votre compartiment S3.

Voici les points de terminaison de service Amazon S3 pour AWS GovCloud (US) Régions.

```
s3-fips-us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))  
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))
```

```
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))  
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
```

L'exemple suivant est un point de terminaison de service FIPS pour un compartiment S3 dans leAWS Région GovCloud (US-West).

```
bucket-name.s3-fips-us-gov-west-1.amazonaws.com
```

Le point de terminaison Amazon CloudFront suivant est requis pour que Storage Gateway obtienne la liste des produits disponibles.AWS Régions.

```
https://d4kdq0yaxexbo.cloudfront.net/
```

Une machine virtuelle Storage Gateway est configurée pour utiliser les serveurs NTP suivants.

```
0.amazon.pool.ntp.org  
1.amazon.pool.ntp.org  
2.amazon.pool.ntp.org  
3.amazon.pool.ntp.org
```

- Storage Gateway : pour prise en chargeAWS Les régions et une liste deAWS points de terminaison de service que vous pouvez utiliser avec Storage Gateway, voir [AWS Storage Gateway Points de terminaison et quotas](#) dans leAWS Référence générale.
- Appliance matérielle Storage Gateway — Pour prise en chargeAWS Régions que vous pouvez utiliser avec l'appliance matérielle, voir [Régions du matériel Storage Gateway](#) dans leAWS Référence générale.

Configuration des groupes de sécurité pour votre instance de passerelle Amazon EC2

DansAWS Storage Gateway, un groupe de sécurité contrôle le trafic vers votre instance de passerelle Amazon EC2. Lorsque vous configurez un groupe de sécurité, nous vous recommandons ce qui suit :

- Le groupe de sécurité ne doit pas autoriser les connexions entrantes en provenance d'Internet. Il doit autoriser uniquement les instances du groupe de sécurité de la passerelle à communiquer avec la passerelle.

Si vous avez besoin d'autoriser les instances à se connecter à la passerelle en dehors de son groupe de sécurité, nous vous recommandons d'autoriser les connexions uniquement sur les ports 3260 (pour les connexions iSCSI) et 80 (pour l'activation).

- Si vous souhaitez activer votre passerelle à partir d'un hôte Amazon EC2 en dehors du groupe de sécurité de la passerelle, autorisez les connexions entrantes sur le port 80 à partir de l'adresse IP de cet hôte. Si vous ne pouvez pas déterminer l'adresse IP de l'hôte d'activation, vous pouvez ouvrir le port 80, activer votre passerelle, puis fermer l'accès sur le port 80 après l'activation.
- Autorisez l'accès au port 22 uniquement si vous utilisez AWS Support à des fins de dépannage. Pour plus d'informations, consultez [Vous voulez AWS Support pour résoudre les problèmes de votre passerelle EC2.](#)

Dans certains cas, vous pouvez utiliser une instance Amazon EC2 comme initiateur (c'est-à-dire, pour vous connecter à des cibles iSCSI sur une passerelle déployée sur Amazon EC2). Dans ce cas, nous vous recommandons une approche en deux étapes :

1. Vous devez lancer l'instance d'initiateur dans le même groupe de sécurité que la passerelle.
2. Vous devez configurer l'accès afin que l'initiateur puisse communiquer avec la passerelle.

Pour plus d'informations sur les ports à ouvrir pour votre passerelle, consultez [Exigences de ports.](#)

Hyperviseurs pris en charge et exigences pour l'hôte

Vous pouvez exécuter Storage Gateway sur site en tant qu'appliance de machine virtuelle ou qu'appliance matérielle physique, ou dans AWS en tant qu'instance Amazon EC2.

Storage Gateway prend en charge les versions d'hyperviseur et les hôtes suivants :

- VMware ESXi Hypervisor (versions 6.0, 6.5 ou 6.7) — Une version gratuite de VMware est disponible sur le [Site Web VMware](#). Pour cette configuration, vous aurez également besoin d'un client VMware vSphere pour vous connecter à l'hôte.
- Microsoft Hyper-V Hypervisor (versions 2012 R2 ou 2016) — Une version autonome et gratuite d'Hyper-V est disponible sur le site web [Centre de téléchargement Microsoft](#). Pour cette configuration, vous aurez besoin d'un Microsoft Hyper-V Manager sur un ordinateur client Microsoft Windows pour vous connecter à l'hôte.
- KVM (machine virtuelle basée sur le noyau Linux) — Technologie de virtualisation libre et open source. KVM est inclus dans toutes les versions de Linux 2.6.20 et plus récentes. Storage Gateway

est testé et pris en charge pour les distributions CentOS/Rhel 7.7, Ubuntu 16.04 LTS et Ubuntu 18.04 LTS. Toute autre distribution Linux moderne peut fonctionner, mais l'interopérabilité ou les performances ne sont pas garanties. Nous recommandons cette option si vous disposez déjà d'un environnement KVM et que vous connaissez déjà le fonctionnement de KVM.

- Instance Amazon EC2 — Storage Gateway fournit une Amazon Machine Image (AMI) qui contient l'image de l'ordinateur virtuel de la passerelle. Pour savoir comment déployer une passerelle sur Amazon EC2, consultez [Déploiement d'une passerelle de fichiers sur un hôte Amazon EC2](#).
- Appliance matérielle Storage Gateway — Storage Gateway fournit une appliance matérielle physique en tant qu'option de déploiement sur site pour les lieux ayant une infrastructure de machine virtuelle limitée.

Note

Storage Gateway ne prend pas en charge la récupération d'une passerelle à partir d'une machine virtuelle créée à partir d'un instantané ou d'un clone d'une autre machine virtuelle de passerelle, ou de votre AMI Amazon EC2. Si l'ordinateur virtuel de la passerelle fonctionne mal, activez une nouvelle passerelle et récupérez vos données pour cette passerelle. Pour plus d'informations, consultez [Récupération après un arrêt inattendu de la machine virtuelle](#). Storage Gateway ne prend pas en charge la mémoire dynamique ni la mémoire virtuelle ballon.

Clients NFS pris en charge pour une passerelle de fichiers

Les passerelles de fichiers prennent en charge les clients NFS (Network File System) suivants :

- Amazon Linux
- Mac OS X

Note

Nous vous recommandons de définir l'`rsizetwsizeoptions` de montage à 64 Ko pour améliorer les performances lors du montage de partages de fichiers NFS sur Mac OS X.

- RHEL 7
- SUSE Linux Enterprise Server 11 et SUSE Linux Enterprise Server 12

- Ubuntu 14.04
- Microsoft Windows 10 Enterprise, Windows Server 2012 et Windows Server 2016. Les clients natifs prennent en charge uniquement NFS version 3.
- Windows 7 Enterprise et Windows Server 2008.

Les clients natifs prennent en charge uniquement NFS version 3. La taille d'E/S NFS maximale prise en charge est de 32 Ko ; vous risquez donc d'être confronté à des performances dégradées sur ces versions de Windows.

Note

Vous pouvez désormais utiliser des partages de fichiers SMB lorsque l'accès est requis via des clients Windows (SMB) au lieu de faire appel à des clients NFS Windows.

Clients SMB pris en charge pour une passerelle de fichiers

Les passerelles de fichiers prennent en charge les clients SMB (Service Message Block) suivants :

- Microsoft Windows Server 2008 et version ultérieure
- Bureau Windows versions : 10, 8 et 7.
- Windows Terminal Server s'exécutant sur Windows Server 2008 et versions ultérieures

Note

Le chiffrement Server Message Block nécessite des clients prenant en charge SMB v2.1.

Opérations de système de fichiers prises en charge pour une passerelle de fichiers

Le client NFS ou SMB peut écrire, lire, supprimer et tronquer des fichiers. Lorsque les clients envoient des écritures à AWS Storage Gateway, l'écriture dans le cache local se fait de manière synchrone. Ensuite, l'écriture vers Amazon S3 est effectuée de façon asynchrone via des transferts optimisés. Les lectures sont tout d'abord diffusées par le biais du cache local. Si les données ne sont pas disponibles, elles sont récupérées via S3 en tant que cache en lecture.

Les lectures et écritures sont optimisées de sorte que seules les parties modifiées ou demandées sont transférées via la passerelle. Supprime les objets supprimés d'Amazon S3. Les répertoires sont gérés en tant qu'objets de dossiers dans S3, en utilisant la même syntaxe que la console Amazon S3.

Des opérations HTTP telles que GET, PUT, UPDATE et DELETE peuvent modifier des fichiers dans un partage de fichiers. Ces opérations sont conformes aux fonctions atomiques de création, lecture, mise à jour et suppression.

Accès à AWS Storage Gateway

Vous pouvez utiliser le plugin [AWS Storage Gateway console](#) pour effectuer différentes configurations de la passerelle et des tâches de gestion. La section de mise en route et diverses autres sections de ce manuel utilisent la console pour illustrer les fonctionnalités de la passerelle.

En outre, vous pouvez utiliser l'API AWS Storage Gateway pour configurer et gérer vos passerelles par programme. Pour plus d'informations sur l'API, consultez [Référence API pour Storage Gateway](#).

Vous pouvez également utiliser l'AWS Les kits SDK pour développer des applications qui interagissent avec Storage Gateway. Le AWS Les kits de développement logiciel SDK pour Java, .NET et PHP enveloppent l'API Storage Gateway sous-jacente afin de simplifier vos tâches de programmation. Pour plus d'informations sur le téléchargement des bibliothèques de kits SDK, consultez le [AWS Centre de développement](#).

Pour de plus amples informations sur la tarification, veuillez consulter [Tarification AWS Storage Gateway](#).

Régions AWS prises en charge

- Storage Gateway — Pour support AWS Les régions et une liste de AWS points de terminaison de service que vous pouvez utiliser avec Storage Gateway, voir [AWS Storage Gateway Points de terminaison et quotas](#) dans le AWS Référence générale.
- Appliance matérielle Storage Gateway — Pour connaître les régions prises en charge que vous pouvez utiliser avec l'appliance matérielle, consultez la section [AWS Storage Gateway Régions matérielles](#) dans le AWS Référence générale.

Utilisation de l'appliance matérielle Storage Gateway

L'appliance matérielle Storage Gateway est une appliance matérielle physique avec le logiciel Storage Gateway qui est préinstallé sur une configuration de serveur validée. Vous pouvez gérer votre appliance matérielle à partir du Matérielsur laAWS Storage Gatewayconsole

L'appliance matérielle est un serveur 1U hautes performances que vous pouvez déployer dans votre centre de données, ou bien sur site, à l'intérieur de votre pare-feu d'entreprise. Lorsque vous achetez et activez votre appliance matérielle, le processus d'activation associe votre appliance matérielle à votre appliance matérielle.AWS. Après l'activation, votre appliance matérielle apparaît sur la console en tant que passerelle sur l'Matériel. Vous pouvez configurer votre appliance matérielle en tant que passerelle de fichier, passerelle de bande ou type de passerelle de volume. La procédure que vous utilisez pour déployer et activer ces types de passerelle sur une appliance matérielle est la même que sur les plateformes virtuelles.

L'appliance matérielle Storage Gateway peut être commandée directement auprès duAWS Storage Gatewayconsole

Pour commander une appliance matérielle

1. Ouvrez la console Storage Gateway à l'adresse<https://console.aws.amazon.com/storagegateway/home>et choisissez leAWSRégion dans laquelle votre appliance doit se trouver.
2. ChoisissezMatérielDans le volet de navigation.
3. ChoisissezAppliance matérielle, puisContinuer. Vous êtes redirigé vers leAWSElemental Appliances et Software Management Console pour demander un devis de vente.
4. Remplissez les informations nécessaires et choisissezSoumettre.

Une fois les informations examinées, un devis de vente est généré et vous pouvez poursuivre le processus de commande et soumettre un bon de commande ou organiser un prépaiement.

Pour afficher un devis de vente ou un historique de commandes pour l'appliance matérielle

1. Ouvrez la console Storage Gateway à l'adresse<https://console.aws.amazon.com/storagegateway/home>.
2. ChoisissezMatérielDans le volet de navigation.

3. Choisissez **Devis et commandes**, puis **Continuer**. Vous êtes redirigé vers le **AWS Elemental Appliances et Software Management Console** pour consulter les devis de vente et l'historique des commandes.

Dans les sections suivantes, vous trouverez des instructions sur la configuration, la configuration, l'activation, le lancement et l'utilisation d'une appliance matérielle Storage Gateway.

Rubriques

- [Régions AWS prises en charge](#)
- [Configuration de votre appliance matérielle](#)
- [Montage en rack de votre appliance matérielle et connexion à l'alimentation](#)
- [Configuration des paramètres réseau](#)
- [Activation de votre appliance matérielle](#)
- [Lancement d'une passerelle](#)
- [Configuration d'une adresse IP pour la passerelle](#)
- [Configuration de votre passerelle](#)
- [Suppression d'une passerelle de l'appliance matérielle](#)
- [Suppression de votre appliance matérielle](#)

Régions AWS prises en charge

L'appliance matérielle Storage Gateway est disponible pour l'expédition dans le monde entier où elle est légalement autorisée et autorisée à exporter par le gouvernement américain. Pour plus d'informations sur la console prise AWS Régions, voir [Régions de l'appliance matérielle Storage](#) dans le AWS Référence générale.

Configuration de votre appliance matérielle

Après avoir reçu votre appliance matérielle Storage Gateway, vous utilisez la console d'appliance matérielle pour configurer la mise en réseau afin de fournir une connexion permanente à l'AWS et activez votre appareil. L'activation associe votre appliance au AWS compte qui a été utilisé pendant le processus d'activation. Une fois l'appliance activée, vous pouvez lancer une passerelle de fichier, de volume ou de bande à partir de la console Storage Gateway.

Pour installer et configurer votre appliance matérielle

1. Montez sur rack l'appliance et raccordez-la au secteur électrique et au réseau. Pour plus d'informations, consultez [Montage en rack de votre appliance matérielle et connexion à l'alimentation](#).
2. Définissez les adresses Internet Protocol version 4 (IPv4) à la fois pour l'appliance matérielle (l'hôte) et Storage Gateway (le service). Pour plus d'informations, consultez [Configuration des paramètres réseau](#).
3. Activer l'appliance matérielle sur la console Matériel dans la AWS Région de votre choix. Pour plus d'informations, consultez [Activation de votre appliance matérielle](#).
4. Installez Storage Gateway sur votre appliance matérielle. Pour plus d'informations, consultez [Configuration de votre passerelle](#).

La configuration des passerelles sur votre appliance matérielle s'effectue de la même manière que celle des passerelles sur VMware ESXi, Microsoft Hyper-V, KVM (machine virtuelle basée sur le noyau Linux) ou Amazon EC2.

Augmentation du stockage de cache utilisable

Vous pouvez augmenter le stockage utilisable sur l'appliance matérielle de 5 To à 12 To. L'augmentation de la taille du cache permet ainsi un accès à faible latence aux données dans AWS. Si vous avez commandé le modèle 5 To, vous pouvez augmenter le stockage utilisable à 12 To en achetant cinq disques SSD de 1,92 To, disponibles pour commande sur console Matériel. Vous pouvez commander les SSD supplémentaires en suivant le même processus de commande que la commande d'une appliance matérielle et la demande de devis de vente à partir de la console Storage Gateway.

Vous pouvez ensuite les ajouter à l'appliance matérielle avant de l'activer. Si vous avez déjà activé l'appliance matérielle et que vous souhaitez augmenter le stockage utilisable sur l'appliance à 12 To, procédez comme suit :

1. Réinitialisez les paramètres d'usine de l'appliance matérielle. Contacter AWS Support des instructions sur la façon d'effectuer cette opération.
2. Ajoutez cinq SSD de 1,92 To à l'appliance.

Options de carte d'interface réseau

Selon le modèle d'appliance que vous avez commandé, il peut être fourni avec une carte réseau cuivre 10G-Base-T ou une carte réseau DA/SFP+ 10G.

- Configuration de la carte réseau 10G-Base-T :
 - Utiliser des câbles CAT6 pour 10G ou CAT5 (e) pour 1G
- Configuration d'une carte réseau DA/SFP+ 10G :
 - Utiliser des câbles à attache directe en cuivre Twinax jusqu'à 5 mètres
 - Modules optiques SFP+ compatibles Dell/Intel (SR ou LR)
 - Émetteur-récepteur en cuivre SFP/SFP+ pour 1G-Base-T ou 10G-Base-T

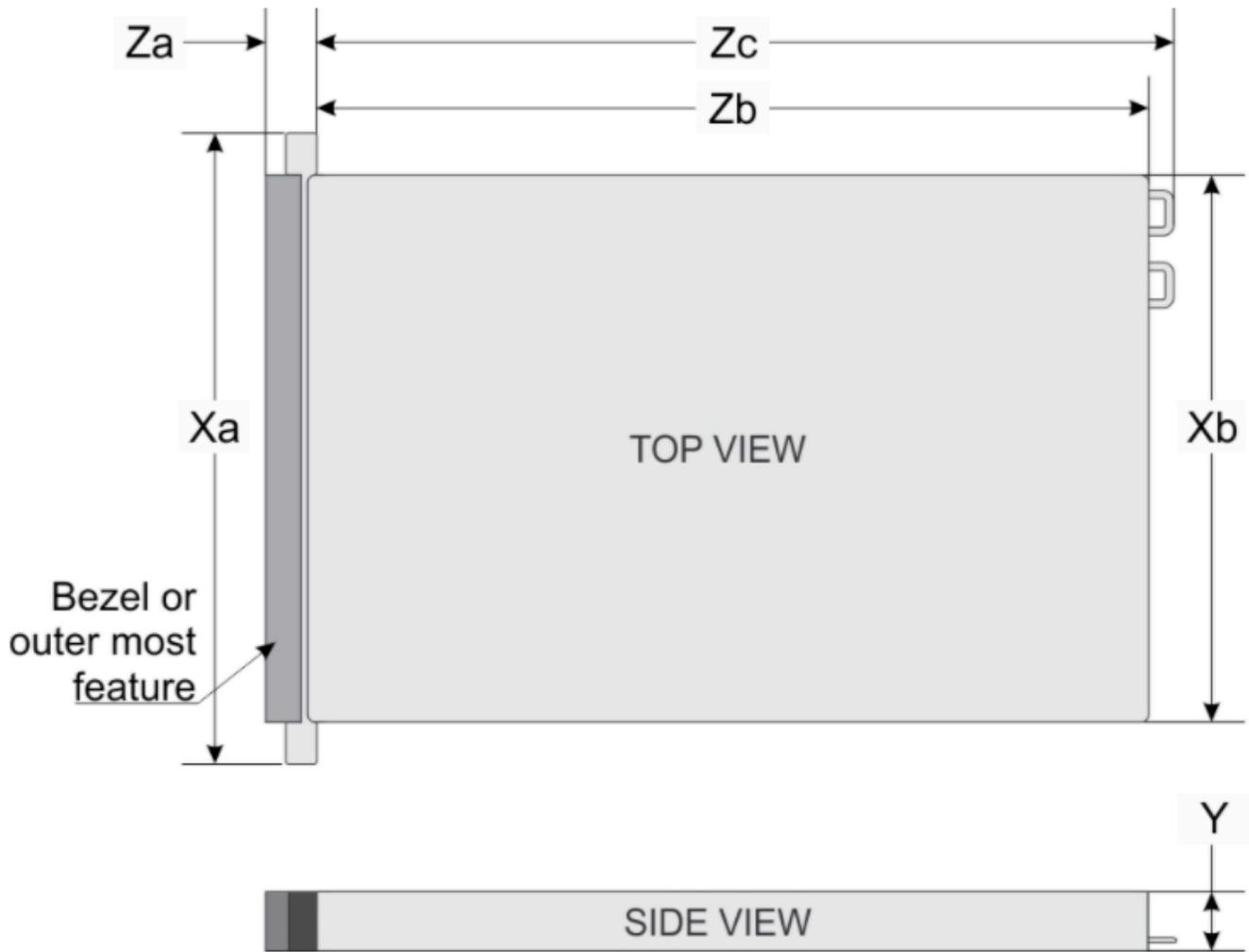
Montage en rack de votre appliance matérielle et connexion à l'alimentation

Après avoir déballé l'appliance matérielle Storage Gateway, suivez les instructions indiquées dans la boîte pour monter sur rack le serveur. Votre appliance est au format 1U et s'intègre dans un rack 19 pouces conforme à la Commission électrotechnique internationale (IEC) standard.

Pour installer l'appliance matérielle, vous devez disposer des éléments indiqués ci-dessous.

- Câble électriques : un obligatoire, deux recommandés.
- Câblage réseau pris en charge (en fonction de la carte d'interface réseau (NIC) incluse dans l'appliance matérielle). Twinax Copper DAC, module optique SFP+ (compatible Intel) ou émetteur-récepteur en cuivre SFP vers Base-T.
- Clavier et moniteur, ou commutateur KVM (clavier/vidéo/souris).

Dimensions de l'appliance matérielle



System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

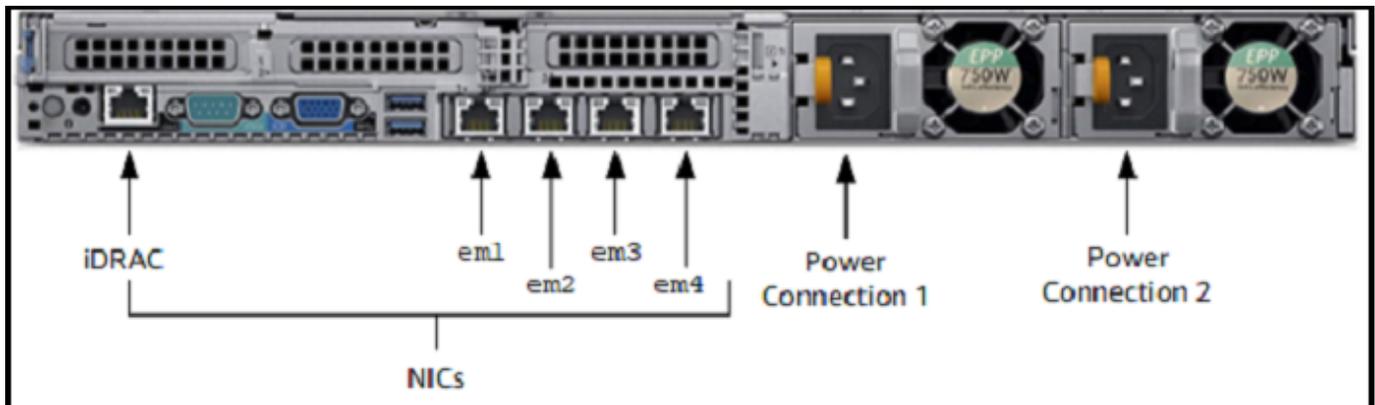
Pour connecter l'appliance matérielle au secteur

Note

Avant d'exécuter la procédure ci-dessous, vérifiez que vous respectez toutes les exigences requises pour l'appliance matérielle Storage Gateway, comme décrit dans la [Exigences en matière de mise en réseau et de pare-feu pour l'appliance matérielle Storage](#).

1. Branchez au secteur chacun des deux blocs d'alimentation. Il est possible d'utiliser un seul connecteur électrique, mais nous vous recommandons d'utiliser les deux.

L'image ci-dessous illustre l'appliance matérielle et ses connecteurs.

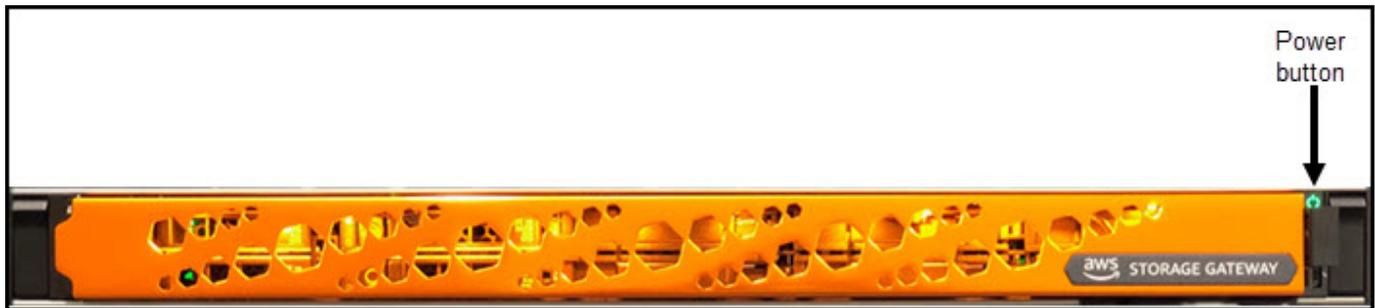


2. Branchez un câble Ethernet dans le port em1 pour obtenir une connexion Internet permanente. Le port em1 est le premier, de gauche à droite, des quatre ports réseau physiques situés à l'arrière.

Note

L'appliance matérielle ne prend pas en charge la jonction VLAN. Configurez le port de commutation auquel vous connectez l'appliance matérielle en tant que port VLAN sans jonction.

3. Branchez le clavier et le moniteur.
4. Mettez le serveur sous tension en appuyant sur le bouton Power (Marche/arrêt) sur le panneau avant, comme l'indique l'image suivante.

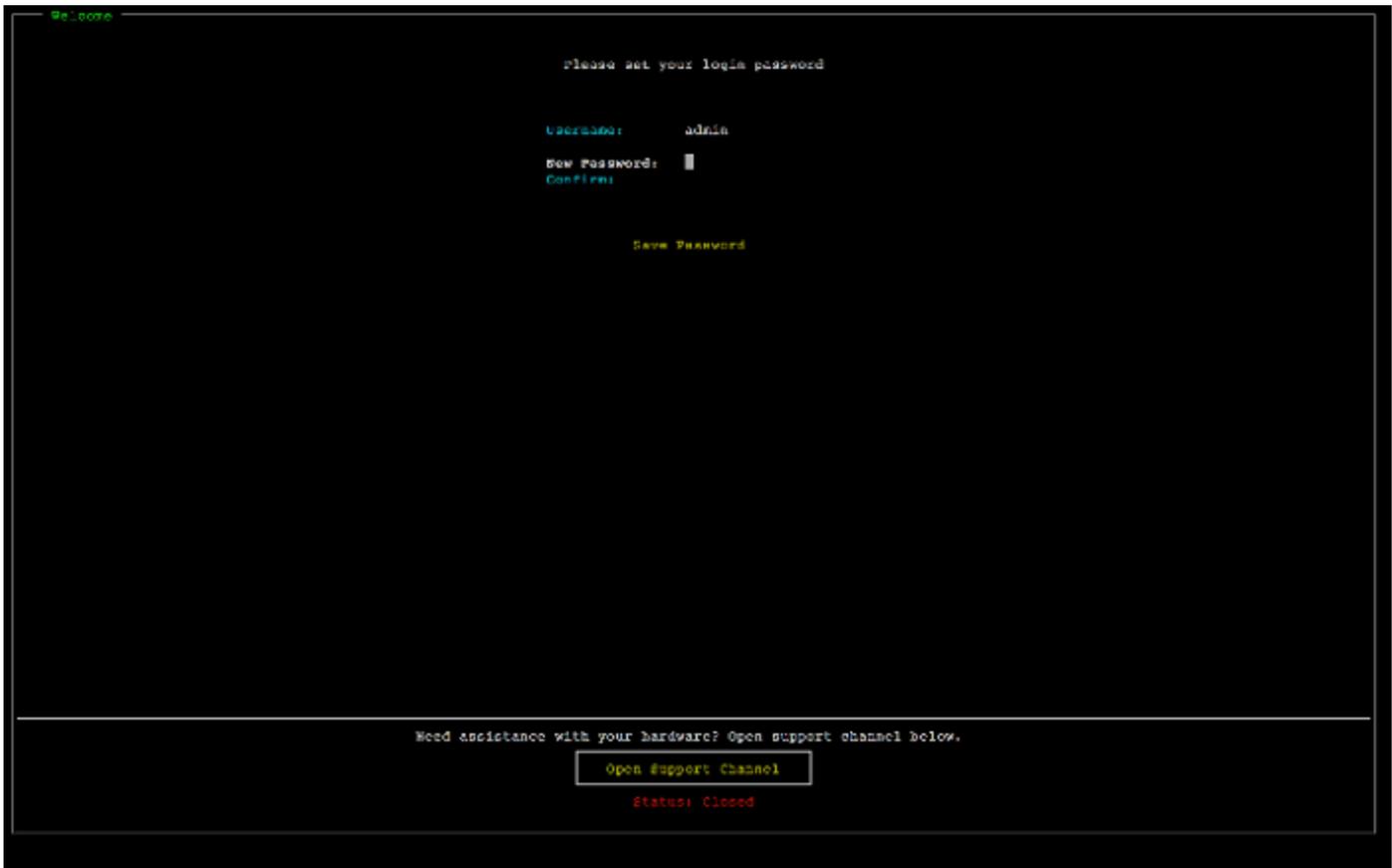


Lorsque le serveur a démarré, la console du matériel apparaît à l'écran. Elle présente une interface utilisateur propre à AWS que vous pouvez utiliser pour configurer les paramètres réseau initiaux. Vous configurez ces paramètres pour connecter la solution matérielle-logicielle à AWS et ouvrez un canal de support technique pour le dépannage par AWS Support.

Pour utiliser la console du matériel, saisissez un texte au clavier et utilisez les touches Up, Down, Right et Left Arrow pour vous déplacer dans l'écran. Utilisez la touche Tab pour passer d'un élément à l'autre sur l'écran. Dans certaines configurations, vous pouvez utiliser la séquence de touches Shift+Tab pour reculer d'un élément à l'autre. Utilisez la touche Enter pour enregistrer les sélections, ou pour choisir un bouton sur l'écran.

Pour définir un mot de passe pour la première fois

1. Pour Set Password (Définir un mot de passe), saisissez un mot de passe, puis appuyez sur Down arrow.
2. Pour Confirm (Confirmer), entrez à nouveau votre mot de passe, puis choisissez Save Password (Enregistrer le mot de passe).



À ce stade, vous vous trouvez dans la console du matériel, comme indiqué ci-dessous.



Étape suivante

[Configuration des paramètres réseau](#)

Configuration des paramètres réseau

Une fois le serveur démarré, vous pouvez saisir votre premier mot de passe dans la console du matériel, comme décrit dans [Montage en rack de votre appliance matérielle et connexion à l'alimentation](#).

Ensuite, sur la console du matériel, procédez comme suit pour configurer les paramètres réseau afin de permettre à votre appliance matérielle de se connecter à AWS.

Pour définir une adresse réseau

1. Choisissez Configure Network (Configurer le réseau) et appuyez sur la touche `Enter`. L'écran Configure Network (Configurer le réseau) illustré ci-dessous s'affiche.



2. Pour Adresse IP, saisissez une adresse IPv4 valide à partir de l'une des sources suivantes :
- Utilisez l'adresse IPv4 attribué par votre serveur DHCP (Dynamic Host Configuration Protocol) à votre port réseau physique.

Notez cette adresse IPv4 pour l'utiliser ultérieurement dans l'étape d'activation.

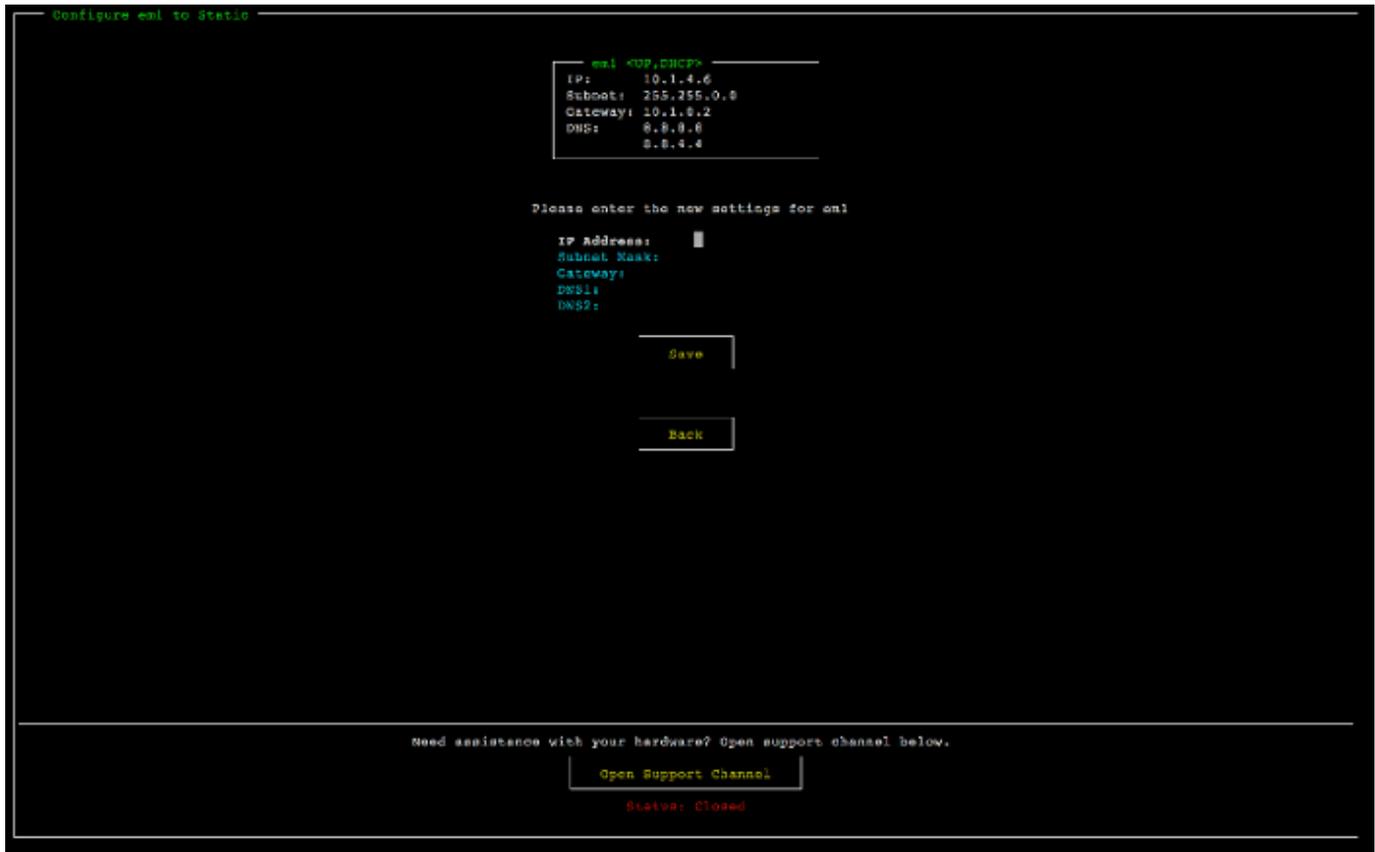
- Attribuez une adresse IPv4 statique. Pour cela, choisissez Static (Statique) dans la section em1 et appuyez sur Enter pour afficher l'écran Configure Static IP (Configurer l'adresse IP statique) illustré ci-dessous.

La section em1 se trouve dans la partie supérieure gauche du groupe des paramètres de ports.

Après avoir entré une adresse IPv4 valide, appuyez sur la touche Down arrow ou Tab.

Note

Si vous configurez une autre interface, elle doit fournir la même connexion permanente à l'AWSpoints de terminaison répertoriés dans les exigences.



3. Pour Subnet (Sous-réseau), entrez un masque de sous-réseau valide, puis appuyez sur Down arrow.
4. Pour Gateway (Passerelle), entrez l'adresse IPv4 de la passerelle réseau et appuyez sur Down arrow.
5. Pour DNS1, entrez l'adresse IPv4 de votre serveur DNS (Domain Name Service), puis appuyez sur Down arrow.
6. (Facultatif) Pour DNS2, entrez une seconde adresse IPv4, puis appuyez sur Down arrow. L'affectation d'un deuxième serveur DNS assure une redondance supplémentaire au cas où le premier serveur DNS devient indisponible.

7. Choisissez Save (Enregistrer), puis appuyez sur Enter pour enregistrer votre adresse IPv4 statique pour l'appliance.

Pour vous déconnecter de la console du matériel

1. Pour revenir à l'écran principal, choisissez Back (Retour).
2. Choisissez Logout (Déconnexion) pour revenir à l'écran Login (Connexion).

Étape suivante

[Activation de votre appliance matérielle](#)

Activation de votre appliance matérielle

Après avoir configuré votre adresse IP, vous devez la saisir dans la page Hardware (Matériel) de la console, comme décrit ci-après. Le processus d'activation vérifie que votre appliance matérielle comporte les informations d'identification de sécurité appropriées et enregistre l'appliance dans votreAWS.

Vous pouvez choisir d'activer votre appliance matérielle dans l'une des options prises en charge.AWSRégions. Pour obtenir une liste desAWSRégions, voir[Régions de l'appliance matérielle Storage](#) dans leAWSRéférence générale.

Pour activer votre appliance pour la première fois ou dans uneAWSRégion dans laquelle aucune passerelle n'a été déployée

1. Connectez-vous à la consoleAWS Management Consoleet ouvrez la console Storage Gateway sur[AWS Storage GatewayManagement Console](#)avec les informations d'identification de compte à utiliser pour activer votre matériel.

S'il s'agit de votre première passerelle dans unAWSRégion, un écran d'accueil apparaît. Après avoir créé une passerelle dans cetteAWSRégion, l'écran ne s'affiche plus.

Note

Pour l'activation uniquement, les conditions suivantes doivent être remplies :

- Votre navigateur doit être sur le même réseau que votre appliance matérielle.

- Votre pare-feu doit autoriser l'accès HTTP sur le port 8080 à l'appliance pour le trafic entrant.

2. Choisissez Mise en route pour afficher l'assistant Créer une passerelle, puis choisissez Appliance matérielle dans la page Sélectionner la plateforme hôte, comme illustré ci-après.
3. Choisissez Suivant pour afficher l'écran Connect to hardware (Se connecter au matériel) illustré ci-après.
4. Pour Adresse IP dans le Connect à l'appliance matérielle, entrez l'adresse IPv4 de votre appliance et choisissez ensuite une Connexion Pour accéder à l'écran Activer le matériel illustré ci-après.
5. Pour Hardware name (Nom du matériel), saisissez un nom pour votre appliance. Les noms peuvent comporter jusqu'à 255 caractères. La barre oblique n'est pas autorisée.
6. Pour Fuseau horaire du matériel, indiquez les paramètres régionaux.

Le fuseau horaire commande le moment où les mises à jour du matériel sont effectuées, soit à 2h00, heure locale.

 Note

Nous vous recommandons de définir le fuseau horaire de votre appliance afin de déterminer une heure de mise à jour standard en dehors des heures ouvrées habituelles.

7. (Facultatif) Laissez RAID Volume Manager (Gestionnaire de volumes RAID) défini sur ZFS.

ZFS est utilisé comme gestionnaire de volumes RAID sur l'appliance matérielle pour offrir de meilleures performances et une protection des données. ZFS, à la fois système de fichiers et gestionnaire de volumes logiques, est open source et de type logiciel. L'appliance matérielle est optimisée spécialement pour ZFS RAID. Pour en savoir plus sur ZFS RAID, consultez la page Wikipedia [ZFS](#).

8. Choisissez Next (Suivant) pour terminer l'activation.

Une bannière de console s'affiche sur la page Matériel, indiquant que l'appliance matérielle a été correctement activée, comme illustré ci-après.

À ce stade, l'appliance est associée à votre compte. L'étape suivante consiste à lancer un fichier, une bande, ou une passerelle de volume mise en cache sur votre appliance.

Storage Gateway

Gateways

File shares

Volumes

Tapes

Hardware

Successfully activated hardware appliance.
Next step is to launch a gateway by selecting the hardware appliance and choosing 'Launch Gateway' from the Actions menu.

Order appliance Quotes and orders Activate appliance Actions

Filter by hardware appliance name, ID or launched gateway type.

<input type="checkbox"/>	Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
<input checked="" type="checkbox"/>	praksuji-bh	vi5loueix9yotyn5	Dell PowerEdge R640	-
<input type="checkbox"/>	praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Details

Name	praksuji-bh	Vendor	Dell
ID	vi5loueix9yotyn5	Model	Dell PowerEdge R640
Time Zone	GMT	Serial Number	5Q8Y0M2
		RAID Volume Manager	ZFS

Étape suivante

[Lancement d'une passerelle](#)

Lancement d'une passerelle

Vous pouvez lancer n'importe laquelle des trois passerelles de stockage sur l'appliance : passerelle de fichiers, passerelle de volume (mise en cache) ou passerelle de bande.

Pour lancer une passerelle sur votre appliance matérielle

1. Connectez-vous à la console AWS Management Console et ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Hardware (Matériel).
3. Pour Actions, choisissez Launch Gateway (Lancer une passerelle).
4. Pour Gateway Type (Type de passerelle), choisissez File Gateway (Passerelle de fichiers), Tape Gateway (Passerelle de bande) ou Volume Gateway (Cached) (Passerelle de volume (Mise en cache)).
5. Pour Gateway name (Nom de la passerelle), saisissez le nom de votre passerelle. Ce nom peut comporter jusqu'à 255 caractères. La barre oblique n'est pas autorisée.
6. Choisissez Launch gateway (Lancer une passerelle).

Le logiciel Storage Gateway correspondant au type de passerelle choisie s'installe sur l'appliance. L'apparition d'une passerelle peut prendre jusqu'à 5 à 10 minutes en ligne dans la console.

Pour attribuer une adresse IP statique à votre passerelle installée, vous devez ensuite configurer ses interfaces réseau afin que vos applications puissent l'utiliser.

Étape suivante

[Configuration d'une adresse IP pour la passerelle](#)

Configuration d'une adresse IP pour la passerelle

Avant d'activer votre appliance matérielle, vous avez attribué une adresse IP à son interface réseau physique. Maintenant que vous avez activé l'appliance et lancé votre Storage Gateway dessus, vous devez attribuer une autre adresse IP à la machine virtuelle Storage Gateway qui s'exécute sur l'appliance matérielle. Pour attribuer une adresse IP statique à une passerelle installée sur votre appliance matérielle, configurez l'adresse IP à partir de la console locale de cette passerelle. Vos applications (client NFS ou SMB, initiateur iSCSI, etc.) se connectent à cette adresse IP. Vous pouvez accéder à la console locale de la passerelle à partir de la console de l'appliance matérielle.

Pour configurer l'adresse IP de la passerelle sur votre appliance pour utiliser des applications

1. Sur la console du matériel, choisissez Open Service Console (Ouvrir la console du service) pour ouvrir un écran de connexion à la console locale de la passerelle.
2. Entrez le mot de passe de connexion à l'hôte local et appuyez sur `Enter`.

Le compte par défaut est `admin` et le mot de passe par défaut est `password`.

3. Changez le mot de passe par défaut. Choisissez Actions, Set Local Password (Définir le mot de passe local) et entrez vos nouvelles informations d'identification dans la boîte de dialogue Set Local Password (Définir le mot de passe local).
4. (Facultatif) Configurez vos paramètres de proxy. Pour obtenir des instructions, consultez [Montage en rack de votre appliance matérielle et connexion à l'alimentation](#).
5. Accédez à la page Network Settings (Paramètres réseau) de la console locale de la passerelle, comme illustré ci-après.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

6. Tapez 2 pour accéder à la page Network Configuration (Configuration du réseau) illustrée ci-après.

```
AWS Storage Gateway Network Configuration

1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: View DNS Configuration
7: View Routes

Press "x" to exit

Enter command: _
```

7. Configurez une adresse IP statique ou DHCP pour le port réseau sur votre appliance matérielle pour fournir une passerelle de fichiers, de volume et de bande pour les applications. Cette adresse IP doit se trouver sur le même sous-réseau que l'adresse IP utilisée pendant l'activation de l'appliance matérielle.

Pour quitter la console locale de la passerelle

- Appuyez sur la séquence de touches `CrtI+] (crochet fermant)`. La console du matériel s'affiche.

Note

La console locale de la passerelle ne peut être fermée qu'en utilisant la séquence de touches indiquée ci-dessus.

Étape suivante

[Configuration de votre passerelle](#)

Configuration de votre passerelle

Une fois que votre appliance matérielle est activée et configurée, votre appliance s'affiche dans la console. Vous pouvez maintenant créer le type de passerelle que vous voulez. Poursuivez l'installation de votre type de passerelle. Pour obtenir des instructions, consultez [Configurer votre passerelle de fichiers Amazon S3](#).

Suppression d'une passerelle de l'appliance matérielle

Pour supprimer un logiciel de passerelle de votre appliance matérielle, utilisez la procédure suivante. Le logiciel de passerelle est alors désinstallé de votre appliance matérielle.

Pour supprimer une passerelle d'une appliance matérielle

1. Cochez la case correspondant à la passerelle.
2. Pour Actions, choisissez Remove Gateway (Supprimer une passerelle).
3. Dans la boîte de dialogue Remove gateway from hardware appliance (Supprimer une passerelle de l'appliance matérielle), choisissez Confirm (Confirmer).

Note

Lorsque vous avez supprimé une passerelle, vous ne pouvez pas annuler sa suppression. Pour certains types de passerelles, vous pouvez perdre des données lors de la suppression, notamment les données mises en cache. Pour plus d'informations sur la suppression d'une passerelle, consultez [Suppression de votre passerelle à l'aide de la Console AWS Storage Gateway et suppression des ressources associées](#).

La suppression d'une passerelle ne supprime pas l'appliance matérielle de la console. L'appliance matérielle reste pour les futurs déploiements de passerelles.

Suppression de votre appliance matérielle

Une fois que vous avez activé votre appliance matérielle dans votreAWS, il est possible que vous ayez besoin de le déplacer et de l'activer dans un autreAWS. Dans ce cas, vous devez d'abord supprimer l'appliance à partir deAWS et activez-le dans un autreAWS. Vous pouvez également avoir besoin de supprimer l'appliance complètement de votreAWS car vous n'en avez plus besoin. Suivez les instructions ci-après pour supprimer votre appliance matérielle.

Pour supprimer votre appliance matérielle

1. Si vous avez installé une passerelle sur l'appliance matérielle, vous devez d'abord supprimer cette dernière avant de pouvoir supprimer l'appliance. Pour obtenir des instructions sur la suppression d'une passerelle de votre appliance matérielle, consultez [Suppression d'une passerelle de l'appliance matérielle](#).
2. Sur la page Matériel, choisissez l'appliance matérielle que vous souhaitez supprimer.
3. Pour Actions, choisissez Delete Appliance (Supprimer l'appliance).
4. Dans la boîte de dialogue Confirm deletion of resource(s) (Confirmer la suppression de la ou des ressources), activez la case à cocher de confirmation et choisissez Supprimer. Un message indiquant la réussite de la suppression s'affiche.

Lorsque vous supprimez l'appliance matérielle, toutes les ressources associées à la passerelle qui est installée sur l'appliance sont également supprimées, mais les données de l'appliance matérielle ne sont pas supprimées.

Démarrer avec AWS Storage Gateway

Dans cette section, vous trouverez des instructions sur le téléchargement et l'activation d'une passerelle de fichiers dans AWS Storage Gateway. Avant de commencer, assurez-vous que votre configuration répond aux conditions préalables requises et aux autres exigences décrites dans [Configuration pour Amazon S3 File Gateway](#).

Rubriques

- [Créer et activer une passerelle de fichiers Amazon S3](#)

Créer et activer une passerelle de fichiers Amazon S3

Dans cette section, vous trouverez des instructions sur le téléchargement, le déploiement et l'activation d'une passerelle de fichiers dans AWS Storage Gateway.

Rubriques

- [Configuration d'une passerelle de fichiers Amazon S3](#)
- [Connect votre passerelle de fichiers Amazon S3 à AWS](#)
- [Vérifiez les paramètres et activez votre passerelle de fichiers Amazon S3](#)
- [Configurer votre passerelle de fichiers Amazon S3](#)

Configuration d'une passerelle de fichiers Amazon S3

Pour configurer une nouvelle passerelle de fichiers S3

1. Ouverture d'AWS Management Console à <https://console.aws.amazon.com/storagegateway/home/>, et choisissez la Région AWS où vous voulez créer votre passerelle.
2. Choisissez Créez une passerelle pour ouvrir Configuration de passerelle.
3. Dans Paramètres de passerelle, procédez comme suit :
 - a. Pour Gateway name (Nom de la passerelle), saisissez le nom de votre passerelle. Une fois votre passerelle créée, vous pouvez rechercher ce nom pour trouver votre passerelle sur les pages de liste du AWS Storage Gateway console
 - b. Pour Fuseau horaire de la, choisissez le fuseau horaire local de la partie du monde où vous souhaitez déployer votre passerelle.

4. Dans Options de passerelle Section, pour Type de passerelle, choisissez Passerelle de fichiers Amazon S3.
5. Dans Options de plateforme, procédez comme suit :
 - a. Pour Plateforme hôte, choisissez la plateforme sur laquelle vous souhaitez déployer votre passerelle. Suivez ensuite les instructions spécifiques à la plateforme affichées sur la page de la console Storage Gateway pour configurer votre plateforme hôte. Choisissez parmi les options suivantes :
 - VMware ESXi— Téléchargez, déployez et configurez la machine virtuelle de passerelle à l'aide de VMware ESXi.
 - Microsoft Hyper-V— Téléchargez, déployez et configurez la machine virtuelle de passerelle à l'aide de Microsoft Hyper-V.
 - KVM Linux— Téléchargez, déployez et configurez la machine virtuelle passerelle à l'aide de la machine virtuelle basée sur le noyau Linux (KVM).
 - Amazon EC2— Configurez et lancez une instance Amazon EC2 pour héberger votre passerelle.
 - Appliance matérielle— Commandez une appliance matérielle physique dédiée auprès de AWS pour héberger votre passerelle.
 - b. Pour Confirmer la configuration de passerelle, activez la case à cocher afin de confirmer que vous avez effectué les étapes de déploiement pour la plate-forme hôte que vous avez choisie. Cette étape n'est pas applicable pour le Appliance matérielle plateforme hôte.
6. Maintenant que votre passerelle est configurée, vous devez choisir la façon dont vous souhaitez qu'elle se connecte et communique avec AWS. Choisissez Suivant pour poursuivre.

Connect votre passerelle de fichiers Amazon S3 à AWS

Pour connecter une nouvelle passerelle de fichiers S3 à AWS

1. Si vous ne l'avez pas déjà fait, suivez la procédure décrite dans [Configuration d'une passerelle de fichiers Amazon S3](#). Lorsque vous avez terminé, choisissez Suivant pour ouvrir Connexion à AWS Page d'AWS Storage Gateway console
2. Dans Options de point de terminaison Section, pour Point de terminaison de service, choisissez le type de point de terminaison avec lequel votre passerelle utilisera pour communiquer avec AWS. Choisissez parmi les options suivantes :

- **Accessible publiquement**— Votre passerelle communique avec AWS sur l'Internet public. Si vous sélectionnez cette option, utilisez le Point de terminaison compatible FIPS pour spécifier si la connexion doit être conforme aux normes FIPS (Federal Information Processing Standards).

 Note

Si vous avez besoin de modules cryptographiques validés FIPS 140-2 lorsque vous accédez à AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison compatible FIPS. Pour plus d'informations, consultez [Federal Information Processing Standard \(FIPS\) 140-2](#).

Le point de terminaison du service FIPS n'est disponible que dans certains AWS Régions. Pour de plus amples informations, veuillez consulter [AWS Storage Gateway Points de terminaison et quotas](#) dans le AWS Référence générale.

- **VPC hébergé**— Votre passerelle communique avec AWS via une connexion privée avec votre virtual private cloud (VPC), vous permettant de contrôler vos paramètres réseau. Si vous sélectionnez cette option, vous devez spécifier un point de terminaison VPC existant en choisissant son ID de point de terminaison VPC dans la liste déroulante. Vous pouvez également fournir son nom VPC système DNS (Domain Name System) ou son adresse IP.
3. Dans Options de connexion de passerelle Section, pour Options de connexion, choisissez comment identifier votre passerelle vers AWS. Choisissez parmi les options suivantes :
- **Adresse IP**— Indiquez l'adresse IP de votre passerelle dans le champ correspondant. Cette adresse IP doit être publique ou accessible depuis votre réseau actuel, et vous devez pouvoir vous y connecter depuis votre navigateur Web.
- Vous pouvez obtenir l'adresse IP de la passerelle en vous connectant à la console locale de la passerelle à partir de votre client hyperviseur, ou en la copiant à partir de la page de détails de votre instance Amazon EC2.
- **Clé d'activation**: indiquez la clé d'activation de votre passerelle dans le champ correspondant. Vous pouvez générer une clé d'activation à l'aide de la console locale de la passerelle. Si l'adresse IP de votre passerelle n'est pas disponible, choisissez cette option.
4. Maintenant que vous avez choisi comment vous souhaitez que votre passerelle se connecte à AWS, vous devez activer la passerelle. Choisissez Suivant pour poursuivre.

Vérifiez les paramètres et activez votre passerelle de fichiers Amazon S3

Pour activer une nouvelle passerelle de fichiers S3

1. Si vous ne l'avez pas déjà fait, suivez les procédures décrites dans les rubriques suivantes :
 - [Configuration d'une passerelle de fichiers Amazon S3](#)
 - [Connect votre passerelle de fichiers Amazon S3 àAWS](#)

Lorsque vous avez terminé, choisissezSuivantpour ouvrirVérifiez et activezPage d'AWS Storage Gatewayconsole

2. Consultez les détails initiaux de la passerelle pour chaque section de la page.
3. Si une section contient des erreurs, choisissezModifierpour revenir à la page des paramètres correspondante et apporter des modifications.

Important

Vous ne pouvez pas modifier les options de la passerelle ou les paramètres de connexion une fois la passerelle activée.

4. Maintenant que vous avez activé votre passerelle, vous devez effectuer la première configuration pour allouer des disques de stockage locaux et configurer la journalisation. ChoisissezSuivantpour poursuivre.

Configurer votre passerelle de fichiers Amazon S3

Pour effectuer la première configuration sur une nouvelle passerelle de fichiers S3

1. Si vous ne l'avez pas déjà fait, suivez les procédures décrites dans les rubriques suivantes :
 - [Configuration d'une passerelle de fichiers Amazon S3](#)
 - [Connect votre passerelle de fichiers Amazon S3 àAWS](#)
 - [Vérifiez les paramètres et activez votre passerelle de fichiers Amazon S3](#)

Lorsque vous avez terminé, choisissezSuivantpour ouvrirConfigurer la passePage d'AWS Storage Gatewayconsole

2. Dans **Configurer le stockage de cache**, utilisez les listes déroulantes pour allouer au moins un disque local ayant une capacité d'au moins 150 gibioctets (GiB) à **Cache**. Les disques locaux répertoriés dans cette section correspondent au stockage physique que vous avez provisionné sur votre plateforme hôte.
3. Dans **Groupe de journaux CloudWatch**, choisissez comment configurer Amazon CloudWatch Logs pour surveiller l'état de santé de votre passerelle. Choisissez parmi les options suivantes :
 - **Création d'un nouveau groupe de journaux**— Configurez un nouveau groupe de journaux pour surveiller votre passerelle.
 - **Utiliser un groupe de journaux existant**— Choisissez un groupe de journaux existant dans la liste déroulante correspondante.
 - **Désactiver la journalisation**— N'utilisez pas Amazon CloudWatch Logs pour surveiller votre passerelle.
4. Dans **Alarmes CloudWatch**, choisissez comment configurer les alarmes Amazon CloudWatch pour vous avertir lorsque les mesures de votre passerelle s'écartent des limites définies. Choisissez parmi les options suivantes :
 - **Désactive les alarmes**— N'utilisez pas d'alarmes CloudWatch pour être averti des mesures de votre passerelle.
 - **Création d'une alarme CloudWatch personnalisée**— Configurez une nouvelle alarme CloudWatch pour être avertie des mesures de votre passerelle. Choisissez **Créez une alarme** pour définir des mesures et spécifier des actions d'alarme dans la console Amazon CloudWatch. Pour obtenir des instructions, consultez [Utilisation des alarmes Amazon CloudWatch](#) dans le Guide de l'utilisateur Amazon CloudWatch..
5. (Facultatif) Dans le **Balises** Section, choisissez **Ajouter un nouveau tag**, puis entrez une paire clé-valeur sensible à la casse pour vous aider à rechercher et filtrer votre passerelle sur les pages de liste dans le **AWS Storage Gateway** console Répétez cette étape pour ajouter autant de balises que vous voulez.
6. (Facultatif) Dans le **Vérifier la configuration de la haute disponibilité de VMware**, si votre passerelle est déployée sur un hôte VMware dans le cadre d'un cluster activé pour VMware High Availability (HA), choisissez **Vérifiez VMware HA** pour vérifier si la configuration HA fonctionne correctement.

 Note

Cette section s'affiche uniquement pour les passerelles exécutées sur la plateforme hôte VMware.

Cette étape n'est pas nécessaire pour terminer le processus de configuration de la passerelle. Vous pouvez tester la configuration HA de votre passerelle à tout moment. La vérification prend quelques minutes et redémarre la machine virtuelle (VM) Storage Gateway.

7. Choisissez `Configuration` pour finaliser la création de votre passerelle.

Pour vérifier l'état de votre nouvelle passerelle, recherchez-la sur la page `Passerelles` de la `AWS Storage Gateway` console

Maintenant que vous avez créé votre passerelle, vous devez créer un partage de fichiers pour qu'elle puisse l'utiliser. Pour obtenir des instructions, consultez [Création d'un partage de fichiers](#).

Création d'un partage de fichiers

Dans cette section, vous trouverez des instructions sur la création d'un partage de fichiers. Vous pouvez créer un partage de fichiers accessible via le protocole Network File System (NFS) ou Server Message Block (SMB).

Note

Lorsqu'un fichier est écrit sur la passerelle de fichiers par un client NFS ou SMB, la passerelle de fichiers télécharge les données du fichier vers Amazon S3 suivies de ses métadonnées (propriétaires, horodatages, etc.). Le téléchargement des données du fichier crée un objet S3, et le téléchargement des métadonnées du fichier met à jour les métadonnées de l'objet S3. Ce processus crée une autre version de l'objet, entraînant deux versions d'un objet. Si la gestion des versions S3 est activée, les deux versions sont stockées.

Si vous modifiez les métadonnées d'un fichier stocké dans votre passerelle de fichiers, un nouvel objet S3 est créé et remplace l'objet S3 existant. Ce comportement est différent de la modification d'un fichier dans un système de fichiers, où la modification d'un fichier n'entraîne pas la création d'un nouveau fichier. Testez toutes les opérations de fichiers que vous envisagez d'utiliser avec AWSStorage Gateway pour que vous compreniez comment chaque opération de fichier interagit avec le stockage Amazon S3.

Pensez attentivement à l'utilisation du versionnement S3 et de la réplication entre régions (CRR) dans Amazon S3 lorsque vous téléchargez des données depuis votre passerelle de fichiers. Le téléchargement de fichiers depuis votre passerelle de fichiers vers Amazon S3 lorsque le versionnement S3 est activé entraîne au moins deux versions d'un objet S3. Certains flux de travail impliquant des fichiers volumineux et des modèles d'écriture de fichiers, tels que les chargements de fichiers effectués en plusieurs étapes, peuvent augmenter le nombre de versions d'objets S3 stockés. Si le cache de la passerelle de fichiers doit libérer de l'espace en raison des taux d'écriture de fichiers élevés, plusieurs versions d'objets S3 peuvent être créées. Ces scénarios augmentent le stockage S3 si le versionnement S3 est activé et augmentent les coûts de transfert associés au CRR. Testez toutes les opérations de fichiers que vous envisagez d'utiliser avec Storage Gateway afin de comprendre comment chaque opération de fichier interagit avec le stockage Amazon S3. L'utilisation de l'utilitaire Rsync avec votre passerelle de fichiers entraîne la création de fichiers temporaires dans le cache et la création d'objets S3 temporaires dans Amazon S3. Cette situation entraîne des frais de suppression précoce dans les classes de stockage S3

standard peu fréquent (S3 standard — Accès peu fréquent) et S3 Intelligent-Tiering (Accès peu fréquent).

Lorsque vous créez un partage NFS, par défaut, toute personne pouvant accéder au serveur NFS peut accéder au partage de fichiers NFS. Vous pouvez limiter l'accès aux clients par l'adresse IP.

Pour SMB, vous pouvez utiliser un des trois modes d'authentification différents :

- Un partage de fichiers avec un accès Microsoft Active Directory (AD). Tout utilisateur Microsoft AD authentifié a accès à ce type de partage de fichiers.
- Un partage de fichiers SMB avec un accès limité. Seuls les utilisateurs et groupes du domaine que vous spécifiez disposent des autorisations d'accès (via une liste d'autorisation). Les utilisateurs et les groupes peuvent également se voir refuser l'accès (via une liste de refus).
- Un partage de fichiers SMB avec un accès invité. Tout utilisateur pouvant fournir le mot de passe invité a accès à ce partage de fichiers.

Note

Les partages de fichiers exportés via la passerelle pour les partages de fichiers NFS prennent en charge les autorisations POSIX. Pour les partages de fichiers SMB, vous pouvez utiliser les listes de contrôle d'accès (ACL) pour gérer les autorisations sur les fichiers et les dossiers de votre partage de fichiers. Pour plus d'informations, consultez [Utilisation des listes ACL Microsoft Windows pour contrôler l'accès à un partage de fichiers SMB](#).

Une passerelle de fichiers peut héberger un ou plusieurs partages de fichiers de types différents. Vous pouvez avoir plusieurs partages de fichiers NFS et SMB sur une passerelle de fichiers.

Important

Pour créer un partage de fichiers, une passerelle de fichiers a besoin que vous activiez AWS Security Token Service (AWS STS). Vérifiez les éléments suivants : AWS STS est activé dans la Région AWS dans laquelle vous créez votre passerelle de fichiers. Si AWS STS n'est pas activé dans cette Région AWS, activez-le. Pour obtenir des informations sur la façon

d'activer AWS STS, voir [Activation et désactivation AWS STS dans un Région AWS](#) dans le AWS Identity and Access Management Guide de l'utilisateur.

Note

Vous pouvez utiliser AWS Key Management Service (AWS KMS) pour chiffrer les objets que votre passerelle de fichiers stocke dans Amazon S3. Pour ce faire à l'aide de la console Storage Gateway, consultez [Création d'un partage de fichiers NFS](#) ou [Création d'un partage de fichiers SMB](#). Vous pouvez également effectuer cette opération à l'aide de l'API Storage Gateway. Pour obtenir des instructions, consultez [Create NFS File Share](#) ou [Create SMB File Share](#) dans le AWS Référence de Storage Gateway.

Par défaut, une passerelle de fichiers utilise le chiffrement côté serveur géré avec Amazon S3 (SSE-S3) lorsqu'elle écrit des données dans un compartiment S3. Si vous effectuez un chiffrement côté serveur avec AWS KMS—managed keys) le chiffrement par défaut pour votre compartiment S3, les objets stockés dans celui-ci par une passerelle de fichiers sont chiffrés à l'aide de SSE-KMS.

Pour chiffrer à l'aide de SSE-KMS avec votre propre clé AWS KMS, vous devez activer le chiffrement SSE-KMS. Lorsque vous effectuez cette opération, fournissez l'Amazon Resource Name (ARN) de la clé KMS lorsque vous créez votre partage de fichiers. Vous pouvez également mettre à jour les paramètres KMS pour votre partage de fichiers à l'aide de l'opération d'API [Update NFS File Share](#) ou [Update SMB File Share](#). Cette mise à jour s'applique aux objets stockés dans les compartiments Amazon S3 après la mise à jour.

Si vous configurez votre passerelle de fichiers pour qu'elle utilise SSE-KMS pour le chiffrement, vous devez ajouter manuellement `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt`, `kms:GenerateDataKey`, et `kms:DescribeKey` autorisations sur le rôle IAM associé au partage de fichiers. Pour de plus amples informations, veuillez consulter [Utilisation des stratégies basées sur l'identité \(stratégies IAM\) pour Storage Gateway](#).

Rubriques

- [Création d'un partage de fichiers NFS](#)
- [Création d'un partage de fichiers SMB](#)

Création d'un partage de fichiers NFS

Utilisez la procédure suivante pour créer un partage de fichiers NFS (Network File System).

Note

Lorsqu'un fichier est écrit sur la passerelle de fichiers par un client NFS, la passerelle de fichiers télécharge les données du fichier vers Amazon S3 suivies de ses métadonnées (propriétaires, horodatages, etc.). Le téléchargement des données du fichier crée un objet S3, et le téléchargement des métadonnées du fichier met à jour les métadonnées de l'objet S3. Ce processus crée une autre version de l'objet, entraînant deux versions d'un objet. Si la gestion des versions S3 est activée, les deux versions sont stockées.

Si vous modifiez les métadonnées d'un fichier stocké dans votre passerelle de fichiers, un nouvel objet S3 est créé et remplace l'objet S3 existant. Ce comportement est différent de la modification d'un fichier dans un système de fichiers, où la modification d'un fichier n'entraîne pas la création d'un nouveau fichier. Testez toutes les opérations de fichiers que vous envisagez d'utiliser avec AWSStorage Gateway pour que vous compreniez comment chaque opération de fichier interagit avec le stockage Amazon S3.

Pensez attentivement à l'utilisation du versionnement S3 et de la réplication entre régions (CRR) dans Amazon S3 lorsque vous téléchargez des données depuis votre passerelle de fichiers. Le téléchargement de fichiers depuis votre passerelle de fichiers vers Amazon S3 lorsque le versionnement S3 est activé entraîne au moins deux versions d'un objet S3. Certains flux de travail impliquant des fichiers volumineux et des modèles d'écriture de fichiers, tels que les chargements de fichiers effectués en plusieurs étapes, peuvent augmenter le nombre de versions d'objets S3 stockés. Si le cache de la passerelle de fichiers doit libérer de l'espace en raison des taux d'écriture de fichiers élevés, plusieurs versions d'objets S3 peuvent être créées. Ces scénarios augmentent le stockage S3 si le versionnement S3 est activé et augmentent les coûts de transfert associés au CRR. Testez toutes les opérations de fichiers que vous envisagez d'utiliser avec Storage Gateway afin de comprendre comment chaque opération de fichier interagit avec le stockage Amazon S3. L'utilisation de l'utilitaire Rsync avec votre passerelle de fichiers entraîne la création de fichiers temporaires dans le cache et la création d'objets S3 temporaires dans Amazon S3. Cette situation entraîne des frais de suppression précoce dans les classes de stockage S3 standard peu fréquent (S3 standard — Accès peu fréquent) et S3 Intelligent-Tiering (Accès peu fréquent).

Pour créer un partage de fichiers NFS

1. Ouverture d'AWSStorage Gateway sur <https://console.aws.amazon.com/storagegateway/home/>.
2. ChoisissezCréation d'un partage de fichierspour ouvrir l'Paramètres de partage de fichiers.
3. PourPasserelle, choisissez votre Amazon S3 File Gateway (Passerelle de fichiers) dans la liste.
4. PourEmplacement Amazon S3, effectuez l'une des actions suivantes :
 - Pour connecter le partage de fichiers directement à un compartiment S3, choisissezNom du compartiment S3, puis entrez le nom du compartiment S3 et, éventuellement, un nom de préfixe pour les objets créés par le partage de fichiers. Votre passerelle utilise ce compartiment pour stocker et récupérer des fichiers. Pour plus d'informations sur la création d'un nouveau compartiment, consultez [Comment créer un compartiment S3 ?](#) dans leGuide de l'utilisateur Amazon S3.
 - Pour connecter le partage de fichiers à un compartiment S3 via un point d'accès, choisissezPoint d'accès S3, puis entrez le nom du point d'accès S3 et, éventuellement, un nom de préfixe pour les objets créés par le partage de fichiers. Votre stratégie de compartiment doit être configurée pour déléguer le contrôle d'accès au point d'accès. Pour plus d'informations sur les points d'accès, consultez [Gestion de l'accès aux données avec les points d'accès Amazon S3](#) et [Délégation du contrôle d'accès aux points d'accès](#) dans leGuide de l'utilisateur Amazon S3.
 - Pour connecter le partage de fichiers à un compartiment S3 via un alias de point d'accès, choisissezAlias de points d'accès S3, puis entrez le nom de l'alias du point d'accès S3 et, éventuellement, un nom de préfixe pour les objets créés par le partage de fichiers. Si vous choisissez cette option, la passerelle de fichiers ne peut pas créer de nouveauAWS Identity and Access Management(IAM) stratégie d'accès et de rôle en votre nom. Vous devez sélectionner un rôle IAM existant et configurer une stratégie d'accès dans leAccès à votre compartiment S3section qui suit. Pour de plus amples informations sur les alias des points d'accès, consultez [Utilisation d'un alias de type compartiment pour votre point d'accès](#) dans leGuide de l'utilisateur Amazon S3.

Note

- Si vous entrez un nom de préfixe ou si vous choisissez de vous connecter via un point d'accès ou un alias de point d'accès, vous devez entrer un nom de partage de fichiers.
- Le nom du préfixe doit se terminer par une barre oblique (/).

- Une fois le partage de fichiers créé, le nom du préfixe ne peut pas être modifié ni supprimé.
- Pour plus d'informations sur l'utilisation des noms de préfixes, consultez [Organisation des objets à l'aide de préfixes](#) dans le Guide de l'utilisateur Amazon S3.

5. Pour Région AWS, choisissez la Région AWS du compartiment S3.
6. Pour Nom du partage de fichiers, entrez un nom pour le partage de fichiers. Le nom par défaut est le nom du compartiment S3 ou le nom du point d'accès.

 Note

- Si vous avez entré un nom de préfixe ou que vous avez choisi de vous connecter via un point d'accès ou un alias de point d'accès, vous devez entrer un nom de partage de fichiers.
- Une fois le partage de fichiers créé, le nom du partage de fichiers ne peut pas être supprimé.

7. (Facultatif) Pour AWS PrivateLink pour S3, procédez comme suit :
 1. Pour configurer le partage de fichiers pour qu'il se connecte à S3 via un point de terminaison d'interface dans votre Virtual Private Cloud (VPC) alimenté par AWS PrivateLink, choisissez l'utilisation d'un point de terminaison VPC.
 2. Pour identifier le point de terminaison de l'interface VPC auquel vous souhaitez que le partage de fichiers se connecte, choisissez l'une des options suivantes : l'identifiant VPC point de terminaison ou le nom DNS du point de terminaison du VPC, puis fournissez les informations requises dans le champ correspondant.

 Note

- Cette étape est requise si le partage de fichiers se connecte à S3 via un point d'accès VPC ou via un alias associé à un point d'accès VPC.
- Les connexions de partage de fichiers utilisant AWS PrivateLink ne sont pas prises en charge sur les passerelles FIPS.

- Pour obtenir des informations sur AWS PrivateLink, voir [AWS PrivateLink pour Amazon S3](#) dans le Guide de l'utilisateur Amazon S3.

8. Pour Access objects using (Accéder aux objets avec), choisissez Network File System (NFS).
9. Pour les Audit logs (Journaux d'audit), choisissez l'une des options suivantes :
 - Pour désactiver la journalisation, choisissez Disable logging (Désactivation de la journalisation)..
 - Pour créer un nouveau journal d'audit, choisissez Créer un nouveau groupe de journaux.
 - Pour utiliser un journal d'audit existant, choisissez Utiliser un groupe de journaux existant, puis choisissez un journal d'audit dans la liste.

Pour de plus amples informations sur les journaux d'audit, veuillez consulter [Comprendre les journaux d'audit de passerelle de fichiers](#).

10. Pour Actualisation automatisée du cache à partir de S3, choisissez Définir l'intervalle de rafraîchissement, et définissez l'heure en jours, heures et minutes pour actualiser le cache du partage de fichiers à l'aide de la fonction Time To Live (TTL). TTL correspond à la durée écoulée depuis la dernière actualisation. Une fois l'intervalle TTL écoulé, l'accès au répertoire entraîne d'abord l'actualisation du contenu de ce répertoire à partir du compartiment Amazon S3.
11. Pour Notification de chargement de fichiers, choisissez Temps de fixation (secondes) pour être averti lorsqu'un fichier a été complètement téléchargé sur S3 par la passerelle de fichiers. Définir la propriété Heure d'installation en secondes pour contrôler le nombre de secondes à attendre après le dernier moment qu'un client a écrit dans un fichier avant de générer un `ObjectUploadedNotification`. Étant donné que les clients peuvent effectuer de nombreuses petites écritures dans des fichiers, il est préférable de définir ce paramètre le plus longtemps possible afin d'éviter de générer plusieurs notifications pour le même fichier dans un petit laps de temps. Pour plus d'informations, consultez [Obtenir une notification de téléchargement de fichiers](#).

Note

Ce paramètre n'a aucun effet sur la synchronisation du chargement de l'objet vers S3, mais uniquement sur le moment de la notification.

12. (Facultatif) Dans la section Add tags (Ajouter des balises), entrez une clé et une valeur pour ajouter des balises à votre partage de fichiers. Une balise est une paire clé-valeur sensible à la casse qui vous aide à gérer, filtrer et rechercher votre partage de fichiers.

13. Choisissez Next (Suivant). LeConfigurer la façon dont les fichiers sont stockés dans Amazon S3s'affiche.
14. PourClasse de stockage pour les nouveaux objets, choisissez la classe de stockage à utiliser pour les nouveaux objets créés dans votre compartiment Amazon S3 :
 - Pour stocker vos données d'objet fréquemment consultées de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les unes des autres, choisissezS3 Standard. Pour de plus amples informations sur la classe de stockage S3 Standard, veuillez consulter.[Classes de stockage pour les objets fréquemment consultés](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.
 - Pour optimiser les coûts de stockage en transférant automatiquement les données vers le niveau d'accès de stockage le plus économique, choisissezS3 Intelligent-Tiering. Pour de plus amples informations sur la classe de stockage S3 Intelligent-Tiering, consultez.[Classe de stockage pour optimiser automatiquement les objets à accès fréquent et peu fréquent](#). dans leManuel de l'utilisateur Amazon Simple Storage Service.
 - Pour stocker vos données d'objet consultées occasionnellement de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les unes des autres, choisissezS3 standard – Accès peu fréquent. Pour de plus amples informations sur la classe de stockage S3 Standard-IA, consultez.[Classes de stockage pour les objets à accès peu fréquent](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.
 - Pour stocker vos données d'objet consultées occasionnellement dans une seule zone de disponibilité, choisissezS3 One Zone-IA. Pour de plus amples informations sur la classe de stockage S3 One Zone-IA, consultez.[Classes de stockage pour les objets à accès peu fréquent](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.

Pour vous aider à surveiller votre facturation S3, utilisezAWS Trusted Advisor. Pour de plus amples informations, veuillez consulter[Outils de surveillance](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.

15. Pour Métadonnées d'objet, choisissez les métadonnées que vous souhaitez utiliser :
 - Pour activer la détermination du type MIME pour les objets chargés à partir des extensions de fichier, choisissezDevinez le type MIME.
 - Pour donner le contrôle total au propriétaire du compartiment S3 qui est mappé sur le partage de fichiers NFS, choisissezDonnez le contrôle total au propriétaire du seau. Pour plus d'informations sur l'utilisation de votre partage de fichiers pour accéder aux objets figurant

dans un compartiment appartenant à un autre compte, consultez [Utilisation d'un partage de fichiers pour l'accès entre comptes](#).

- Si vous utilisez ce partage de fichiers sur un compartiment qui exige que le demandeur ou le lecteur paie les frais d'accès au lieu du propriétaire du compartiment, choisissez Activer le paiement par le demandeur. Pour de plus amples informations, veuillez consulter [Compartiments de type Paiement par le demandeur](#).

16. Pour l'accès à votre compartiment S3, choisissez le AWS Identity and Access Management (IAM) que votre passerelle de fichiers doit utiliser pour accéder à votre compartiment Amazon S3 :

- Pour activer la passerelle de fichiers à créer un rôle et une stratégie d'accès IAM en votre nom, choisissez Création d'un nouveau rôle IAM. Cette option n'est pas disponible si le partage de fichiers se connecte à Amazon S3 à l'aide d'un alias de point d'accès.
- Pour sélectionner un rôle IAM existant et configurer manuellement la stratégie d'accès, choisissez Utiliser un rôle IAM existant. Vous devez utiliser cette option si votre partage de fichiers se connecte à Amazon S3 à l'aide d'un alias de point d'accès. Dans le rôle IAM, saisissez l'Amazon Resource Name (ARN) du rôle utilisé pour accéder à votre compartiment. Pour obtenir des informations sur les rôles IAM, veuillez consulter [IAM roles \(Rôles IAM\)](#) dans le Guide de l'utilisateur AWS Identity and Access Management.

Pour de plus amples informations sur l'accès à votre compartiment S3, consultez [Octroi d'accès à un compartiment Amazon S3](#).

17. Pour le chiffrement, choisissez le type de clés de chiffrement à utiliser pour chiffrer les objets stockés par votre passerelle de fichiers dans Amazon S3 :

- Pour utiliser le chiffrement côté serveur géré avec Amazon S3 (SSE-S3), choisissez Clés de chiffrement gérées par S3 (SSE-S3).
- Pour utiliser le chiffrement côté serveur géré avec AWS Key Management Service (SSE-KMS), choisissez Clés de chiffrement gérées par KMS (SSE-KMS). Dans Clé primaire, choisissez une AWS KMS key ou choisissez Création d'une nouvelle clé KMS pour créer une nouvelle clé KMS dans le AWS Key Management Service (AWS KMS) console. Pour plus d'informations sur AWS KMS, voir [Présentation d'AWS Key Management Service?](#) dans le AWS Key Management Service Manuel du développeur.

 Note

Pour spécifier unAWS KMSavec un alias qui n'est pas répertorié ou qui utilise unAWS KMSclé d'une autreCompte AWS, vous devez utiliser leAWS Command Line Interface(AWS CLI). Pour de plus amples informations, veuillez consulter[CreateNFSFileShare](#)dans leAWSRéférence de Storage Gateway. Les clés KMS asymétriques ne sont pas prises en charge.

18. ChoisissezSuivantpour configurer les paramètres d'accès aux fichiers.

Pour configurer les paramètres d'accès aux fichiers

1. PourClients autorisés, spécifiez si chaque client doit autoriser ou restreindre l'accès de chaque client à votre partage de fichiers. Indiquez l'adresse IP ou la notation CIDR des clients que vous souhaitez autoriser. Pour de plus amples informations sur les clients NFS pris en charge, veuillez consulter [Clients NFS pris en charge pour une passerelle de fichiers](#).
2. PourDes options de montage, spécifiez les options souhaitéesNiveau de squashetExporter as as.

Pour Niveau Squash, choisissez l'une des options suivantes :

- Tous les courges : Tous les accès utilisateur sont mappés sur l'ID utilisateur (UID) (65534) et l'ID de groupe (GID) (65534).
- Sans courge racine : Le super-utilisateur distant (root) reçoit un accès root.
- Courge racine (par défaut) : L'accès pour le super-utilisateur distant (racine) est mappé à UID (65534) et à GID (65534).

Pour Exporter en tant que, choisissez l'une des options suivantes :

- Lecture/écriture
- Lecture seule

Note

Pour les partages de fichiers montés sur un client Microsoft Windows, si vous choisissez Lecture seule, vous pouvez voir un message d'erreur indiquant qu'une erreur imprévue vous empêche de créer le dossier. Vous pouvez ignorer ce message.

3. Pour Valeurs par défaut des métadonnées des fichiers, vous pouvez modifier Autorisations sur le répertoire, Autorisations de fichiers, ID utilisateur et ID de groupe. Pour plus d'informations, consultez [Modification des métadonnées par défaut pour votre partage de fichiers NFS](#).
4. Choisissez Next (Suivant).
5. Vérifiez les paramètres de votre configuration de partage de fichiers, puis choisissez Terminer.

Une fois votre partage de fichiers NFS créé, vous pouvez consulter ses paramètres dans l'onglet Détails (Détails) du partage de fichiers.

Étape suivante

[Montez votre partage de fichiers NFS sur votre client](#)

Création d'un partage de fichiers SMB

Avant de créer un partage de fichiers SMB (Server Message Block), assurez-vous de configurer les paramètres de sécurité SMB pour votre passerelle de fichiers. Vous devez également configurer Microsoft Active Directory (AD) ou un accès invité pour l'authentification. Un partage de fichiers fournit seulement un type d'accès SMB. Pour obtenir des instructions, consultez [Modification des paramètres SMB pour une passerelle](#).

Note

Un partage de fichiers SMB ne fonctionne pas correctement si les ports requis ne sont pas ouverts dans votre groupe de sécurité. Pour plus d'informations, consultez [Exigences de ports](#).

 Note

Lorsqu'un fichier est écrit sur la passerelle de fichiers par un client SMB, la passerelle de fichiers télécharge les données du fichier vers Amazon S3 suivies de ses métadonnées (propriétaires, horodatages, etc.). Le téléchargement des données du fichier crée un objet S3, et le téléchargement des métadonnées du fichier met à jour les métadonnées de l'objet S3. Ce processus crée une autre version de l'objet, entraînant deux versions d'un objet. Si la gestion des versions S3 est activée, les deux versions sont stockées.

Si vous modifiez les métadonnées d'un fichier stocké dans votre passerelle de fichiers, un nouvel objet S3 est créé et remplace l'objet S3 existant. Ce comportement est différent de la modification d'un fichier dans un système de fichiers, où la modification d'un fichier n'entraîne pas la création d'un nouveau fichier. Testez toutes les opérations de fichiers que vous envisagez d'utiliser avec AWSStorage Gateway pour que vous compreniez comment chaque opération de fichier interagit avec le stockage Amazon S3.

Pensez attentivement à l'utilisation du versionnement S3 et de la réplication entre régions (CRR) dans Amazon S3 lorsque vous téléchargez des données depuis votre passerelle de fichiers. Le téléchargement de fichiers depuis votre passerelle de fichiers vers Amazon S3 lorsque le versionnement S3 est activé entraîne au moins deux versions d'un objet S3. Certains flux de travail impliquant des fichiers volumineux et des modèles d'écriture de fichiers, tels que les chargements de fichiers effectués en plusieurs étapes, peuvent augmenter le nombre de versions d'objets S3 stockés. Si le cache de la passerelle de fichiers doit libérer de l'espace en raison des taux d'écriture de fichiers élevés, plusieurs versions d'objets S3 peuvent être créées. Ces scénarios augmentent le stockage S3 si le versionnement S3 est activé et augmentent les coûts de transfert associés au CRR. Testez toutes les opérations de fichiers que vous envisagez d'utiliser avec Storage Gateway afin de comprendre comment chaque opération de fichier interagit avec le stockage Amazon S3. L'utilisation de l'utilitaire Rsync avec votre passerelle de fichiers entraîne la création de fichiers temporaires dans le cache et la création d'objets S3 temporaires dans Amazon S3. Cette situation entraîne des frais de suppression précoce dans les classes de stockage S3 standard peu fréquent (S3 standard — Accès peu fréquent) et S3 Intelligent-Tiering (Accès peu fréquent).

Création d'un partage de fichiers SMB

Pour créer un partage de fichiers SMB

1. Ouverture d'AWSStorage Gateway sur <https://console.aws.amazon.com/storagegateway/home/>.
2. Choisissez **Création d'un partage de fichiers** pour ouvrir l'**Paramètres de partage de fichiers**.
3. Pour **Passerelle**, choisissez votre Amazon S3 File Gateway (Passerelle de fichiers) dans la liste.
4. Pour **Emplacement Amazon S3**, effectuez l'une des actions suivantes :
 - Pour connecter le partage de fichiers directement à un compartiment S3, choisissez **Nom du compartiment S3**, puis entrez le nom du compartiment et, éventuellement, un nom de préfixe pour les objets créés par le partage de fichiers. Votre passerelle utilise ce compartiment pour stocker et récupérer des fichiers. Pour plus d'informations sur la création d'un nouveau compartiment, consultez [Comment créer un compartiment S3 ?](#) dans le **Guide de l'utilisateur Amazon S3**.
 - Pour connecter le partage de fichiers à un compartiment S3 via un point d'accès, choisissez **Point d'accès S3**, puis entrez le nom du point d'accès S3 et, éventuellement, un nom de préfixe pour les objets créés par le partage de fichiers. Votre stratégie de compartiment doit être configurée pour déléguer le contrôle d'accès au point d'accès. Pour plus d'informations sur les points d'accès, consultez [Gestion de l'accès aux données avec les points d'accès Amazon S3](#) et [Délégation du contrôle d'accès aux points d'accès](#) dans le **Guide de l'utilisateur Amazon S3**.
 - Pour connecter le partage de fichiers à un compartiment S3 via un alias de point d'accès, choisissez **Alias de points d'accès S3**, puis entrez le nom de l'alias du point d'accès S3 et, éventuellement, un nom de préfixe pour les objets créés par le partage de fichiers. Si vous choisissez cette option, la passerelle de fichiers ne peut pas créer de nouveau **AWS Identity and Access Management (IAM) stratégie d'accès et de rôle** en votre nom. Vous devez sélectionner un rôle IAM existant et configurer une stratégie d'accès dans le **Accès à votre compartiment S3** section qui suit. Pour de plus amples informations sur les alias des points d'accès, consultez [Utilisation d'un alias de type compartiment pour votre point d'accès](#) dans le **Guide de l'utilisateur Amazon S3**.

Note

- Si vous entrez un nom de préfixe ou si vous choisissez de vous connecter via un point d'accès ou un alias de point d'accès, vous devez entrer un nom de partage de fichiers.
- Le nom du préfixe doit se terminer par une barre oblique (/).
- Une fois le partage de fichiers créé, le nom du préfixe ne peut pas être modifié ni supprimé.
- Pour plus d'informations sur l'utilisation des noms de préfixes, consultez [Organisation des objets à l'aide de préfixes](#) dans le Guide de l'utilisateur Amazon S3.

5. Pour Région AWS, choisissez le Région AWS du compartiment S3.
6. Pour Nom du partage de fichiers, entrez un nom pour le partage de fichiers. Le nom par défaut est le nom du compartiment S3 ou le nom du point d'accès.

Note

- Si vous avez entré un nom de préfixe ou que vous avez choisi de vous connecter via un point d'accès ou un alias de point d'accès, vous devez entrer un nom de partage de fichiers.
- Une fois le partage de fichiers créé, le nom du partage de fichiers ne peut pas être supprimé.

7. (Facultatif) Pour AWS PrivateLink pour S3, procédez comme suit :
 1. Pour configurer le partage de fichiers pour qu'il se connecte à S3 via un point de terminaison d'interface dans votre Virtual Private Cloud (VPC) alimenté par AWS PrivateLink, choisissez Utilisation d'un point de terminaison VPC.
 2. Pour identifier le point de terminaison de l'interface VPC auquel vous souhaitez que le partage de fichiers se connecte, choisissez l'une des options suivantes : Identifiant VPC point de terminaison d'ou Nom DNS du point de terminaison du VPC, puis fournissez les informations requises dans le champ correspondant.

Note

- Cette étape est requise si le partage de fichiers se connecte à S3 via un point d'accès VPC ou via un alias associé à un point d'accès VPC.
- Connexions de partage de fichiers utilisant AWS PrivateLink ne sont pas pris en charge sur les passerelles FIPS.
- Pour obtenir des informations sur AWS PrivateLink, voir [AWS PrivateLink pour Amazon S3](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.

8. Pour Access objects using (Accéder aux objets avec), choisissez Server Message Block (SMB).
9. Pour les Audit logs (Journaux d'audit), choisissez l'une des options suivantes :
 - Pour désactiver la journalisation, choisissez Disable logging (Désactivation de la journalisation)..
 - Pour créer un nouveau journal d'audit, choisissez Créer un nouveau groupe de journaux.
 - Pour utiliser un groupe de journaux existant, choisissez Utiliser un groupe de journaux existant, puis choisissez un journal d'audit dans la liste.

Pour de plus amples informations sur les journaux d'audit, veuillez consulter [Comprendre les journaux d'audit de passerelle de fichiers](#).

10. Pour Actualisation automatisée du cache à partir de S3, choisissez Définir l'intervalle de rafraîchissement, puis définissez l'heure en jours, heures et minutes pour actualiser le cache du partage de fichiers à l'aide de la fonction Time To Live (TTL). TTL correspond à la durée écoulée depuis la dernière actualisation. Une fois l'intervalle TTL écoulé, l'accès au répertoire entraîne d'abord l'actualisation du contenu de ce répertoire à partir du compartiment Amazon S3.
11. Pour Notification de chargement de fichiers, choisissez Temps de fixation (secondes) pour être averti lorsqu'un fichier a été complètement téléchargé sur S3 par la passerelle de fichiers. Définir la propriété Heure d'installation en secondes pour contrôler le nombre de secondes à attendre après le dernier moment qu'un client a écrit dans un fichier avant de générer un ObjectUploadedNotification. Étant donné que les clients peuvent effectuer de nombreuses petites écritures dans des fichiers, il est préférable de définir ce paramètre le plus longtemps possible afin d'éviter de générer plusieurs notifications pour le même fichier dans un petit laps de temps. Pour plus d'informations, consultez [Obtenir une notification de téléchargement de fichiers](#).

 Note

Ce paramètre n'a aucun effet sur la synchronisation du chargement de l'objet vers S3, mais uniquement sur le moment de la notification.

12. (Facultatif) Dans leBalises, choisissezAjouter une nouvelle balise, puis entrez une clé et une valeur pour ajouter des balises à votre partage de fichiers. Une balise est une paire clé-valeur sensible à la casse qui vous aide à gérer, filtrer et rechercher votre partage de fichiers.
13. Choisissez Next (Suivant). LeParamètres de stockage Amazon S3s'affiche.
14. PourClasse de stockage pour les nouveaux objets, choisissez la classe de stockage à utiliser pour les nouveaux objets créés dans votre compartiment Amazon S3 :
 - Pour stocker vos données d'objet fréquemment consultées de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les unes des autres, choisissezS3 Standard. Pour de plus amples informations sur la classe de stockage S3 Standard, veuillez consulter.[Classes de stockage pour les objets fréquemment consultés](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.
 - Pour optimiser les coûts de stockage en transférant automatiquement les données vers le niveau d'accès de stockage le plus économique, choisissezS3 Intelligent-Tiering. Pour de plus amples informations sur la classe de stockage S3 Intelligent-Tiering, consultez.[Classe de stockage pour optimiser automatiquement les objets à accès fréquent et peu fréquent](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.
 - Pour stocker vos données d'objet consultées occasionnellement de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les unes des autres, choisissezS3 standard – Accès peu fréquent. Pour de plus amples informations sur la classe de stockage S3 Standard-IA, consultez.[Classes de stockage pour les objets à accès peu fréquent](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.
 - Pour stocker vos données d'objet consultées occasionnellement dans une seule zone de disponibilité, choisissezS3 One Zone-IA. Pour de plus amples informations sur la classe de stockage S3 One Zone-IA, consultez.[Classes de stockage pour les objets à accès peu fréquent](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.

Pour vous aider à surveiller votre facturation S3, utilisezAWS Trusted Advisor. Pour de plus amples informations, veuillez consulter[Outils de surveillance](#) dans leManuel de l'utilisateur Amazon Simple Storage Service.

15. Pour Métadonnées d'objet, choisissez les métadonnées que vous souhaitez utiliser :
- Pour activer la détermination du type MIME pour les objets chargés à partir des extensions de fichier, choisissez **Devinez le type MIME**.
 - Pour donner le contrôle total au propriétaire du compartiment S3 qui est mappé sur le partage de fichiers SMB, choisissez **Donnez le contrôle total au propriétaire du seau**. Pour plus d'informations sur l'utilisation de votre partage de fichiers pour accéder aux objets figurant dans un compartiment appartenant à un autre compte, consultez [Utilisation d'un partage de fichiers pour l'accès entre comptes](#).
 - Pour donner le contrôle total au propriétaire du compartiment S3 qui est mappé sur le partage de fichiers SMB, choisissez **Activer le paiement par le demandeur**. Pour de plus amples informations, veuillez consulter [Compartiments de type Paiement par le demandeur](#).
16. Pour Accès à votre compartiment S3, choisissez le **AWS Identity and Access Management(IAM)** que votre passerelle de fichiers doit utiliser pour accéder à votre compartiment Amazon S3 :
- Pour activer la passerelle de fichiers à créer un rôle et une stratégie d'accès IAM en votre nom, choisissez **Création d'un nouveau rôle IAM**. Cette option n'est pas disponible si le partage de fichiers se connecte à Amazon S3 à l'aide d'un alias de point d'accès.
 - Pour sélectionner un rôle IAM existant et configurer manuellement la stratégie d'accès, choisissez **Utiliser un rôle IAM existant**. Vous devez utiliser cette option si votre partage de fichiers se connecte à Amazon S3 à l'aide d'un alias de point d'accès. Dans **Rôle IAM**, saisissez l'Amazon Resource Name (ARN) du rôle utilisé pour accéder à votre compartiment. Pour obtenir des informations sur les rôles IAM, veuillez consulter [IAM roles \(Rôles IAM\)](#) dans le Guide de l'utilisateur AWS Identity and Access Management.

Pour de plus amples informations sur l'accès à votre compartiment S3, consultez [Octroi d'accès à un compartiment Amazon S3](#).

17. Pour **Chiffrement**, choisissez le type de clés de chiffrement à utiliser pour chiffrer les objets stockés par votre passerelle de fichiers dans Amazon S3 :
- Pour utiliser le chiffrement côté serveur géré avec Amazon S3 (SSE-S3), choisissez **Clés de chiffrement gérées par S3 (SSE-S3)**.
 - Pour utiliser le chiffrement côté serveur géré avec **AWS Key Management Service(SSE-KMS)**, choisissez **Clés de chiffrement gérées par KMS (SSE-KMS)**. Dans **Clé primaire**, choisissez une **AWS KMS key** ou choisissez **Création d'une nouvelle clé KMS** pour créer une nouvelle clé KMS dans le **AWS Key Management Service(AWS KMS)** console. Pour plus

d'informations sur AWS KMS, voir [Présentation d'AWS Key Management Service?](#) dans le AWS Key Management Service Manuel du développeur.

 Note

Pour spécifier un AWS KMS avec un alias qui n'est pas répertorié ou qui utilise un AWS KMS clé d'une autre Compte AWS, vous devez utiliser le AWS Command Line Interface (AWS CLI). Pour de plus amples informations, veuillez consulter [Create NFS File Share](#) dans le AWS Référence de Storage Gateway. Les clés KMS asymétriques ne sont pas prises en charge.

18. Choisissez Next (Suivant). Le Paramètres d'accès aux fichiers s'affiche.
19. Pour Méthode d'authentification, choisissez la méthode d'authentification que vous souhaitez utiliser.
 - Pour utiliser votre Microsoft AD d'entreprise pour un accès utilisateur authentifié à votre partage de fichiers SMB, choisissez Active Directory. Votre passerelle de fichiers doit être jointe à un domaine.
 - Pour ne fournir qu'un accès invité, choisissez Accès invité. Si vous choisissez cette méthode d'authentification, votre passerelle de fichiers n'a pas besoin de faire partie d'un domaine Microsoft AD. Vous pouvez également utiliser une passerelle de fichiers membre d'un domaine AD pour créer des partages de fichiers avec un accès invité. Vous devez définir un mot de passe invité pour votre serveur SMB dans le champ correspondant.

 Note

Les deux types d'accès sont disponibles en même temps.

20. Dans Paramètres de partage SMB, choisissez vos paramètres.

Pour Exporter en tant que, choisissez l'une des options suivantes :

- Lecture/écriture (valeur par défaut)
- Lecture seule

 Note

Pour les partages de fichiers montés sur un client Microsoft Windows, si vous choisissez Lecture seule, vous pouvez voir un message d'erreur indiquant qu'une erreur imprévue vous empêche de créer le dossier. Vous pouvez ignorer ce message.

Pour File/directory access controlled by (Accès fichier/répertoire contrôlé par), choisissez l'une des options suivantes ::

- Pour définir des autorisations précises sur les fichiers et les dossiers de votre partage de fichiers SMB, choisissez Liste de contrôle d'accès Windows. Pour plus d'informations, consultez [Utilisation des listes ACL Microsoft Windows pour contrôler l'accès à un partage de fichiers SMB](#).
- Pour utiliser les autorisations POSIX pour contrôler l'accès aux fichiers et répertoires stockés via un partage de fichiers NFS ou SMB, choisissez Autorisations POSIX.

Si votre méthode d'authentification est Active Directory, pour Utilisateurs/groupes d'administrateurs, entrez une liste séparée par des virgules d'utilisateurs et de groupes AD. Utilisez cette procédure si vous voulez que l'utilisateur administrateur dispose des privilèges requis pour mettre à jour les listes de contrôle d'accès (ACL) sur tous les fichiers et dossiers du partage de fichiers. Ces utilisateurs et groupes ont alors des droits d'administrateur sur le partage de fichiers. Un groupe doit comporter le préfixe @personnage, par exemple, @group1.

Pour Sensibilité à la casse, choisissez l'une des options suivantes :

- Pour permettre à la passerelle de contrôler la sensibilité de la casse, choisissez spécifié par le client.
- Pour permettre au client de contrôler la sensibilité à la casse, choisissez Forcer la sensibilité au boîtier.

 Note

- Si cette option est sélectionnée, ce paramètre s'applique immédiatement aux nouvelles connexions client SMB. Les connexions client SMB existantes doivent se

déconnecter du partage de fichiers et se reconnecter pour que le paramètre prenne effet.

Pour l'énumération basée sur l'accès, choisissez l'une des options suivantes :

- Pour rendre les fichiers et dossiers du partage visibles uniquement par les utilisateurs ayant accès en lecture, choisissez **Désactivé** pour les fichiers et les répertoires.
- Pour rendre les fichiers et les dossiers du partage visibles par tous les utilisateurs pendant l'énumération des répertoires, choisissez **Activé** pour les fichiers et les répertoires.

 Note

L'énumération basée sur l'accès est un système qui filtre l'énumération des fichiers et des dossiers sur un partage de fichiers SMB en fonction des listes de contrôle d'accès (ACL) du partage.

Pour la serrure opportuniste (oplock), choisissez l'une des options suivantes :

- Pour permettre au partage de fichiers d'utiliser un verrouillage opportuniste afin d'optimiser la stratégie de mise en mémoire tampon des fichiers, choisissez **Activé**. Dans la plupart des cas, l'activation du verrouillage opportuniste améliore les performances, en particulier en ce qui concerne les menus contextuels Windows.
- Pour éviter l'utilisation d'un verrouillage opportuniste, choisissez **Désactivé**. Si plusieurs clients Windows de votre environnement modifient fréquemment les mêmes fichiers simultanément, la désactivation du verrouillage opportuniste peut parfois améliorer les performances.

 Note

L'activation du verrouillage opportuniste sur les partages sensibles à la casse n'est pas recommandée pour les charges de travail qui impliquent l'accès à des fichiers portant le même nom dans des cas différents.

21. (Facultatif) Dans le **Accès au partage de fichiers utilisateur et de groupe**, choisissez vos paramètres.

Pour Utilisateurs et groupes autorisés, choisissez Ajout d'un utilisateur autorisé ou Ajouter un groupe autorisé et entrez un utilisateur ou un groupe AD que vous voulez autoriser l'accès au partage de fichiers. Répétez cette procédure pour autoriser autant d'utilisateurs et de groupes que nécessaire.

Pour Utilisateurs et groupes refusés, choisissez Ajout d'un utilisateur refusé ou Ajouter un groupe refusé et entrez un utilisateur ou un groupe AD que vous voulez refuser l'accès au partage de fichiers. Répétez cette procédure pour refuser autant d'utilisateurs et de groupes que nécessaire.

 Note

L'accès au partage de fichiers utilisateur et de groupes affiche uniquement si Active Directory est sélectionné.

Entrez uniquement le nom d'utilisateur ou de groupe AD. Le nom de domaine est induit par l'appartenance de la passerelle à l'Active Directory spécifique auquel celle-ci est jointe.

Si vous ne spécifiez aucun utilisateur ou groupe autorisé ou refusé, tout utilisateur AD authentifié peut exporter le partage de fichiers.

22. Choisissez Next (Suivant).

23. Vérifiez les paramètres de votre configuration de partage de fichiers, puis choisissez Terminer.

Une fois votre partage de fichiers SMB créé, vous pouvez consulter ses paramètres dans l'onglet Détails du partage de fichiers.

Étape suivante

[Montez votre partage de fichiers SMB sur votre client](#)

Montez et utilisez votre partage de fichiers

Vous trouverez ci-dessous des instructions sur la montage de votre partage de fichiers sur votre client, l'utilisation de votre partage et le test de votre passerelle de fichiers et le nettoyage des ressources selon les besoins. Pour plus d'informations sur les clients NFS (Network File System) pris en charge, consultez [Clients NFS pris en charge pour une passerelle de fichiers](#). Pour plus d'informations sur les clients SMB (Service Message Block) pris en charge, consultez [Clients SMB pris en charge pour une passerelle de fichiers](#).

Vous pouvez trouver des exemples de commande pour monter votre partage de fichiers dans AWS Management Console. Dans les sections suivantes, vous trouverez des détails sur le montage de votre partage de fichiers sur votre client, le test de votre passerelle de fichiers et le nettoyage des ressources selon les besoins.

Rubriques

- [Montez votre partage de fichiers NFS sur votre client](#)
- [Montez votre partage de fichiers SMB sur votre client](#)
- [Utilisation de partages de fichiers sur un compartiment avec des objets préexistants](#)
- [Testez votre passerelle de fichiers S3](#)
- [Comment procéder ensuite ?](#)

Montez votre partage de fichiers NFS sur votre client

Montez le partage de fichiers NFS sur un lecteur de votre client et mappez-le à votre compartiment Amazon S3.

Pour monter un partage de fichiers et le mapper à un compartiment Amazon S3

1. Si vous utilisez un client Microsoft Windows, nous vous recommandons de [créer un partage de fichiers SMB](#) et d'y accéder à l'aide d'un client SMB qui déjà installé sur le client Windows. Si vous utilisez NFS, activez les services pour NFS dans Windows.
2. Montez votre partage de fichiers NFS :
 - Pour votre client Linux, tapez la commande suivante à l'invite de commande.

```
sudo mount -t nfs -o nolock,hard [Your gateway VM IP address]:/[S3 bucket name] [mount path on your client]
```

- Pour vos clients MacOS, tapez la commande suivante à l'invite de commande.

```
sudo mount_nfs -o vers=3,nolock,rwsize=65536,hard -v [Your gateway VM IP address]:/[S3 bucket name] [mount path on your client]
```

- Pour votre client Windows, tapez la commande suivante à l'invite de commande.

```
mount -o nolock -o mtype=hard [Your gateway VM IP address]:/[S3 bucket name] [Drive letter on your windows client]
```

Par exemple, supposez que sur un client Windows l'adresse IP de votre ordinateur virtuel soit 123.123.1.2 et que le nom de votre compartiment Amazon S3 soit `test-bucket`. Supposez également que vous souhaitez effectuer un mappage avec le lecteur T. Dans ce cas, la commande ressemble à ce qui suit.

```
mount -o nolock -o mtype=hard 123.123.1.2:/test-bucket T:
```

Note

En cas de montage de partages de fichiers, gardez à l'esprit les points suivants :

- Il se peut qu'un dossier et un objet existent dans un compartiment Amazon S3 et portent le même nom. Dans ce cas, si l'objet ne contient pas de barre oblique, seul le dossier s'affiche dans une passerelle de fichiers. Par exemple, si un compartiment contient un objet nommé `testtoutest/` et un dossier nommé `test/test1`, uniquement `test/ettest/test1` sont visibles dans une passerelle de fichiers.
- Vous devrez peut-être remonter le partage de fichiers après le redémarrage du client.
- Par défaut, Windows utilise un montage logiciel pour votre partage NFS. Le délai des montages logiciels expire plus facilement en cas de problèmes de connexion. Nous recommandons d'utiliser un montage physique, qui est plus sûr et permet de mieux conserver vos données. La commande de montage conditionnel omet le commutateur **-o mtype=hard**. La commande de montage inconditionnel Windows utilise le commutateur `-o mtype=hard`.
- Si vous utilisez des clients Windows, vérifiez vos options `mount` après le montage en exécutant la commande `mount` sans options. La réponse doit confirmer que le partage

de fichiers a été monté en fonction des dernières options que vous avez indiquées. Elle doit également confirmer que vous n'utilisez pas d'entrées anciennes mises en cache, dont l'effacement prend au moins 60 secondes.

Étape suivante

[Testez votre passerelle de fichiers S3](#)

Montez votre partage de fichiers SMB sur votre client

Montez maintenant votre partage de fichiers SMB et mappez-le à une unité accessible par votre client. La section Passerelle de fichiers de la console montre les commandes de montage prises en charge que vous pouvez utiliser pour les clients SMB. Vous trouverez ci-après des options supplémentaires pour essayer.

Vous pouvez utiliser plusieurs méthodes différentes pour monter les partages de fichiers SMB, dont les suivantes :

- Invite de commande (`cmdkeyetnet use`) : Utilisez l'invite de commande pour monter votre partage de fichiers. Stockez vos identifiants avec `cmdkey`, puis montez le disque avec `net use` et incluez `/persistent:yeset/savecreds` si vous souhaitez que la connexion persiste lors des redémarrages du système. Les commandes spécifiques que vous utilisez seront différentes selon que vous souhaitez monter le lecteur pour un accès Microsoft Active Directory (AD) ou invité. Des exemples sont donnés ci-après.
- Explorateur de fichiers (Map Network Drive) : utilisez l'Explorateur de fichiers Windows pour monter votre partage de fichiers. Configurez les paramètres pour spécifier si vous souhaitez que la connexion persiste pendant les redémarrages du système et demandez des informations d'identification réseau.
- Script PowerShell : créez un script PowerShell personnalisé pour monter votre partage de fichiers. Selon les paramètres spécifiés dans le script, la connexion peut être persistante lors des redémarrages du système et le partage peut être visible ou invisible par le système d'exploitation lorsqu'il est monté.

Note

Si vous êtes un utilisateur Microsoft AD, consultez votre administrateur pour vous assurer que vous avez accès au partage de fichiers SMB avant de monter le partage de fichiers sur votre système local.

Si vous êtes un utilisateur invité, assurez-vous que vous disposez du mot de passe du compte utilisateur invité avant de tenter de monter le partage de fichiers.

Pour monter votre partage de fichiers SMB pour les utilisateurs Microsoft AD autorisés à l'aide de l'invite de commande :

1. Assurez-vous que l'utilisateur Microsoft AD dispose des autorisations nécessaires sur le partage de fichiers SMB avant de monter le partage de fichiers sur le système de l'utilisateur.
2. Saisissez les informations suivantes à l'invite de commande pour monter le partage de fichiers :

```
net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /  
persistent:yes
```

Pour monter votre partage de fichiers SMB avec une combinaison spécifique de nom d'utilisateur et de mot de passe à l'aide de l'invite de commande :

1. Assurez-vous que le compte utilisateur ait accès au partage de fichiers SMB avant de monter le partage de fichiers sur le système.
2. Saisissez les informations suivantes à l'invite de commande pour enregistrer les informations d'identification de l'utilisateur dans Windows Credential Manager :

```
cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
```

3. Saisissez les informations suivantes à l'invite de commande pour monter le partage de fichiers :

```
net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /  
persistent:yes /savecred
```

Pour monter votre partage de fichiers SMB pour les utilisateurs invités à l'aide de l'invite de commande :

1. Assurez-vous que vous disposez du mot de passe du compte utilisateur invité avant de monter le partage de fichiers.
2. Saisissez ce qui suit à l'invite de commandes pour enregistrer les informations d'identification de l'invité dans le Gestionnaire d'informations d'identification Windows :

```
cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
```

3. Saisissez les informations suivantes à l'invite de commande.

```
net use WindowsDriveLetter: \\$GatewayIPAddress\Path /user:$GatewayID\smbguest /persistent:yes /savecred
```

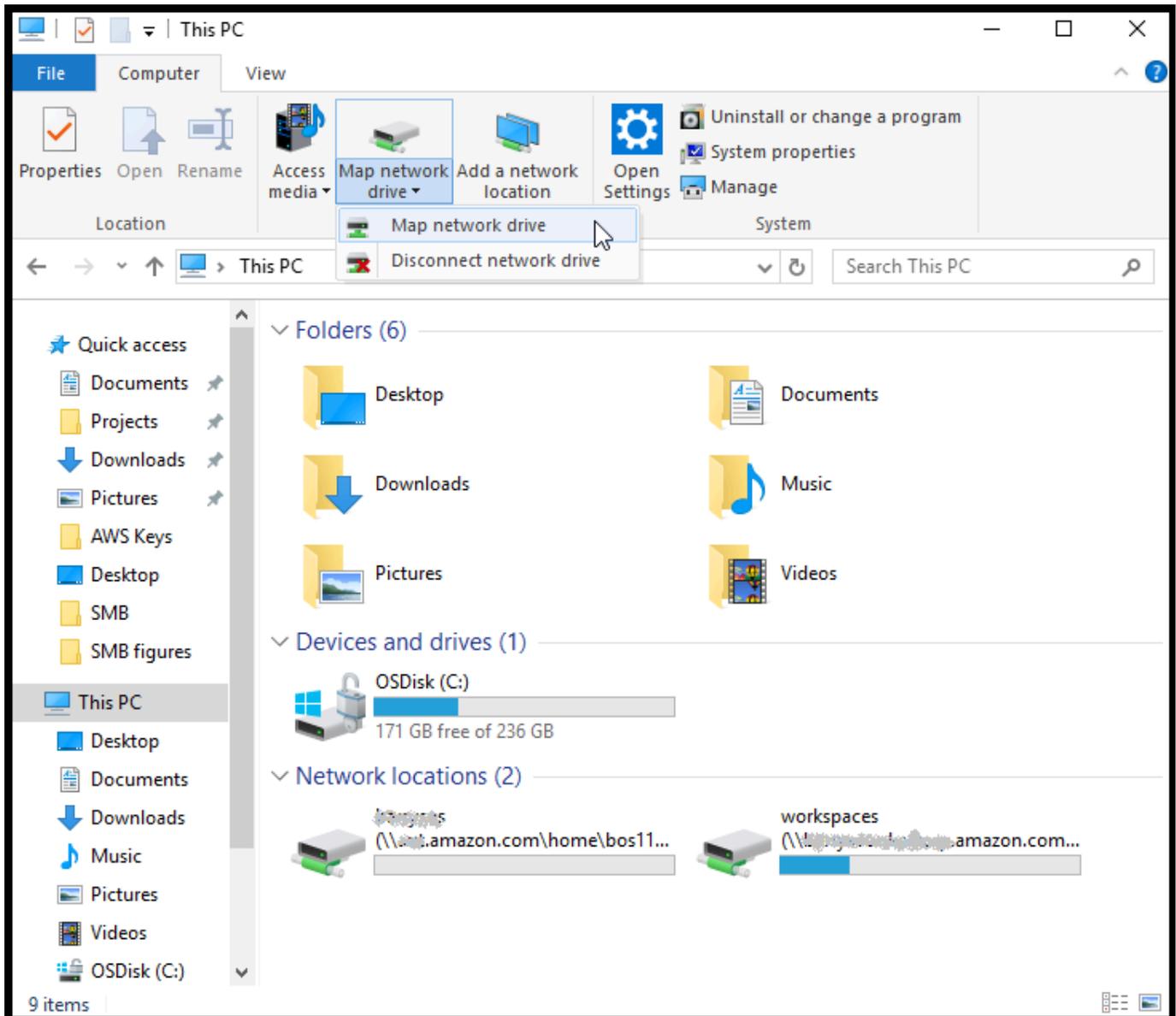
Note

En cas de montage de partages de fichiers, gardez à l'esprit les points suivants :

- Il se peut qu'un dossier et un objet existent dans un compartiment Amazon S3 et portent le même nom. Dans ce cas, si l'objet ne contient pas de barre oblique, seul le dossier s'affiche dans une passerelle de fichiers. Par exemple, si un compartiment contient un objet nommé `testoutest/` et un dossier nommé `test/test1`, uniquement `test/etest/test1` sont visibles dans une passerelle de fichiers.
- À moins que vous ne configuriez votre connexion de partage de fichiers pour enregistrer vos informations d'identification utilisateur et persister pendant les redémarrages du système, vous devrez peut-être remonter votre partage de fichiers chaque fois que vous redémarrez votre système client.

Pour monter un partage de fichiers SMB à l'aide de l'Explorateur de fichiers Windows

1. Appuyez sur la touche Windows et tapez **File Explorer** dans la zone Rechercher dans Windows ou appuyez sur **Win+E**.
2. Dans le volet de navigation, sélectionnez Ce PC, puis choisissez Connecter un lecteur réseau pour Connecter un lecteur réseau dans l'onglet Ordinateur, comme illustré dans la capture d'écran suivante.



3. Dans la boîte de dialogue Connecter un lecteur réseau, choisissez une lettre de lecteur pour Lecteur.
4. Pour Dossier, tapez `\\[File Gateway IP]\[SMB File Share Name]`, ou choisissez Parcourir pour sélectionner votre partage de fichiers SMB dans la boîte de dialogue.
5. (Facultatif) Sélectionnez Se reconnecter lors de la connexion si vous voulez que votre point de montage persiste après le redémarrage.
6. (Facultatif) Sélectionnez Se connecter à l'aide d'informations d'identification différentes si vous voulez qu'un utilisateur entre les informations de connexion Microsoft AD ou le mot de passe utilisateur du compte invité.
7. Choisissez Terminer pour terminer votre point de montage.

Vous pouvez modifier les paramètres de partage de fichiers, les autorisations accordées et refusées aux utilisateurs et aux groupes, ainsi que le mot de passe d'accès invité à partir de la console de gestion AWS Storage Gateway. Vous pouvez également actualiser les données dans le cache du partage de fichiers et supprimer un partage de fichiers à partir de la console.

Pour modifier les propriétés de votre partage de fichiers SMB

1. Ouvrez la console Storage Gateway à l'adresse <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le volet de navigation, choisissez Partages de fichiers.
3. Sur la page Partages de fichiers, cochez la case en regard du partage de fichiers SMB que vous souhaitez modifier.
4. Pour Actions, sélectionnez l'action de votre choix :
 - Choisissez Configurer les paramètres du partage de fichiers pour modifier les paramètres du partage d'accès.
 - Choisissez Edit allowed/denied users (Modifier des utilisateurs autorisés/refusés) pour ajouter ou supprimer des utilisateurs et des groupes, puis indiquez les utilisateurs et les groupes autorisés et refusés dans les zones Allowed Users (Utilisateurs autorisés), Denied Users (Utilisateurs refusés), Allowed Groups (Groupes autorisés) et Denied Groups (Groupes refusés). Utilisez les boutons Ajouter une entrée pour créer des droits d'accès, et le bouton (X) pour supprimer un accès.
5. Lorsque vous avez terminé, choisissez Enregistrer.

Lorsque vous indiquez des utilisateurs et des groupes autorisés, vous créez une liste d'autorisations. Sans liste d'autorisation, tous les utilisateurs Microsoft AD authentifiés peuvent accéder au partage de fichiers SMB. Tous les utilisateurs et les groupes marqués comme refusés sont ajoutés à une liste de refus et ne peuvent pas accéder au partage de fichiers SMB. Dans les cas où un utilisateur ou un groupe se trouve à la fois sur la liste de refus et d'autorisation, la liste de refus est prioritaire.

Vous pouvez activer les listes de contrôle d'accès (ACL) sur votre partage de fichiers SMB. Pour plus d'informations sur l'activation des listes ACL, consultez [Utilisation des listes ACL Microsoft Windows pour contrôler l'accès à un partage de fichiers SMB](#).

Étape suivante

[Testez votre passerelle de fichiers S3](#)

Utilisation de partages de fichiers sur un compartiment avec des objets préexistants

Vous pouvez exporter un partage de fichiers sur un compartiment Amazon S3 avec des objets créés en dehors de la passerelle de fichiers à l'aide de NFS ou de SMB. Les objets du compartiment créés en dehors de la passerelle s'affichent en tant que fichiers dans le système de fichiers NFS ou SMB lorsque vos clients de système de fichiers y accèdent. L'accès et les autorisations POSIX (Portable Operating System Interface) standard sont utilisés dans le partage de fichiers. Lorsque vous réécrivez des fichiers dans un compartiment Amazon S3, ceux-ci prennent les propriétés et les droits d'accès que vous leur attribuez.

Vous pouvez charger des objets dans un compartiment S3 à tout moment. Pour que le partage de fichiers affiche ces objets nouvellement ajoutés en tant que fichiers, vous devez actualiser le compartiment S3. Pour plus d'informations, consultez [the section called "Actualisation des objets dans votre compartiment Amazon S3"](#).

Note

Nous ne vous recommandons pas d'avoir plusieurs enregistreurs pour un compartiment Amazon S3. Si vous le faites, veillez à lire la section « Puis-je avoir plusieurs enregistreurs sur mon compartiment Amazon S3 ? » dans le [FAQ Storage Gateway](#).

Pour attribuer des métadonnées par défaut à des objets accessibles à l'aide de NFS, consultez [Modification des métadonnées par défaut dans Gestion de votre passerelle Amazon S3 File Gateway](#).

Pour SMB, vous pouvez exporter un partage via un accès Microsoft AD ou invité vers un compartiment Amazon S3 avec des objets pré-existants. Les objets exportés via un partage de fichiers SMB hérite de la propriété et des autorisations POSIX du répertoire parent juste au-dessus. Pour les objets sous le dossier racine, les listes de contrôle d'accès (ACL) racine sont héritées. Pour la liste ACL racine, le propriétaire est `smbgues t`, les autorisations pour les fichiers sont 666 et les répertoires sont 777. Cela s'applique à toutes les formes d'accès authentifié (Microsoft AD et invité)

Testez votre passerelle de fichiers S3

Vous pouvez copier des fichiers et des dossiers sur votre lecteur mappé. Les fichiers se chargent automatiquement dans votre compartiment Amazon S3.

Pour télécharger les fichiers de votre client Windows vers Amazon S3

1. Sur le client Windows, accédez au lecteur sur lequel vous avez monté le partage de fichiers. Le nom de votre lecteur est précédé du nom de votre compartiment S3.
2. Copiez des fichiers ou un dossier sur le lecteur.
3. Sur Amazon S3 Management Console, accédez au compartiment mappé. Vous devez voir les fichiers et les dossiers que vous avez copiés dans le compartiment Amazon S3 spécifié.

Vous pouvez voir le partage de fichiers que vous avez créé dans lepartages de fichiersdans l'ongletAWSConsole de gestion Storage Gateway

Votre client NFS ou SMB peut écrire, lire, supprimer, renommer et tronquer des fichiers.

Note

Les passerelles de fichiers ne prennent pas en charge la création de liens symboliques ou physiques sur un partage de fichiers.

Tenez compte des points suivants concernant l'interaction entre les passerelles de fichiers et S3 :

- Les lectures sont diffusées à partir d'un cache de lecture. Cela signifie que si les données ne sont pas disponibles, elles sont récupérées à partir de S3 et ajoutées au cache.
- Les écritures sont envoyées à S3 via des chargements partitionnés optimisés par le biais d'un cache à écriture différée.
- Les lectures et les écritures sont optimisées afin que seuls les éléments qui sont demandés ou modifiés soient transférés sur le réseau.
- Les opérations de suppression suppriment les objets de S3.
- Les répertoires sont gérés en tant qu'objets de dossiers dans S3, en utilisant la même syntaxe que la console Amazon S3. Vous pouvez renommer les répertoires vides.
- Les performances de fonctionnement du système de fichiers récursif (par exemple, `ls -l`) dépendent du nombre d'objets dans le compartiment.

Étape suivante

[Comment procéder ensuite ?](#)

Comment procéder ensuite ?

Dans les sections précédentes, vous avez créé et lancé une passerelle de fichiers, et notamment monté un partage de fichiers et testé la configuration.

D'autres sections de ce manuel incluent des informations sur les procédures suivantes :

- Pour gérer votre passerelle de fichiers, consultez [Gestion de votre passerelle Amazon S3 File Gateway](#).
- Pour optimiser votre passerelle de fichiers, consultez [Optimisation des performances de la passerelle](#).
- Pour résoudre les problèmes liés à la passerelle, consultez [Résolution des problèmes de passerelle](#).
- Pour en savoir plus sur les métriques Storage Gateway et sur le contrôle des performances de la passerelle, consultez.

Nettoyez les ressources dont vous n'avez pas besoin

Si vous avez créé la passerelle à titre d'exercice ou de test, pensez à nettoyer les ressources dont vous n'avez pas besoin pour éviter les frais inattendus ou inutiles.

Pour nettoyer les ressources dont vous n'avez pas besoin

1. A moins que vous ayez l'intention de continuer à utiliser la passerelle, supprimez-la. Pour plus d'informations, consultez [Suppression de votre passerelle à l'aide de la Console AWS Storage Gateway et suppression des ressources associées](#).
2. Supprimez l'ordinateur virtuel Storage Gateway de votre hôte sur site. Si vous avez créé votre passerelle sur une instance Amazon EC2, mettez fin à l'instance.

Activer une passerelle dans un cloud privé virtuel

Vous pouvez créer une connexion privée entre votre appliance logicielle sur site et une infrastructure de stockage basée sur le cloud. Vous pouvez ensuite utiliser l'appliance logicielle pour transférer des données vers AWS stockage sans que votre passerelle ne communique avec AWS services de stockage via l'Internet public. À l'aide du service Amazon VPC, vous pouvez lancer AWS 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 le VPCs, consultez [Qu'est-ce qu'Amazon VPC ?](#) dans le Amazon VPC User Guide.

Pour utiliser une passerelle avec un point de terminaison de VPC Storage Gateway dans votre VPC, procédez comme suit :

- Utilisez la console VPC pour créer un point de terminaison de VPC pour Storage Gateway et obtenir l'ID du point de terminaison de VPC. Spécifiez cet ID de point de terminaison VPC lorsque vous créez et activez la passerelle.
- Si vous activez une passerelle de fichiers, créez un point de terminaison de VPC pour Amazon S3. Spécifiez ce point de terminaison VPC lorsque vous créez des partages de fichiers pour votre passerelle.
- Si vous activez une passerelle de fichiers, vous devez définir un proxy HTTP et le configurer dans la console locale de la machine virtuelle de passerelle de fichiers. Ce proxy est nécessaire pour les passerelles de fichiers locales qui sont basées sur l'hyperviseur, telles que celles basées sur VMware, Microsoft HyperV et KVM (machine virtuelle basée sur le noyau Linux). Dans ces cas, vous avez besoin du proxy pour activer les points de terminaison privés Amazon S3 depuis l'extérieur de votre VPC. Pour plus d'informations sur la configuration d'un proxy HTTP, consultez [Configuration d'un proxy HTTP](#)

Note

Votre passerelle doit être activée dans la même région que celle où votre point de terminaison de VPC a été créé.

Pour la passerelle de fichiers, le stockage Amazon S3 configuré pour le partage de fichiers doit se trouver dans la même région que celle où vous avez créé le point de terminaison de VPC pour Amazon S3.

Rubriques

- [Création d'un point de terminaison de VPC pour Storage Gateway](#)
- [Configuration et configuration d'un proxy HTTP \(passerelles de fichiers sur site uniquement\)](#)
- [Autorisation du trafic vers les ports requis dans votre proxy HTTP](#)

Création d'un point de terminaison de VPC pour Storage Gateway

Suivez ces instructions pour créer un point de terminaison de VPC. Si vous disposez déjà d'un point de terminaison de VPC pour Storage Gateway, vous pouvez l'utiliser.

Pour créer un point de terminaison de VPC pour Storage Gateway

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoints (Points de terminaison), puis Create Endpoint (Créer un point de terminaison).
3. Dans la page Créez un point de terminaison, choisissez AWS Services pour Catégorie de services.
4. Pour Service Name (Nom du service), choisissez `com.amazonaws.region.storagegateway`. Par exemple, `com.amazonaws.us-east-2.storagegateway`.
5. Pour VPC, sélectionnez votre VPC et notez ses zones de disponibilité et sous-réseaux.
6. Vérifiez que Enable Private DNS Name (Activer le nom DNS privé) n'est pas sélectionné.
7. Pour Groupe de sécurité, choisissez le groupe de sécurité que vous souhaitez utiliser pour votre VPC. Vous pouvez accepter le groupe de sécurité par défaut. Vérifiez que tous les ports TCP suivants sont autorisés dans votre groupe de sécurité :
 - TCP 443
 - TCP 1026
 - TCP 1027
 - TCP 1028
 - TCP 1031
 - TCP 2222

8. Choisissez Create endpoint (Créer un point de terminaison). L'état initial du point de terminaison est pending (en attente). Lorsque le point de terminaison est créé, prenez note de l'ID du point de terminaison de VPC que vous venez de créer.
9. Lorsque le point de terminaison est créé, choisissez Endpoints (Points de terminaison), puis choisissez le nouveau point de terminaison de VPC.
10. Dans la section DNS Names (Noms DNS), utilisez le premier nom DNS qui ne spécifie aucune zone de disponibilité. Votre nom DNS ressemble à ceci : `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Maintenant que vous disposez d'un point de terminaison de VPC, vous pouvez créer votre passerelle.

Important

Si vous créez une passerelle de fichiers, vous devez créer un point de terminaison pour Amazon S3 également. Suivez les mêmes étapes que celles présentées dans la section Pour créer un point de terminaison de VPC pour Storage Gateway ci-dessus, mais choisissez `com.amazonaws.us-east-2.s3` sous Nom du service à la place. Ensuite, sélectionnez la table de routage à laquelle sera associé le point de terminaison S3 au lieu du groupe de sous-réseau/sécurité. Pour obtenir des instructions, consultez [Création d'un point de terminaison de passerelle](#).

Configuration et configuration d'un proxy HTTP (passerelles de fichiers sur site uniquement)

Si vous activez une passerelle de fichiers, vous devez définir un proxy HTTP et le configurer via la console locale de la machine virtuelle de passerelle de fichiers. Ce proxy est nécessaire pour que la passerelle de fichiers sur site accède aux points de terminaison privés Amazon S3 depuis l'extérieur de votre VPC. Si vous disposez déjà d'un proxy HTTP dans Amazon EC2, vous pouvez l'utiliser. Toutefois, vous devez vérifier que tous les ports TCP suivants sont autorisés dans votre groupe de sécurité :

- TCP 443
- TCP 1026
- TCP 1027

- TCP 1028
- TCP 1031
- TCP 2222

Si vous n'avez pas de proxy Amazon EC2, procédez comme suit pour définir et configurer un proxy HTTP.

Pour définir un serveur proxy

1. Lancez une AMI Linux Amazon EC2. Nous vous recommandons d'utiliser une famille d'instances optimisée pour le réseau telle que c5n.large.
2. Utilisez la commande suivante pour installer Squid : **sudo yum install squid**. Cette opération crée un fichier de configuration par défaut dans `/etc/squid/squid.conf`.
3. Remplacez le contenu de ce fichier par ce qui suit.

```
#
# Recommended minimum configuration:
#

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8           # RFC1918 possible internal network
acl localnet src 172.16.0.0/12      # RFC1918 possible internal network
acl localnet src 192.168.0.0/16    # RFC1918 possible internal network
acl localnet src fc00::/7          # RFC 4193 local private network range
acl localnet src fe80::/10         # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl SSL_ports port 1026
acl SSL_ports port 1027
acl SSL_ports port 1028
acl SSL_ports port 1031
acl SSL_ports port 2222
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
```

```

http_access deny !SSL_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:                1440      20%      10080
refresh_pattern ^gopher:             1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%       0
refresh_pattern .                     0         20%     4320

```

4. Si vous n'avez pas besoin de verrouiller le serveur proxy ni d'apporter de modifications, activez et démarrez-le à l'aide des commandes suivantes. Ces commandes permettent de démarrer le serveur à l'initialisation.

```

sudo chkconfig squid on
sudo service squid start

```

Vous pouvez désormais configurer le proxy HTTP de Storage Gateway qui sera utilisé par. Lorsque vous configurez la passerelle pour qu'elle utilise un proxy, spécifiez le port squid par défaut 3128. Le fichier squid.conf qui est généré couvre les ports TCP obligatoires suivants par défaut :

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Pour utiliser la console locale de la machine virtuelle pour configurer le proxy HTTP

1. Connectez-vous à la console locale de machine virtuelle de la passerelle. Pour plus d'informations sur la façon de connecter, consultez [Connexion à la console locale de la passerelle de fichiers](#).
2. Dans le menu principal, choisissez Configure proxy HTTP (Configurer un proxy HTTP).
3. Dans le menu Configuration, choisissez Configure HTTP proxy (Configurer un proxy HTTP).
4. Fournissez le nom d'hôte et le port de votre serveur proxy.

Pour obtenir des informations détaillées sur la façon de configurer un proxy HTTP, consultez [Configuration d'un proxy HTTP](#).

Autorisation du trafic vers les ports requis dans votre proxy HTTP

Si vous utilisez un proxy HTTP, assurez-vous d'autoriser le trafic depuis Storage Gateway vers les destinations et les ports répertoriés ci-dessous.

Lorsque Storage Gateway communique via les points de terminaison publics, il utilise les services Storage Gateway suivants.

```
anon-cp.storagegateway.region.amazonaws.com:443  
client-cp.storagegateway.region.amazonaws.com:443  
proxy-app.storagegateway.region.amazonaws.com:443  
dp-1.storagegateway.region.amazonaws.com:443  
storagegateway.region.amazonaws.com:443 (Required for making API calls)  
s3.region.amazonaws.com (Required only for File Gateway)
```

⚠ Important

En fonction de votre passerelleAWSRégion, remplacer*région* dans le point de terminaison avec la chaîne de région correspondante. Par exemple, si vous créez une passerelle dans la région USA Ouest (Oregon), le point de terminaison doit être similaire à `:storagegateway.us-west-2.amazonaws.com:443`.

Lorsque Storage Gateway communique via le point de terminaison de VPC, il utilise leAWSvia plusieurs ports sur le point de terminaison de VPC Storage Gateway et le port 443 du point de terminaison privé Amazon S3.

- Ports TCP sur un point de terminaison de VPC de passerelle de fichiers
 - 443, 1026, 1027, 1028, 1031 et 2222
- Port TCP sur point de terminaison privé S3
 - 443

Gestion de votre passerelle Amazon S3 File Gateway

Vous trouverez ci-après des informations sur la façon de gérer les ressources de votre Amazon S3 File Gateway.

Rubriques

- [Ajout d'un partage de fichiers](#)
- [Suppression d'un partage de fichiers](#)
- [Modification des paramètres de votre partage de fichiers NFS](#)
- [Modification des métadonnées par défaut pour votre partage de fichiers NFS](#)
- [Modification des paramètres d'accès de votre partage de fichiers NFS](#)
- [Modification des paramètres SMB pour une passerelle](#)
- [Modification des paramètres de votre partage de fichiers SMB](#)
- [Actualisation des objets dans votre compartiment Amazon S3](#)
- [Utilisation de la fonctionnalité de verrouillage des objets S3 avec une passerelle de fichiers Amazon S3](#)
- [Comprendre l'état du partage de fichiers](#)
- [Bonnes pratiques de partage de fichiers](#)

Ajout d'un partage de fichiers

Une fois que votre passerelle de fichiers S3 est activée et est en cours d'exécution, vous pouvez ajouter des partages de fichiers supplémentaires et accorder l'accès aux compartiments Amazon S3. Les compartiments auxquels vous pouvez accorder l'accès incluent les compartiments dans un autre compte AWS que votre partage de fichiers. Pour plus d'informations sur la façon d'ajouter un partage de fichiers, consultez [Création d'un partage de fichiers](#).

Rubriques

- [Octroi d'accès à un compartiment Amazon S3](#)
- [Prévention du député confus entre services](#)
- [Utilisation d'un partage de fichiers pour l'accès entre comptes](#)

Octroi d'accès à un compartiment Amazon S3

Lorsque vous créez un partage de fichiers, votre passerelle de fichiers nécessite un accès pour charger des fichiers dans votre compartiment Amazon S3 et pour effectuer des actions sur tous les points d'accès ou les points de terminaison de cloud privé virtuel (VPC) qu'elle utilise pour se connecter au compartiment. Pour accorder cet accès, votre passerelle de fichiers prend en compte une AWS Identity and Access Management (IAM) associé à une stratégie IAM qui octroie cet accès.

Le rôle requiert cette stratégie IAM avec une relation d'approbation de service de jetons de sécurité (STS). La stratégie détermine les actions que le rôle peut effectuer. De plus, votre compartiment S3 et tous les points d'accès ou points de terminaison VPC associés doivent avoir une stratégie d'accès qui permet au rôle IAM d'y accéder.

Vous pouvez créer vous-même le rôle et la stratégie d'accès, ou votre passerelle de fichiers peut les créer pour vous. Si votre passerelle de fichiers crée la stratégie pour vous, celle-ci contient une liste d'actions S3. Pour plus d'informations sur les rôles et les autorisations, consultez [Création d'un rôle pour la délégation d'autorisations à un Service AWS](#) dans le IAM User Guide.

L'exemple de stratégie d'approbation suivant permet à votre passerelle de fichiers d'assumer un rôle IAM.

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

Si vous ne voulez pas que votre passerelle de fichiers crée une stratégie en votre nom, créez-en une vous-même et attachez-la à votre partage de fichiers. Pour plus d'informations sur cette étape, consultez [Création d'un partage de fichiers](#).

L'exemple de stratégie suivant autorise votre passerelle de fichiers à effectuer toutes les actions Amazon S3 qui y sont répertoriées. La première partie de l'instruction permet de toutes les actions

répertoriées d'être exécutées sur le compartiment S3 nommé TestBucket. La seconde partie autorise les actions répertoriées sur tous les objets dans TestBucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketLocation",
        "s3:GetBucketVersioning",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:ListBucketMultipartUploads"
      ],
      "Resource": "arn:aws:s3:::TestBucket",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectVersion",
        "s3:ListMultipartUploadParts",
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::TestBucket/*",
      "Effect": "Allow"
    }
  ]
}
```

L'exemple de stratégie suivant est similaire à la stratégie précédente, mais permet à votre passerelle de fichiers d'effectuer les actions nécessaires pour accéder à un compartiment via un point d'accès.

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

```
    "Action": [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:GetObject",
      "s3:GetObjectAcl",
      "s3:GetObjectVersion",
      "s3:ListMultipartUploadParts",
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:us-east-1:123456789:accesspoint/
TestAccessPointName/*",
    "Effect": "Allow"
  }
]
```

Note

Si vous devez connecter votre partage de fichiers à un compartiment S3 via un point de terminaison VPC, consultez [Stratégies de point de terminaison pour Amazon S3](#) dans le AWS PrivateLink Guide de l'utilisateur.

Prévention du député confus entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. Dans AWS, l'emprunt d'identité entre services peut entraîner le problème de député confus. L'emprunt d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé pour utiliser ses autorisations afin d'agir sur les ressources d'un autre client de manière à ce qu'il ne soit pas autorisé à y accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous vous recommandons d'utiliser les clés de contexte de condition globale [aws:SourceArn](#) et [aws:SourceAccount](#) dans les politiques de ressources pour limiter les autorisations à la ressource octroyées par AWS Storage Gateway à un autre service. 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 politique.

`Pouraws:SourceArn` doit être l'ARN de Storage Gateway auquel votre partage de fichiers est associé.

Le moyen le plus efficace de se protéger contre le problème de député confus consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (*) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:service:123456789012:*`.

L'exemple suivant montre comment utiliser les `aws:SourceArn` et `aws:SourceAccount` clés de contexte de condition globale dans Storage Gateway pour éviter le problème confus des adjoints.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "storagegateway.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws:storagegateway:us-east-1:123456789012:gateway/sgw-712345DA"
      }
    }
  }
}
```

Utilisation d'un partage de fichiers pour l'accès entre comptes

Cross-comptes l'accès s'effectue lorsqu'un compte Amazon Web Services et les utilisateurs de ce compte obtiennent l'accès à des ressources qui appartiennent à un autre compte Amazon Web

Services. Avec les passerelles de fichiers, vous pouvez utiliser un partage de fichiers dans un compte Amazon Web Services pour accéder à des objets figurant dans un compartiment Amazon S3 qui appartient à un autre compte Amazon Web Services.

Pour utiliser un partage de fichiers appartenant à un compte Amazon Web Services afin d'accéder à un compartiment S3 dans un autre compte Amazon Web Services

1. Assurez-vous que le propriétaire du compartiment S3 a accordé à votre compte Amazon Web Services l'accès au compartiment S3 auquel vous avez besoin d'accéder et aux objets de ce compartiment. Pour plus d'informations sur la façon d'accorder cet accès, consultez [Exemple 2 : Propriétaire d'un compartiment octroyant des autorisations entre comptes sur un](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service. Pour obtenir la liste des autorisations requises, consultez [Octroi d'accès à un compartiment Amazon S3](#).
2. Assurez-vous que le rôle IAM que votre partage de fichiers utilise pour accéder au compartiment S3 inclut des autorisations pour les opérations telles que `s3:GetObjectAc1` et `s3:PutObjectAc1`. De plus, assurez-vous que le rôle IAM inclut une stratégie d'approbation qui autorise votre compte à assumer ce rôle IAM. Pour voir un exemple d'une telle stratégie d'approbation, consultez [Octroi d'accès à un compartiment Amazon S3](#).

Si votre partage de fichiers utilise un rôle existant pour accéder au compartiment S3, vous devez inclure des autorisations pour les opérations telles que `s3:GetObjectAc` et `s3:PutObjectAc1`. Le rôle a également besoin d'une stratégie d'approbation qui autorise votre compte à endosser ce rôle. Pour voir un exemple d'une telle stratégie d'approbation, consultez [Octroi d'accès à un compartiment Amazon S3](#).

3. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
4. Choisissez Accorder le contrôle total au propriétaire du compartiment dans les paramètres Métadonnées d'objet dans la boîte de dialogue Configurer les paramètres du partage de fichiers.

Une fois que vous avez créé ou mis à jour votre partage de fichiers pour l'accès entre comptes et monté le partage de fichiers sur site, nous vous recommandons vivement de tester votre configuration. Pour ce faire, vous pouvez répertorier le contenu du répertoire ou écrire des fichiers de test et vérifier que les fichiers apparaissent en tant qu'objets dans le compartiment S3.

Important

Assurez-vous de configurer les stratégies correctement pour accorder un accès entre comptes au compte utilisé par votre partage de fichiers. Dans le cas contraire, les mises

à jour des fichiers par le biais de vos applications sur site ne se propagent pas dans le compartiment Amazon S3 que vous utilisez.

Ressources

Pour plus d'informations sur les stratégies d'accès et les listes de contrôle d'accès, consultez les ressources suivantes :

[Instructions d'utilisation des options de stratégie d'accès disponibles](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service

[Présentation de la liste de contrôle d'accès \(ACL\)](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service

Suppression d'un partage de fichiers

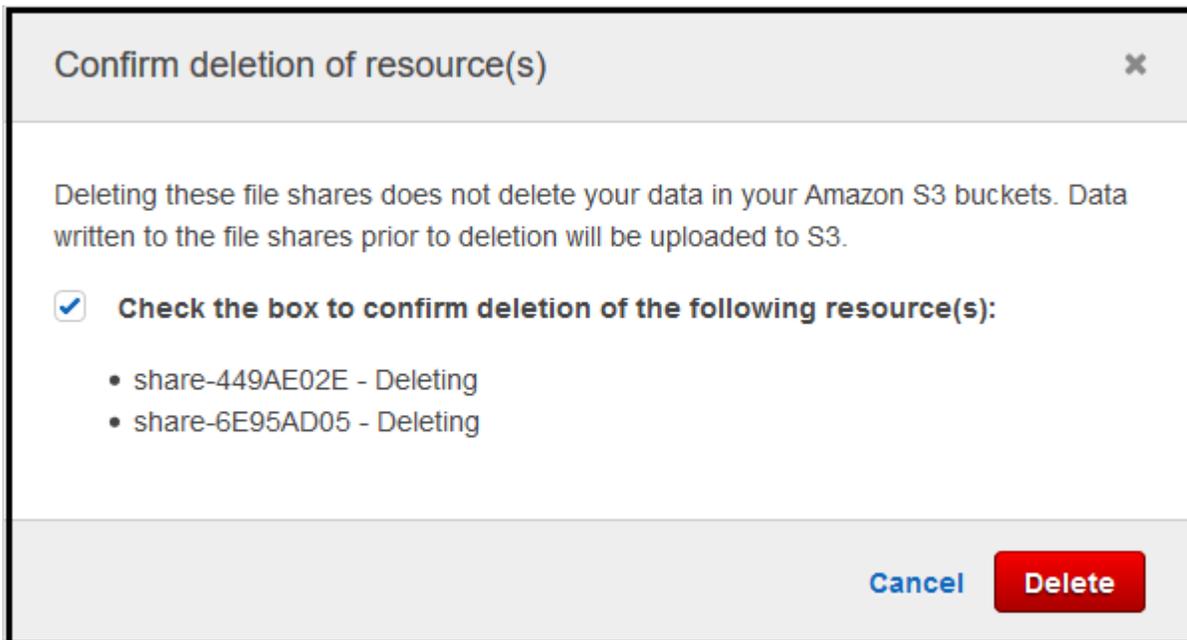
Si vous n'avez plus besoin d'un partage de fichiers, vous pouvez le supprimer de la console Storage Gateway. Lorsque vous supprimez un partage de fichiers, la passerelle est détachée du compartiment Amazon S3 auquel le partage de fichiers est mappé. Toutefois, le compartiment S3 et son contenu ne sont pas supprimés.

Si votre passerelle charge des données dans un compartiment S3 lorsque vous supprimez un partage de fichiers, le processus de suppression ne se termine pas tant que toutes les données ne sont pas chargées. Le partage de fichiers reste dans l'état SUPPRESSION tant que toutes les données ne sont pas complètement chargées.

Si vous voulez que vos données soient complètement chargées, utilisez la procédure suivante Pour supprimer un partage de fichiers. Si vous ne souhaitez pas attendre que vos données soient entièrement chargées, reportez-vous à la procédure Pour supprimer de force un partage de fichiers plus loin dans cette rubrique.

Pour supprimer un partage de fichiers

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Partages de fichiers, puis le partage de fichiers que vous souhaitez supprimer.
3. En regard de Actions, choisissez Supprimer un partage de fichiers. La boîte de dialogue de confirmation suivante s'affiche.



4. Dans la boîte de dialogue de confirmation, cochez la case pour le ou les partages de fichiers à supprimer, puis choisissez Supprimer.

Dans certains cas, vous pouvez souhaiter ne pas attendre que toutes les données écrites dans les fichiers du partage de fichiers NFS (Network File System) soient chargées avant de supprimer le partage de fichiers. Par exemple, vous pouvez souhaiter supprimer intentionnellement des données qui ont été écrites mais ne sont pas encore chargées. Dans un autre exemple, le compartiment Amazon S3 ou les objets constituant le partage de fichiers peuvent avoir déjà été supprimés, ce qui signifie que le chargement des données spécifiées n'est plus possible.

Dans ce cas, vous pouvez forcer la suppression du partage de fichiers en utilisant le `AWS Management Console` ou le `DeleteFileShareOpération` d'API. Cette opération annule le processus de chargement de données. Dans ce cas, le partage de fichiers passe à l'état `FORCE_DELETING`. Pour forcer la suppression d'un partage de fichiers à partir de la console, consultez la procédure suivante.

Pour forcer la suppression d'un partage de fichiers

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Partages de fichiers et sélectionnez le partage de fichiers dont vous voulez forcer la suppression, puis attendez quelques secondes. Un message de suppression s'affiche sous l'onglet Détails (Détails).

Details

 **This file share is being deleted.**
Data already written to the file share is being uploaded to your Amazon S3 bucket, chrisreesfileshare. If you don't want this data to be uploaded, you can delete the file share immediately.

Check the box to confirm forced deletion of `share-17F2A172`. This operation cannot be undone.

Force delete now

 Note

Vous ne pouvez pas annuler l'opération de suppression de force.

3. Dans le message qui s'affiche sous l'onglet Détails, vérifiez l'ID du partage de fichiers dont vous souhaitez forcer la suppression, sélectionnez la boîte de dialogue de confirmation, puis choisissez Forcer la suppression maintenant.

Vous pouvez aussi utiliser l'opération d'API [DeleteFileShare](#) pour forcer la suppression du partage de fichiers.

Modification des paramètres de votre partage de fichiers NFS

Vous pouvez modifier la classe de stockage de votre compartiment Amazon S3, le nom du partage de fichiers, les métadonnées d'objet, le niveau de squash, l'exportation sous et les paramètres d'actualisation automatisée du cache.

 Note

Vous ne pouvez pas modifier un partage de fichiers existant pour pointer vers un nouveau compartiment ou un nouveau point d'accès, ni pour modifier les paramètres du point de terminaison du VPC. Vous pouvez configurer ces paramètres uniquement lors de la création d'un partage de fichiers.

Pour modifier les paramètres de partage de fichiers

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Partages de fichiers, puis le partage de fichiers que vous souhaitez mettre à jour.
3. Pour Actions, choisissez Modifier les paramètres du partage.
4. Effectuez une ou plusieurs des actions suivantes :

- (Facultatif) Pour **Nom** du partage de fichiers, entrez un nouveau nom pour le partage de fichiers.
- Pour les **Audit logs** (Journaux d'audit), choisissez l'une des options suivantes :
 - Choisissez **Disable logging** (Désactivation de la journalisation).pour désactiver la journalisation.
 - Choisissez **Création d'un nouveau groupe de journaux**pour créer un nouveau journal d'audit.
 - Choisissez **Utilisation d'un groupe de journaux existant**, puis choisissez un journal d'audit existant dans la liste.

Pour de plus amples informations sur les journaux d'audit, veuillez consulter [Comprendre les journaux d'audit de passerelle de fichiers](#).

- (Facultatif) Pour **Actualisation automatisée du cache à partir de S3**, cochez la case et définissez l'heure en jours, heures et minutes pour actualiser le cache du partage de fichiers à l'aide de la fonction **Time To Live (TTL)**. **TTL** correspond à la durée écoulée depuis la dernière actualisation. Une fois l'intervalle **TTL** écoulé, l'accès au répertoire entraîne d'abord l'actualisation du contenu de ce répertoire à partir du compartiment Amazon S3.
- (Facultatif) Pour **Notification du chargement de fichiers**, cochez la case à cocher pour être averti lorsqu'un fichier a été complètement téléchargé sur S3 par la passerelle de fichiers S3. Définir la propriété **Heure d'installation en secondes** pour contrôler le nombre de secondes à attendre après le dernier moment qu'un client a écrit dans un fichier avant de générer un **ObjectUploadedNotification**. Étant donné que les clients peuvent effectuer de nombreuses petites écritures dans des fichiers, il est préférable de définir ce paramètre le plus longtemps possible afin d'éviter de générer plusieurs notifications pour le même fichier dans un petit laps de temps. Pour plus d'informations, consultez [Obtenir une notification de téléchargement de fichiers](#).

 **Note**

Ce paramètre n'a aucun effet sur la synchronisation du chargement de l'objet vers S3, mais uniquement sur le moment de la notification.

- Pour **Classe de stockage** pour les nouveaux objets Choisissez la classe de stockage à utiliser pour les nouveaux objets créés dans votre compartiment Amazon S3 :
 - Choisissez **S3 Standard** pour stocker vos données d'objet fréquemment consultées de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les

unes des autres. Pour de plus amples informations sur la classe de stockage S3 Standard, consultez [Classes de stockage pour les objets fréquemment consultés](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.

- Choisissez S3 Intelligent-Tiering (Hiérarchisation intelligente S3) pour optimiser les coûts de stockage en transférant automatiquement les données vers le niveau d'accès de stockage le plus économique. Pour de plus amples informations sur la classe de stockage S3 Intelligent-Tiering, consultez [Classe de stockage pour optimiser automatiquement les objets à accès fréquent et peu fréquent](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.
- Choisissez S3 Standard-IA pour stocker vos données d'objet consultées occasionnellement de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les unes des autres. Pour de plus amples informations sur la classe de stockage S3 Standard-IA, consultez [Classes de stockage pour les objets à accès peu fréquent](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.
- Choisissez S3 One Zone_IA pour stocker vos données d'objet consultées occasionnellement dans une seule zone de disponibilité. Pour de plus amples informations sur la classe de stockage S3 One Zone-IA, consultez [Classes de stockage pour les objets à accès peu fréquent](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.
- Pour Métadonnées d'objet, choisissez les métadonnées que vous souhaitez utiliser :
 - Choisissez Deviner le type MIME pour activer la détermination du type MIME pour les objets chargés à partir des extensions de fichier.
 - Choisissez Give bucket owner full control (Accorder le contrôle total au propriétaire du compartiment) pour donner le contrôle total au propriétaire du compartiment S3 mappé sur le partage de fichiers NFS/SMB. Pour plus d'informations sur l'utilisation de votre partage de fichiers pour accéder aux objets figurant dans un compartiment appartenant à un autre compte, consultez [Utilisation d'un partage de fichiers pour l'accès entre comptes](#).
 - Choisissez Activer le paiement par le demandeur si vous utilisez ce partage de fichiers sur un compartiment qui exige que le demandeur ou le lecteur paie les frais d'accès au lieu du propriétaire du compartiment. Pour de plus amples informations, consultez [Compartiments de type Paiement par le demandeur](#).
- Pour Niveau Squash, choisissez le paramètre de niveau d'écrasement souhaité pour votre partage de fichiers NFS, puis choisissez Enregistrer.

Note

Vous pouvez choisir un paramètre de niveau d'écrasement pour les partages de fichiers NFS uniquement. Les partages de fichiers SMB n'utilisent pas les paramètres d'écrasement.

Les valeurs possibles sont les suivantes :

- Ecrasement racine (par défaut) : l'accès pour le super-utilisateur distant (racine) est mappé à UID (65534) et à GID (65534).
- Aucun écrasement racine – Le superuser distant (root) reçoit un accès root.
- All squash : tout l'accès utilisateur est mappé à l'UID (65534) et au GID (65534).

La valeur par défaut pour le niveau d'écrasement est Root squash (Écrasement racine).

- Pour Exporter de sous, choisissez une option pour votre partage de fichiers. La valeur par défaut est Lecture/écriture.

Note

Pour les partages de fichiers montés sur un client Microsoft Windows, si vous sélectionnez l'option Lecture seule pour Exportez en tant que, vous pouvez voir un message d'erreur indiquant qu'une erreur imprévue vous empêche de créer le dossier. Ce message d'erreur est problème connu lié à NFS version 3. Vous pouvez ignorer le message.

5. Choisissez Save (Enregistrer).

Modification des métadonnées par défaut pour votre partage de fichiers NFS

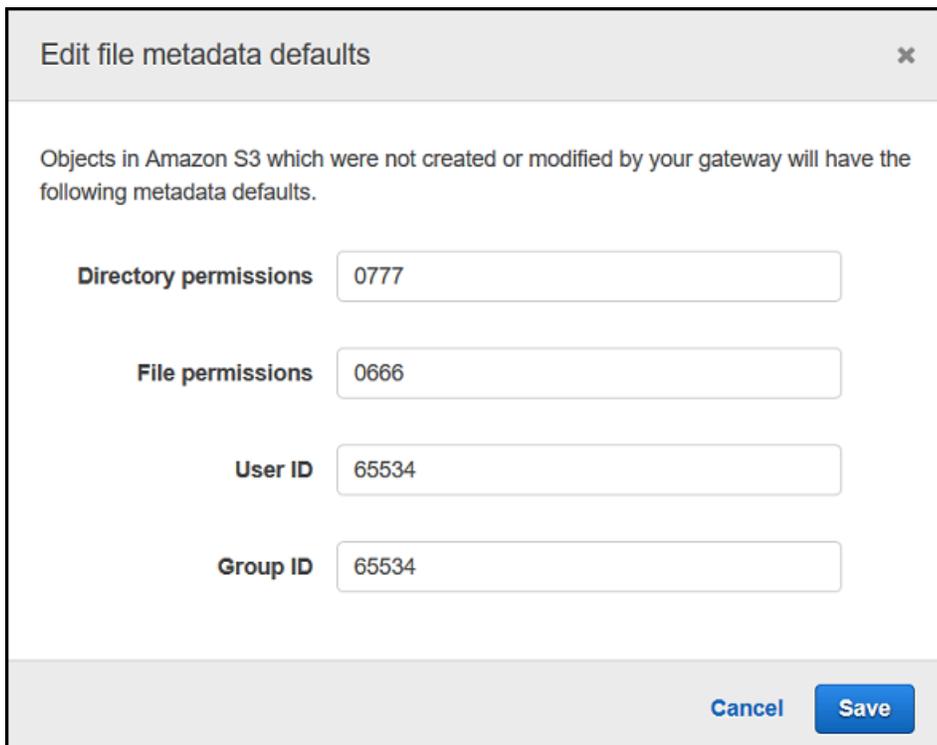
Si vous ne définissez pas les valeurs de métadonnées pour vos fichiers ou répertoires dans votre compartiment, votre passerelle de fichiers S3 définit les valeurs de métadonnées par défaut. Ces valeurs incluent des autorisations Unix pour les fichiers et dossiers. Vous pouvez modifier les métadonnées par défaut dans la console Storage Gateway.

Quand la passerelle de fichiers S3 stocke des fichiers et des dossiers dans Amazon S3, les autorisations sur les fichiers Unix sont stockées dans des métadonnées d'objet. Quand la passerelle de fichiers S3 découvre des objets qui n'étaient pas stockés par la passerelle de fichiers S3, des autorisations sur les fichiers Unix par défaut leur sont attribuées. Le tableau suivant présente les autorisations Unix par défaut.

Metadonnées	Description
Autorisations sur le répertoire	Le mode de répertoire Unix sous la forme « nnnn ». Par exemple, « 0666 » représente le mode d'accès pour tous les répertoires au sein du partage de fichiers. La valeur par défaut est 0777.
Autorisations de fichiers	Le mode de fichier Unix sous la forme « nnnn ». Par exemple, « 0666 » représente le mode de fichier au sein du partage de fichiers. La valeur par défaut est 0666.
ID de l'utilisateur	ID de propriétaire par défaut pour les fichiers situés dans le partage de fichiers. La valeur par défaut est 65534.
ID du groupe	ID de groupe par défaut pour le partage de fichiers. La valeur par défaut est 65534.

Pour modifier les métadonnées par défaut

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Partages de fichiers, puis le partage de fichiers que vous souhaitez mettre à jour.
3. Pour Actions, choisissez Modifier les métadonnées.
4. Dans la boîte de dialogue Modifier les métadonnées, fournissez les informations sur les métadonnées et choisissez Enregistrer.



Edit file metadata defaults ✕

Objects in Amazon S3 which were not created or modified by your gateway will have the following metadata defaults.

Directory permissions

File permissions

User ID

Group ID

Cancel **Save**

Modification des paramètres d'accès de votre partage de fichiers NFS

Nous vous recommandons de modifier les paramètres de client NFS autorisé pour votre partage de fichiers NFS. Si vous ne le faites pas, tout client de votre réseau peut effectuer un montage sur votre partage de fichiers.

Pour modifier les paramètres d'accès NFS

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Partages de fichiers, puis le partage de fichiers NFS que vous souhaitez modifier.
3. Pour Actions, choisissez Edit share access settings (Modifier les paramètres de partage d'accès).
4. Dans Modifier les clients autorisés, choisissez Ajouter une entrée, fournissez l'adresse IP ou la notation CIDR pour les clients dont vous voulez autoriser l'accès, puis choisissez Enregistrer.

Modification des paramètres SMB pour une passerelle

Les paramètres SMB au niveau de la passerelle vous permettent de configurer la stratégie de sécurité, l'authentification Active Directory, l'accès invité, les autorisations de groupe local et la visibilité du partage de fichiers pour les partages de fichiers SMB sur une passerelle.

Pour modifier les paramètres SMB au niveau de la passerelle

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Passerelles, puis choisissez la passerelle dont vous souhaitez modifier les paramètres SMB.
3. De la Actions, choisissez Modifier les paramètres SMB, puis choisissez les paramètres que vous voulez modifier.

Pour plus d'informations, consultez les rubriques suivantes.

Rubriques

- [Définition d'un niveau de sécurité pour votre passerelle](#)
- [Utilisation d'Active Directory pour authentifier les utilisateurs](#)
- [Fourniture d'un accès invité à votre partage de fichiers](#)
- [Configurez les groupes locaux pour votre passerelle](#)
- [Définition de la visibilité du partage de fichiers](#)

Définition d'un niveau de sécurité pour votre passerelle

En utilisant une passerelle de fichiers S3, vous pouvez spécifier un niveau de sécurité pour votre passerelle. En spécifiant ce niveau de sécurité, vous pouvez définir si votre passerelle doit exiger une connexion SMB (Server Message Block) ou un chiffrement SMB, ou si vous souhaitez activer SMB version 1.

Pour configurer un niveau de sécurité

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Passerelles, puis choisissez la passerelle dont vous souhaitez modifier les paramètres SMB.

3. De la Actions, choisissez Modifier les paramètres SMB, puis Paramètres de sécurité SMB.
4. Pour Security level (Niveau de sécurité), choisissez l'une des actions suivantes :

 Note

Ce paramètre est appelé `SMBSecurityStrategy` dans la référence de l'API.
Un haut niveau de sécurité peut avoir un impact sur les performances.

- Appliquez le chiffrement— Si vous choisissez cette option, la passerelle de fichiers S3 autorise uniquement les connexions depuis des clients SMBv3 avec chiffrement activé. Cette option est vivement recommandée pour les environnements qui gèrent des données sensibles. Cette option fonctionne avec les clients SMB sur Microsoft Windows 8, Windows Server 2012 ou version ultérieure.
- Appliquez la signature— Si vous choisissez cette option, la passerelle de fichiers S3 autorise uniquement les connexions depuis des clients SMB2 ou SMBv3 avec signature activée. Cette option fonctionne avec les clients SMB sur Microsoft Windows Vista, Windows Server 2008 ou version ultérieure.
- Négociation du client— Si vous choisissez cette option, les demandes sont établies en fonction de ce qui est négocié par le client. Cette option est recommandée lorsque vous souhaitez maximiser la compatibilité entre plusieurs clients de votre environnement.

 Note

Pour les passerelles activées avant le 20 juin 2019, le niveau de sécurité par défaut est Client negotiated (Négocié par le client).

Pour les passerelles activées à partir du 20 juin 2019, le niveau de sécurité par défaut est Enforce encryption (Appliquer le chiffrement).

5. Choisissez Save (Enregistrer).

Utilisation d'Active Directory pour authentifier les utilisateurs

Pour utiliser votre accès utilisateur authentifié pour le système Active Directory d'entreprise pour accéder à votre partage de fichiers SMB, modifiez les paramètres SMB pour votre passerelle avec vos informations d'identification de domaine Microsoft AD. Cela permet à votre passerelle

de rejoindre votre domaine Active Directory et d'autoriser les membres du domaine à accéder au partage de fichiers SMB.

 Note

Utilisation d'AWS Directory Service, vous pouvez créer un service de domaine Active Directory hébergé dans leAWS Cloud.

Toute personne pouvant fournir le mot de passe correct obtient un accès invité au partage de fichiers SMB.

Vous pouvez également activer les listes de contrôle d'accès (ACL) sur votre partage de fichiers SMB. Pour plus d'informations sur l'activation des listes ACL, consultez [Utilisation des listes ACL Microsoft Windows pour contrôler l'accès à un partage de fichiers SMB](#).

Pour activer l'authentification Active Directory

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Passerelles, puis choisissez la passerelle dont vous souhaitez modifier les paramètres SMB.
3. De la Actions dans le menu déroulant, choisissez Modifier les paramètres SMB, puis Paramètres Active Directory.
4. Pour Domain name (Nom du domaine), indiquez le domaine que vous voulez que la passerelle rejoigne. Vous pouvez joindre un domaine à l'aide de son adresse IP ou de son unité organisationnelle. Une unité organisationnelle est une sous-division Active Directory qui peut contenir des utilisateurs, des groupes, des ordinateurs et d'autres unités d'organisation.

 Note

Si votre passerelle ne peut pas rejoindre un répertoire Active Directory, essayez la jonction avec l'adresse IP du répertoire à l'aide de l'opération d'API [JoinDomain](#).

 Note

L'état Active Directory indique Detached (Détaché) lorsqu'une passerelle n'a jamais rejoint un domaine.

5. Indiquez le nom d'utilisateur et le mot de passe pour le domaine, puis choisissez Save (Enregistrer).

Un message en haut de la section Gateways (Passerelles) de votre console indique que votre passerelle a rejoint votre domaine AD.

Pour limiter l'accès au partage de fichiers à des utilisateurs et des groupes AD

1. Dans la console Storage Gateway, choisissez le partage de fichiers auquel vous voulez limiter l'accès.
2. De la Actions dans le menu déroulant, choisissez Modifier les paramètres d'accès au partage de fichiers.
3. Dans Accès au partage de fichiers utilisateur et de groupe, choisissez vos paramètres.

Pour Utilisateurs et groupes autorisés, choisissez Ajout d'un utilisateur autorisé ou Ajout d'un groupe autorisé et entrez un utilisateur ou un groupe AD que vous voulez autoriser l'accès au partage de fichiers. Répétez cette procédure pour autoriser autant d'utilisateurs et de groupes que nécessaire.

Pour Utilisateurs et groupes refusés, choisissez Ajout d'un utilisateur refusé ou Ajout d'un groupe refusé et entrez un utilisateur ou un groupe AD que vous voulez refuser l'accès au partage de fichiers. Répétez cette procédure pour refuser autant d'utilisateurs et de groupes que nécessaire.

 Note

Le Accès au partage de fichiers utilisateur et de groupes affiche uniquement si Active Directory est sélectionné.

Entrez uniquement le nom d'utilisateur ou de groupe AD. Le nom de domaine est induit par l'appartenance de la passerelle à l'Active Directory spécifique auquel celle-ci est jointe.

Si vous ne spécifiez aucun utilisateur ou groupe autorisé ou refusé, tout utilisateur AD authentifié peut exporter le partage de fichiers.

4. Une fois l'ajout d'entrées terminé, choisissez Save (Enregistrer).

Fourniture d'un accès invité à votre partage de fichiers

Si vous souhaitez fournir uniquement un accès invité, votre passerelle de fichiers S3 n'a pas besoin de faire partie d'un domaine Microsoft AD. Vous pouvez également utiliser une passerelle de fichiers S3 membre d'un domaine AD pour créer des partages de fichiers avec un accès invité. Avant de créer un partage de fichiers via un accès invité, vous devez modifier le mot de passe par défaut.

Pour modifier le mot de passe d'accès invité

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Passerelles, puis choisissez la passerelle dont vous souhaitez modifier les paramètres SMB.
3. De la Actions dans le menu déroulant, choisissez Modifier les paramètres SMB, puis Paramètres d'accès des clients.
4. Pour Mot de passe, fournissez un mot de passe, puis choisissez Enregistrer.

Configurez les groupes locaux pour votre passerelle

Les paramètres de groupe local vous permettent d'accorder aux utilisateurs ou aux groupes Active Directory des autorisations spéciales pour les partages de fichiers SMB sur votre passerelle.

Vous pouvez utiliser les paramètres de groupe local pour attribuer des autorisations d'administrateur de passerelle. Les administrateurs de passerelle peuvent utiliser le composant logiciel enfichable Dossiers partagés Microsoft Management Console pour forcer la fermeture des fichiers ouverts et verrouillés.

Note

Vous devez ajouter au moins un utilisateur ou un groupe Admin de passerelle avant de pouvoir rejoindre votre passerelle à un domaine Active Directory.

Pour attribuer des administrateurs de passerelle

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Passerelles, puis choisissez la passerelle dont vous souhaitez modifier les paramètres SMB.
3. De la Actions, choisissez Modifier les paramètres SMB, puis Paramètres du groupe local.
4. Dans Paramètres du groupe local, choisissez vos paramètres. Cette section s'affiche uniquement pour les partages de fichiers qui utilisent Active Directory.

Pour Gateway Admins, ajoutez des utilisateurs et des groupes Active Directory auxquels vous souhaitez accorder des autorisations d'administrateur de passerelle locale. Ajoutez un utilisateur ou un groupe par ligne, y compris le nom de domaine. Par exemple, **corp\Domain Admins**. Pour créer des lignes supplémentaires, choisissez Ajouter un nouvel administrateur de passerelle.

Note

La modification des administrateurs de passerelle déconnecte et reconnecte tous les partages de fichiers SMB.

5. Choisissez Enregistrez les modifications, puis Continuer pour accuser réception du message d'avertissement qui s'affiche.

Définition de la visibilité du partage de fichiers

La visibilité des partages de fichiers contrôle si les partages d'une passerelle sont visibles lors de la mise en vente des partages aux utilisateurs.

Pour définir la visibilité du partage de fichiers

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Passerelles, puis choisissez la passerelle dont vous souhaitez modifier les paramètres SMB.
3. De la Actions dans le menu déroulant, choisissez Modifier les paramètres SMB, puis Paramètres de visibilité du partage de fichiers.
4. Pour Statut de visibilité, activez la case à cocher pour que les partages sur cette passerelle apparaissent lors de la mise en vente des partages aux utilisateurs. Conservez la case à cocher

pour que les partages de cette passerelle n'apparaissent pas lorsque vous mettez en vente des partages aux utilisateurs.

Modification des paramètres de votre partage de fichiers SMB

Une fois que vous avez créé un partage de fichiers SMB, vous pouvez modifier la classe de stockage de votre compartiment Amazon S3, les métadonnées d'objet, la sensibilité à la casse, l'énumération basée sur l'accès, les journaux d'audit, l'actualisation automatique du cache et l'exportation en tant que paramètres pour votre partage de fichiers.

Note

Vous ne pouvez pas modifier un partage de fichiers existant pour pointer vers un nouveau compartiment ou un nouveau point d'accès, ni pour modifier les paramètres du point de terminaison du VPC. Vous pouvez configurer ces paramètres uniquement lors de la création d'un partage de fichiers.

Pour modifier les paramètres de partage de fichiers SMB

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Partages de fichiers, puis le partage de fichiers que vous souhaitez mettre à jour.
3. Pour Actions, choisissez Modifier les paramètres du partage.
4. Effectuez une ou plusieurs des actions suivantes :
 - (Facultatif) Pour Nom du partage de fichiers, entrez un nouveau nom pour le partage de fichiers.
 - Pour les Audit logs (Journaux d'audit), choisissez l'une des options suivantes :
 - Choisissez Disable logging (Désactivation de la journalisation) pour désactiver la journalisation.
 - Choisissez Création d'un nouveau groupe de journaux pour créer un nouveau journal d'audit.
 - Choisissez Utilisation d'un groupe de journaux existant, puis choisissez un journal d'audit existant dans la liste.

Pour de plus amples informations sur les journaux d'audit, veuillez consulter [Comprendre les journaux d'audit de passerelle de fichiers](#).

- (Facultatif) Pour Actualisation automatisée du cache à partir de S3 après, cochez la case et définissez l'heure en jours, heures et minutes pour actualiser le cache du partage de fichiers à l'aide de la fonction Time To Live (TTL). TTL correspond à la durée écoulée depuis la dernière actualisation. Une fois l'intervalle TTL écoulé, l'accès au répertoire entraîne d'abord l'actualisation du contenu de ce répertoire à partir du compartiment Amazon S3.
- (Facultatif) Pour Notification du chargement de fichiers, cochez la case à cocher pour être averti lorsqu'un fichier a été complètement téléchargé sur S3 par la passerelle de fichiers S3. Définir la propriété Heure d'installation en secondes pour contrôler le nombre de secondes à attendre après le dernier moment qu'un client a écrit dans un fichier avant de générer un `ObjectUploadedNotification`. Étant donné que les clients peuvent effectuer de nombreuses petites écritures dans des fichiers, il est préférable de définir ce paramètre le plus longtemps possible afin d'éviter de générer plusieurs notifications pour le même fichier dans un petit laps de temps. Pour plus d'informations, consultez [Obtenir une notification de téléchargement de fichiers](#).

 Note

Ce paramètre n'a aucun effet sur la synchronisation du chargement de l'objet vers S3, mais uniquement sur le moment de la notification.

- Pour Classe de stockage pour les nouveaux objets, choisissez la classe de stockage à utiliser pour les nouveaux objets créés dans votre compartiment Amazon S3 :
 - Choisissez S3 Standard pour stocker vos données d'objet fréquemment consultées de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les unes des autres. Pour de plus amples informations sur la classe de stockage S3 Standard, consultez [Classes de stockage pour les objets fréquemment consultés](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.
 - Choisissez S3 Intelligent-Tiering (Hiérarchisation intelligente S3) pour optimiser les coûts de stockage en transférant automatiquement les données vers le niveau d'accès de stockage le plus économique. Pour de plus amples informations sur la classe de stockage S3 Intelligent-Tiering, consultez [Classe de stockage pour optimiser automatiquement les objets à accès fréquent et peu fréquent](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.
 - Choisissez S3 Standard-IA pour stocker vos données d'objet consultées occasionnellement de manière redondante dans plusieurs zones de disponibilité géographiquement séparées les unes des autres. Pour de plus amples informations sur la classe de stockage S3

Standard-IA, consultez [Classes de stockage pour les objets à accès peu fréquent](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.

- Choisissez S3 One Zone_IA pour stocker vos données d'objet consultées occasionnellement dans une seule zone de disponibilité. Pour de plus amples informations sur la classe de stockage S3 One Zone-IA, consultez [Classes de stockage pour les objets à accès peu fréquent](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.
- Pour Métadonnées d'objet, choisissez les métadonnées que vous souhaitez utiliser :
 - Choisissez Deviner le type MIME pour activer la détermination du type MIME pour les objets chargés à partir des extensions de fichier.
 - Choisissez Give bucket owner full control (Accorder le contrôle total au propriétaire du compartiment) pour donner le contrôle total au propriétaire du compartiment S3 mappé sur le partage de fichiers NFS/SMB. Pour plus d'informations sur l'utilisation de votre partage de fichiers pour accéder aux objets figurant dans un compartiment appartenant à un autre compte, consultez [Utilisation d'un partage de fichiers pour l'accès entre comptes](#).
 - Choisissez Activer le paiement par le demandeur si vous utilisez ce partage de fichiers sur un compartiment qui exige que le demandeur ou le lecteur paie les frais d'accès au lieu du propriétaire du compartiment. Pour de plus amples informations, consultez [Compartiments de type Paiement par le demandeur](#).
- Pour Exporter de sous, choisissez une option pour votre partage de fichiers. La valeur par défaut est Lecture/écriture.

 Note

Pour les partages de fichiers montés sur un client Microsoft Windows, si vous sélectionnez Lecture seule pour Exporter de sous Vous pouvez voir un message d'erreur indiquant qu'une erreur imprévue vous empêche de créer le dossier. Ce message d'erreur est problème connu lié à NFS version 3. Vous pouvez ignorer le message.

- Pour File/directory access controlled by (Accès fichier/répertoire contrôlé par), choisissez l'une des options suivantes ::
 - Choisissez Windows Access Control List (Liste ACL Windows) pour définir des autorisations précises sur les fichiers et les dossiers dans votre partage de fichiers SMB. Pour plus d'informations, consultez [Utilisation des listes ACL Microsoft Windows pour contrôler l'accès à un partage de fichiers SMB](#).

- Choisissez POSIX permissions (Autorisations POSIX) pour utiliser les autorisations POSIX afin de contrôler l'accès aux fichiers et répertoires stockés via un partage de fichiers NFS ou SMB.

Si votre méthode d'authentification est Active Directory, pour Utilisateurs/groupes d'administrateurs, entrez une liste séparée par des virgules d'utilisateurs et de groupes AD. Cela permet de donner à un utilisateur administrateur de disposer des privilèges requis pour mettre à jour les listes ACL sur tous les fichiers et dossiers du partage de fichiers. Ces utilisateurs et groupes ont alors des droits d'administrateur sur le partage de fichiers. Un groupe doit comporter le préfixe du @personnage, par exemple, @group1.

- Pour Sensibilité à la casse, activez la case à cocher pour permettre à la passerelle de contrôler la sensibilité à la casse ou désactivez la case à cocher pour permettre au client de contrôler la sensibilité à la casse.

Note

- Si vous activez cette case à cocher, ce paramètre s'applique immédiatement aux nouvelles connexions client SMB. Les connexions client SMB existantes doivent se déconnecter du partage de fichiers et se reconnecter pour que le paramètre prenne effet.
- Si vous désactivez cette case à cocher, ce paramètre peut entraîner la perte d'accès à des fichiers dont les noms ne diffèrent que dans leur cas.

- Pour Énumération basée sur l'accès, activez la case à cocher pour que les fichiers et dossiers du partage soient visibles uniquement par les utilisateurs ayant accès en lecture. Gardez la case à cocher désactivée pour rendre les fichiers et dossiers du partage visibles par tous les utilisateurs pendant l'énumération des répertoires.

Note

L'énumération basée sur l'accès est un système qui filtre l'énumération des fichiers et des dossiers sur un partage de fichiers SMB en fonction des listes de contrôle d'accès (ACL) du partage.

- Pour Serrure opportuniste (oplock), choisissez l'une des options suivantes :
 - Choisissez Activé pour permettre au partage de fichiers d'utiliser un verrouillage opportuniste pour optimiser la stratégie de mise en mémoire tampon des fichiers, ce qui améliore

les performances dans la plupart des cas, en particulier en ce qui concerne les menus contextuels Windows.

- Choisissez **Désactivé** pour empêcher l'utilisation d'un verrouillage opportuniste. Si plusieurs clients Windows de votre environnement modifient fréquemment les mêmes fichiers simultanément, la désactivation du verrouillage opportuniste peut parfois améliorer les performances.

Note

L'activation du verrouillage opportuniste sur les partages sensibles à la casse n'est pas recommandée pour les charges de travail qui impliquent l'accès à des fichiers portant le même nom dans des cas différents.

5. Choisissez **Save changes** (Enregistrer les modifications).

Actualisation des objets dans votre compartiment Amazon S3

Lorsque votre client NFS ou SMB réalise des opérations sur le système de fichiers, votre passerelle gère un inventaire des objets contenus dans un compartiment S3 associé à votre partage de fichiers. Votre passerelle utilise cet inventaire mis en cache pour diminuer la latence et la fréquence des demandes S3. Cette opération n'importe pas de fichiers dans le stockage de cache de la passerelle de fichiers S3. Il met uniquement à jour l'inventaire mis en cache pour refléter les modifications apportées à l'inventaire des objets du compartiment S3.

Pour actualiser le compartiment S3 pour votre partage de fichiers, vous pouvez utiliser la console Storage Gateway, la [RefreshCached](#) dans l'API Storage Gateway, ou dans un AWS Lambda.

Pour actualiser les objets d'un compartiment S3 à partir de la console

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez **Partages de fichiers**, puis le partage de fichiers associé au compartiment S3 que vous souhaitez actualiser.
3. Pour **Actions**, sélectionnez **Actualiser le cache**.

La durée du processus d'actualisation dépend du nombre d'objets mis en cache sur la passerelle et du nombre d'objets qui ont été ajoutés au compartiment S3 ou supprimés de celui-ci.

Pour actualiser des objets dans un compartiment S3 à l'aide d'unAWS Lambda fonction

1. Identifiez le compartiment S3 utilisé par la passerelle de fichiers S3.
2. Vérifiez que le Événement est vide. Il se remplit automatiquement ultérieurement.
3. Créer un rôle IAM et autoriser la relation de confiance pour Lambda `lambda.amazonaws.com`.
4. Utilisez la stratégie suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "StorageGatewayPermissions",
      "Effect": "Allow",
      "Action": "storagegateway:RefreshCache",
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchLogsPermissions",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:CreateLogGroup",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

5. Créez une fonction Lambda à partir de la console Lambda.
6. Utilisez la fonction suivante pour votre tâche Lambda.

```
import json
import boto3
client = boto3.client('storagegateway')
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406774878:share/
share-E51FBD9C'
    )
```

```
print(response)
return 'Your FileShare cache has been refreshed'
```

7. Pour Rôle d'exécution, choisissez le rôle IAM que vous avez créé.
8. Facultatif : ajoutez un déclencheur pour Amazon S3 et sélectionnez l'événement `ObjectCreated` ou `ObjectRemoved`.

Note

`RefreshCache` doit terminer un processus avant d'en commencer un autre. Lorsque vous créez ou supprimez de nombreux objets dans un compartiment, les performances peuvent se dégrader. Par conséquent, nous vous recommandons de ne pas utiliser les déclencheurs S3. Utilisez plutôt la règle Amazon CloudWatch décrite ci-dessous.

9. Créez une règle CloudWatch sur la console CloudWatch et ajoutez une planification. En général, nous recommandons un `fixeDe` de 30 minutes. Cependant, vous pouvez utiliser 1 à 2 heures sur un grand compartiment S3.
10. Ajoutez un nouveau déclencheur pour les événements CloudWatch et choisissez la règle que vous venez de créer.
11. Enregistrez votre configuration Lambda. Choisissez `Test`.
12. Choisissez `S3 MI` Set personnalisez le test selon vos besoins.
13. Le test doit réussir. Si ce n'est pas le cas, modifiez le JSON en fonction de vos besoins et retestez.
14. Ouvrez la console Amazon S3 et vérifiez que l'événement que vous avez créé et l'ARN de la fonction Lambda sont présents.
15. Charger un objet dans le compartiment S3 à l'aide de la console Amazon S3 ou de la `AWS CLI`.

La console CloudWatch génère une sortie CloudWatch similaire à la sortie suivante.

```
{
  u'Records': [
    {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
    u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
    u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
    u'object': {u'sequenceNumber': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
    u'bucket': {u'arn': u'arn:aws:s3:::MY-BUCKET', u'name': u'MY-GATEWAY-
    NAME', u'ownerIdentity': {u'principalId': u'A30KNBZ72HVPP9'}}, u's3SchemaVersion':
    u'1.0'},
```

```

    u'responseElements': {u'x-amz-id-2':
u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsgdgsq+IhvAg5M=',
u'x-amz-request-id': u'651C2D4101D31593'},
    u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
u'eventSource': u'aws:s3'}
  ]
}

```

L'invocation Lambda vous donne des résultats similaires à ce qui suit.

```

{
  u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
  'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
  'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
  'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
  }
}
}

```

Votre partage NFS monté sur votre client reflétera cette mise à jour.

Note

Pour les caches qui mettent à jour la création ou la suppression d'objets volumineux dans de grands compartiments contenant des millions d'objets, les mises à jour peuvent prendre des heures.

16. Supprimez votre objet manuellement à l'aide de la console Amazon S3 ou AWS CLI.
17. Affichez le partage NFS monté sur votre client. Vérifiez que votre objet a disparu (car votre cache a été actualisé).
18. Vérifiez vos journaux CloudWatch pour voir le journal de votre suppression avec l'événement `ObjectRemoved:Delete`.

```
{
```

```
u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-  
type': u'Scheduled Event', u'source': u'aws.events',  
u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':  
u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',  
u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']  
}
```

Note

Pour les tâches cron ou les tâches planifiées, votre événement CloudWatch log est u'detail-type': u'Scheduled Event'.

L'actualisation du cache ne faut que lancer l'opération d'actualisation. Lorsque l'actualisation du cache est terminée, cela ne signifie pas nécessairement que l'actualisation du fichier est terminée. Pour déterminer si l'opération d'actualisation du fichier est terminée avant de rechercher de nouveaux fichiers sur le partage de fichiers de la passerelle, utilisez la notification `refresh-complete`. Pour cela, vous pouvez vous abonner à la réception d'une notification via un événement Amazon CloudWatch lorsque votre [RefreshCache](#) l'opération est terminée. Pour plus d'informations, consultez [Réception de notifications sur les opérations de fichiers](#).

Utilisation de la fonctionnalité de verrouillage des objets S3 avec une passerelle de fichiers Amazon S3

Amazon S3 File Gateway prend en charge l'accès aux compartiments S3 pour lesquels le verrouillage des objets Amazon S3 est activé. Le verrouillage des objets Amazon S3 vous permet de stocker des objets selon un modèle « Write Once Read Many » (WORM). Lorsque vous utilisez le verrouillage des objets Amazon S3, vous pouvez empêcher la suppression ou le remplacement d'un objet dans votre compartiment S3. Le verrouillage des objets Amazon S3 fonctionne conjointement avec le contrôle de version d'objet pour protéger vos données.

Si vous activez le verrouillage des objets Amazon S3, vous pouvez toujours modifier l'objet. Par exemple, il est possible d'y inscrire des données, supprimées ou renommées via un partage de fichiers sur une passerelle de fichiers S3. Lorsque vous modifiez un objet de cette façon, la passerelle de fichiers S3 place une nouvelle version de l'objet sans affecter la version précédente (c'est-à-dire l'objet verrouillé).

Par exemple, si vous utilisez la passerelle de fichiers S3 NFS ou l'interface SMB pour supprimer un fichier et si l'objet S3 correspondant est verrouillé, la passerelle place un marqueur de suppression S3 en tant que la prochaine version de l'objet et laisse la version d'objet initiale en place. De la même manière, si une passerelle de fichiers S3 modifie le contenu ou les métadonnées d'un objet verrouillé, une nouvelle version de l'objet est chargée avec les modifications, mais la version de l'objet verrouillé d'origine reste inchangée.

Pour de plus amples informations sur la fonctionnalité de verrouillage des objets Amazon S3, veuillez consulter [Verrouillage d'objets avec la fonctionnalité de verrouillage des objets S3](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.

Comprendre l'état du partage de fichiers

Chaque partage de fichiers est associé à un état qui vous indique rapidement l'intégrité du partage de fichiers. La plupart du temps, l'état indique que le partage de fichiers fonctionne normalement et qu'aucune action de votre part n'est nécessaire. Dans certains cas, l'état indique un problème qui exige ou non une action de votre part.

Vous pouvez voir l'état du partage de fichiers sur la console Storage Gateway. Celui-ci s'affiche dans la colonne Status (État) pour chaque partage de fichiers dans votre passerelle. Un partage de fichiers qui fonctionne normalement a l'état DISPONIBLE.

Le tableau suivant décrit chaque état du partage de fichiers et indique si vous devez intervenir en fonction de l'état. Un partage de fichiers doit avoir l'état DISPONIBLE en permanence ou la plupart du temps lorsqu'il est utilisé.

État	Signification
DISPONIBLE	Le partage de fichiers est correctement configuré et est disponible pour l'utilisation. L'état AVAILABLE est l'état d'exécution normal d'un partage de fichiers.
CREATION	Le partage de fichiers est en cours de création et ne peut pas encore être utilisé. L'état CREATION est transitionnel. Aucune action n'est requise. Si le partage de fichiers est bloqué dans cet état, c'est probablement parce que l'ordinateur virtuel de la passerelle a perdu la connexion à AWS.

État	Signification
UPDATING	La configuration du partage de fichier est en cours de mise à jour. Si un partage de fichiers est bloqué dans cet état, c'est probablement parce que l'ordinateur virtuel de la passerelle a perdu la connexion àAWS.
SUPPRESSION	Le partage de fichiers est en cours de suppression. Le partage de fichiers n'est pas supprimé tant que toutes les données ne sont pas chargées surAWS. L'état DELETING est transitionnel et aucune action est requise.
FORCE_DELETING	Le partage de fichiers est en cours de suppression forcée. Le partage de fichiers est supprimé immédiatement et le chargement surAWSest avorté. L'état FORCE_DELETING est transitionnel et aucune action n'est requise.
UNAVAILABLE	Le partage de fichiers est dans un état non sain. À la suite de certains problèmes, le partage de fichiers peut passer à un état non sain, Par exemple, à la suite d'erreurs affectant les stratégies de rôle ou si le partage de fichiers est mappé à un compartiment Amazon S3 qui n'existe pas. Une fois que le problème qui a provoqué l'état non sain est résolu, le fichier retourne à l'état AVAILABLE.

Bonnes pratiques de partage de fichiers

Dans cette section, vous trouverez de plus amples informations sur les bonnes pratiques en matière de création de partages de fichiers.

Rubriques

- [Empêcher l'écriture de plusieurs partages de fichiers dans votre compartiment Amazon S3](#)
- [Autoriser des clients NFS spécifiques à monter votre partage de fichiers](#)

Empêcher l'écriture de plusieurs partages de fichiers dans votre compartiment Amazon S3

Lorsque vous créez un partage de fichiers, nous vous recommandons de configurer votre compartiment Amazon S3 de sorte qu'un seul partage de fichiers puisse y écrire. Si vous configurez le compartiment S3 pour que plusieurs partages de fichiers puissent y écrire, des résultats imprévisibles peuvent se produire. Afin d'empêcher cela, créez une stratégie de compartiment S3 qui refuse à tous les rôles, sauf celui utilisé pour le partage de fichiers, de placer ou de supprimer des objets dans le compartiment. Puis, attachez cette stratégie au compartiment S3.

L'exemple de stratégie suivant refuse à tous les rôles, à l'exception de celui qui a créé le compartiment, l'écriture dans le compartiment S3. Les actions `s3:DeleteObject` et `s3:PutObject` sont refusées pour tous les rôles à l'exception de "TestUser". La stratégie s'applique à tous les objets du compartiment `arn:aws:s3:::TestBucket/*`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"DenyMultiWrite",
      "Effect":"Deny",
      "Principal": "*",
      "Action":[
        "s3:DeleteObject",
        "s3:PutObject"
      ],
      "Resource":"arn:aws:s3:::TestBucket/*",
      "Condition":{"
        "StringNotLike":{"
          "aws:userid":"TestUser:*"
        }
      }
    }
  ]
}
```

Autoriser des clients NFS spécifiques à monter votre partage de fichiers

Nous vous recommandons de modifier les paramètres de client NFS autorisé pour votre partage de fichiers. Si vous ne le faites pas, tout client de votre réseau peut monter votre partage de fichiers.

Pour plus d'informations sur la modification de vos paramètres client NFS, consultez [Modification des paramètres d'accès de votre partage de fichiers NFS](#).

Surveillance de la passerelle de fichiers

Vous pouvez surveiller votre passerelle de fichiers et les ressources associées dans AWS Storage Gateway en utilisant les mesures Amazon CloudWatch et les journaux d'audit des partages de fichiers. Vous pouvez également utiliser CloudWatch Events pour recevoir une notification lorsque vos opérations sur les fichiers sont terminées. Pour plus d'informations sur les métriques de type passerelle de fichiers, consultez [Surveillance de la passerelle de fichiers](#).

Rubriques

- [Obtention des journaux d'intégrité de la passerelle de fichiers avec les groupes de journaux CloudWatch](#)
- [Utilisation des métriques Amazon CloudWatch](#)
- [Réception de notifications sur les opérations de fichiers](#)
- [Présentation des métriques de la passerelle](#)
- [Comprendre les mesures de partage de fichiers](#)
- [Comprendre les journaux d'audit de passerelle de fichiers](#)

Obtention des journaux d'intégrité de la passerelle de fichiers avec les groupes de journaux CloudWatch

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir des informations sur l'état de votre passerelle de fichiers et des ressources connexes. Vous pouvez utiliser les journaux pour surveiller votre passerelle afin de détecter les erreurs qu'elle rencontre. En outre, vous pouvez utiliser les filtres d'abonnement Amazon CloudWatch pour automatiser le traitement des informations des journaux en temps réel. Pour de plus amples informations, veuillez consulter [Traitement en temps réel des données de journaux avec les abonnements](#) dans le Guide de l'utilisateur Amazon CloudWatch.

Par exemple, vous pouvez configurer un groupe de journaux CloudWatch pour surveiller votre passerelle et recevoir une notification lorsque votre passerelle de fichiers ne parvient pas à charger des fichiers dans un compartiment Amazon S3. Vous pouvez configurer le groupe lorsque vous activez la passerelle ou une fois que la passerelle est activée et opérationnelle. Pour plus d'informations sur la façon de configurer un groupe de journaux CloudWatch lors de l'activation d'une passerelle, consultez [Configurer votre passerelle de fichiers Amazon S3](#). Pour obtenir des informations générales sur les groupes de journaux CloudWatch, consultez [Gestion des groupes de journaux et des flux de journaux](#) dans le Guide de l'utilisateur Amazon CloudWatch.

Voici un exemple d'erreur signalée par une passerelle de fichiers.

```
{
  "severity": "ERROR",
  "bucket": "bucket-smb-share2",
  "roleArn": "arn:aws:iam::123456789012:role/my-bucket",
  "source": "share-E1A2B34C",
  "type": "InaccessibleStorageClass",
  "operation": "S3Upload",
  "key": "myFolder/myFile.text",
  "gateway": "sgw-B1D123D4",
  "timestamp": "1565740862516"
}
```

Cette erreur signifie que la passerelle de fichiers n'est pas en mesure de charger l'objet `myFolder/myFile.text` vers Amazon S3, car il est passé de la classe de stockage Amazon S3 Standard vers la classe de stockage S3 Glacier Flexible Retrieval ou la classe de stockage S3 Glacier Deep Archive.

Dans le journal de l'état de la passerelle précédent, ces éléments spécifient les informations données :

- `source`: `share-E1A2B34C` indique le partage de fichiers qui a rencontré cette erreur.
- `"type": "InaccessibleStorageClass"` indique le type d'erreur qui s'est produite. Dans ce cas, cette erreur s'est produite lorsque la passerelle a tenté de charger l'objet spécifié sur Amazon S3 ou de lire à partir d'Amazon S3. Toutefois, dans ce cas, l'objet a été transféré vers Amazon S3 Glacier. La valeur de `"type"` peut être n'importe quelle erreur rencontrée par la passerelle de fichiers. Pour obtenir la liste des erreurs possibles, consultez [Dépannage des problèmes de passerelle de fichiers](#)
- `"operation": "S3Upload"` indique que cette erreur s'est produite lorsque la passerelle a tenté de charger cet objet dans S3.
- `"key": "myFolder/myFile.text"` indique l'objet à l'origine de l'échec.
- `gateway`: `"sgw-B1D123D4"` indique la passerelle de fichiers qui a rencontré cette erreur.
- `"timestamp": "1565740862516"` indique l'heure à laquelle l'erreur s'est produite.

Pour de plus amples informations sur la façon de résoudre et corriger ces types d'erreurs, veuillez consulter [Dépannage des problèmes de passerelle de fichiers](#).

Configuration d'un groupe de journaux CloudWatch après l'activation de votre passerelle

La procédure suivante vous montre comment configurer un groupe de journaux CloudWatch après l'activation de la passerelle.

Pour configurer un groupe de journaux CloudWatch afin qu'il fonctionne avec votre passerelle de fichiers

1. Connectez-vous à la console AWS Management Console et ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle pour laquelle vous souhaitez configurer le groupe de journaux CloudWatch.
3. Pour Actions, choisissez Modification d'informations. Ou, sur le Détails onglet, sous Journaux de Health Non activé, choisissez Configurer un groupe de journaux pour ouvrir Modifier Nom de la passerelle client boîte de dialogue.
4. Pour Groupe de journaux d'intégrité de passerelle, choisissez l'une des options suivantes :
 - Disable logging (Désactivation de la journalisation). si vous ne souhaitez pas surveiller votre passerelle à l'aide de groupes de journaux CloudWatch.
 - Création d'un nouveau groupe de journaux Pour créer un nouveau groupe de journaux CloudWatch.
 - Utiliser un groupe de journaux existant pour utiliser un groupe de journaux CloudWatch existant déjà.

Choisissez un groupe de journaux dans Liste des groupes de journaux existants.

5. Choisissez Save changes (Enregistrer les modifications).
6. Pour afficher les journaux d'intégrité de votre passerelle, procédez comme suit :
 1. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle pour laquelle vous avez configuré le groupe de journaux CloudWatch.
 2. Cliquez sur l'onglet Détails et sous Journaux de Health, choisissez CloudWatch Logs. Le Détails du groupe de journaux s'ouvre dans la console CloudWatch.

Pour configurer un groupe de journaux CloudWatch afin qu'il fonctionne avec votre passerelle de fichiers

1. Connectez-vous à la console AWS Management Console et ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Passerelles, puis sélectionnez la passerelle pour laquelle vous souhaitez configurer le groupe de journaux CloudWatch.
3. Pour Actions, choisissez Modification d'informations. Ou, dans le Détails, à côté de Journalisation, sous Non activé, choisissez Configurer un groupe de journaux pour ouvrir Modification d'informations boîte de dialogue.
4. Pour Groupe de journaux de passerelle, choisissez Utiliser un groupe de journaux existant, puis choisissez le groupe de journaux que vous souhaitez utiliser.

Si vous n'avez pas de groupe de journaux, choisissez Create a new log group (Créer un nouveau groupe de journaux) pour en créer un. Vous êtes dirigé vers la console CloudWatch Logs où vous pouvez créer le groupe de journaux. Si vous créez un nouveau groupe de journaux, cliquez sur le bouton d'actualisation pour afficher le nouveau groupe de journaux dans la liste déroulante.

5. Lorsque vous avez terminé, choisissez Save.
6. Pour afficher les journaux relatifs à la passerelle, choisissez la passerelle, puis choisissez l'Détails onglet.

Pour plus d'informations sur la résolution des erreurs, consultez [Dépannage des problèmes de passerelle de fichiers](#).

Utilisation des métriques Amazon CloudWatch

Vous pouvez obtenir des données de surveillance relatives à la passerelle en utilisant l'AWS Management Console ou l'API CloudWatch. La console affiche un ensemble de graphiques basés sur les données brutes obtenues avec l'API CloudWatch. L'API CloudWatch peut également être utilisée via l'un des [AWS Kits SDK](#) ou [Amazon CloudWatch API](#) outils. En fonction de vos besoins, vous pouvez utiliser les graphiques affichés dans la console ou extraits de l'API.

Quelle que soit la méthode que vous utilisez pour travailler avec les métriques, vous devez spécifier les informations suivantes :

- La dimension de métrique à utiliser. Une dimension est une paire nom-valeur qui vous aide à identifier une métrique de façon unique. Les dimensions de Storage Gateway sont `GatewayId` et `GatewayName`. Dans la console CloudWatch, vous pouvez utiliser le `Gateway Metrics` pour sélectionner des dimensions spécifiques à la passerelle. Pour obtenir de plus amples informations sur les dimensions, consultez [Dimensions](#) dans le Guide de l'utilisateur Amazon CloudWatch.
- Le nom de la métrique, par exemple `ReadBytes`.

Le tableau suivant résume les types de données de métriques de Storage Gateway disponibles.

Amazon CloudWatch Namespace	Dimension	Description
AWS/StorageGateway	<code>GatewayId</code> , <code>GatewayName</code>	<p>Ces dimensions filtrent les données des métriques qui décrivent des aspects de la passerelle. Vous pouvez identifier une passerelle de fichiers à utiliser en spécifiant les dimensions <code>GatewayId</code> et <code>GatewayName</code> .</p> <p>Les données de débit et de latence d'une passerelle reposent sur tous les partages de fichiers de la passerelle.</p> <p>Les données sont disponibles automatiquement toutes les 5 minutes sans coût aucun.</p>

L'utilisation des métriques de passerelle et de fichier est similaire à l'utilisation des autres métriques de service. Vous trouverez des informations sur certaines des tâches de métriques les plus courantes dans la documentation CloudWatch indiquée ci-après :

- [Affichage des métriques disponibles](#)
- [Obtention des statistiques d'une métrique](#)
- [Création d'alarmes CloudWatch](#)

Réception de notifications sur les opérations de fichiers

Storage Gateway peut lancer CloudWatch Events lorsque vos opérations sur les fichiers sont terminées :

- Vous pouvez être informé lorsque la passerelle termine le chargement asynchrone de vos fichiers à partir du partage de fichiers vers Amazon S3. Utilisation de l'[NotificationPolicy](#) Pour demander une notification de chargement de fichier. Cela envoie une notification pour chaque téléchargement de fichier terminé vers Amazon S3. Pour plus d'informations, consultez [Obtenir une notification de téléchargement de fichiers](#).
- Vous pouvez être informé lorsque la passerelle termine le chargement asynchrone de votre jeu de fichiers de travail à partir du partage de fichiers vers Amazon S3. Utilisation de l'[NotifyWhenUploaded](#) Opération API pour demander une notification de téléchargement de jeux de fichiers de travail. Cela envoie une notification lorsque tous les fichiers du jeu de fichiers de travail ont été chargés dans Amazon S3. Pour plus d'informations, consultez [Obtention d'une notification de téléchargement de jeux de fichiers](#).
- Vous pouvez être informé lorsque la passerelle termine l'actualisation du cache pour votre compartiment S3. Lorsque vous invoquez le [RefreshCache](#) via la console ou l'API Storage Gateway, abonnez-vous à la notification lorsque l'opération est terminée. Pour plus d'informations, consultez [Recevoir une notification de cache d'actualisation](#).

Lorsque l'opération sur les fichiers que vous avez demandée est terminée, Storage Gateway vous envoie une notification via CloudWatch Events. Vous pouvez configurer CloudWatch Events pour que la notification vous soit envoyée par le biais d'événement cibles, par exemple par Amazon SNS, Amazon SQS ou un AWS Lambda. Par exemple, vous pouvez configurer une cible Amazon SNS pour que la notification vous soit envoyée aux utilisateurs Amazon SNS, comme un e-mail ou un SMS. Pour plus d'informations sur CloudWatch Events, voir [Qu'est-ce que CloudWatch Events ?](#)

Pour configurer une notification CloudWatch Events

1. Créez une cible, telle qu'une rubrique Amazon SNS ou une fonction Lambda, à invoquer lorsque l'événement que vous avez demandé dans Storage Gateway est déclenché.
2. Créez une règle dans la console CloudWatch Events pour appeler des cibles basées sur un événement dans Storage Gateway.
3. Dans cette règle, créez un modèle d'événement pour le type d'événement. La notification est déclenchée lorsque l'événement correspond à ce modèle de règle.

4. Sélectionnez la cible et configurez les paramètres.

L'exemple suivant montre une règle qui initie le type d'événement spécifié dans la passerelle spécifiée et dans la passerelle spécifiée.AWS Région . Par exemple, vous pouvez spécifier Storage Gateway File Upload Event comme type d'événement.

```
{
  "source": [
    "aws.storagegateway"
  ],
  "resources": [
    "arn:aws:storagegateway:AWS Region:account-id
      :gateway/gateway-id"
  ],
  "detail-type": [
    "Event type"
  ]
}
```

Pour plus d'informations sur l'utilisation de CloudWatch Events pour déclencher des règles, consultez [Création d'une règle CloudWatch Events qui se déclenche sur un événement](#) dans le Guide de l'utilisateur Amazon CloudWatch Events.

Obtenir une notification de téléchargement de fichiers

Vous pouvez utiliser la notification de chargement de fichier dans deux cas :

- Pour l'automatisation du traitement dans le cloud de fichiers qui sont en cours de chargement, vous pouvez appeler le `NotificationPolicy` et récupérer un ID de notification. La notification qui est déclenchée lorsque les fichiers ont été chargés a le même ID de notification que celui qui a été renvoyé par l'API. Si vous mappez cet ID de notification pour suivre la liste des fichiers que vous chargez, vous pouvez déclencher le traitement du fichier qui est chargé dans AWS lorsque l'événement portant le même ID est généré.
- Pour les cas d'utilisation de distribution de contenu, vous pouvez avoir deux passerelles de fichiers mappées au même compartiment Amazon S3. Le partage de fichiers client pour Gateway1 peut télécharger de nouveaux fichiers sur Amazon S3 et les fichiers sont lus par les clients de partage de fichiers sur Gateway2. Les fichiers sont chargés dans Amazon S3, mais ils ne sont pas visibles dans Gateway2, car une version des fichiers mis en cache localement dans Amazon S3 est utilisée. Pour rendre les fichiers visibles dans Gateway2, vous pouvez utiliser

leNotificationPolicyPour demander une notification de chargement de fichier à Gateway1 et ainsi être informé de la fin du téléchargement du fichier. Vous pouvez ensuite utiliser CloudWatch Events pour émettre automatiquement un[RefreshCache](#)Demande de partage de fichiers sur Gateway2. Lorsque[RefreshCache](#)La requête est terminée, le nouveau fichier est visible dans Gateway2.

Exemple Exemple — Notification de chargement de fichier

L'exemple suivant montre une notification de chargement de fichier qui vous est envoyée via CloudWatch lorsque l'événement correspond à la règle que vous avez créée. Cette notification est au format JSON. Vous pouvez configurer cette notification pour qu'elle soit envoyée à la cible en tant que SMS. Le detail-type est Storage Gateway Object Upload Event.

```
{
  "version": "0",
  "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
  "detail-type": "Storage Gateway Object Upload Event",
  "source": "aws.storagegateway",
  "account": "123456789012",
  "time": "2020-11-05T12:34:56Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
    "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
    "arn:aws:s3:::do-not-delete-bucket"
  ],
  "detail": {
    "object-size": 1024,
    "modification-time": "2020-01-05T12:30:00Z",
    "object-key": "my-file.txt",
    "event-type": "object-upload-complete",
    "prefix": "prefix/",
    "bucket-name": "my-bucket",
  }
}
```

Noms de champ	Description
version ;	Version actuelle de la stratégie IAM.

Noms de champ	Description
id	ID qui identifie la stratégie IAM.
detail-type	Description de l'événement qui a déclenché la notification qui a été envoyée.
source	LeAWSqui est la source de la demande et de la notification.
compte	ID duAWSà partir duquel la demande et la notification ont été générées.
time	Moment où la demande de chargement des fichiers sur Amazon S3 a été effectuée.
Région	LeAWSRégion à partir de laquelle la demande et la notification ont été envoyées.
resources	Ressources de la passerelle de stockage auxquelles la stratégie s'applique.
taille de l'objet	Taille de l'objet en octets.
Heure de modification	Heure à laquelle le client a modifié le fichier.
Clé d'objet	Chemin d'accès au fichier.
event-type	CloudWatch Events ayant déclenché la notification.
prefix	Nom du préfixe du compartiment S3.
bucket-name	Nom du compartiment S3.

Obtention d'une notification de téléchargement de jeux de fichiers

Il existe deux cas d'utilisation dans lesquels vous pouvez utiliser la notification de chargement de jeux de fichiers de travail :

- Pour l'automatisation du traitement dans le cloud de fichiers qui sont en cours de chargement, vous pouvez appeler le `NotifyWhenUploadedAPI` et récupérez un ID de notification. La notification qui est déclenchée lorsque l'ensemble de fichiers de travail a été chargé a le même ID de notification que celui qui a été renvoyé par l'API. Si vous mappez cet ID de notification pour suivre la liste des fichiers que vous chargez, vous pouvez déclencher le traitement du jeu de fichiers qui sont chargés dans AWS lorsque l'événement portant le même ID est généré.
- Pour les cas d'utilisation de distribution de contenu, vous pouvez avoir deux passerelles de fichiers mappées au même compartiment Amazon S3. Le partage de fichiers client pour Gateway1 peut télécharger de nouveaux fichiers sur Amazon S3 et les fichiers sont lus par les clients de partage de fichiers sur Gateway2. Les fichiers sont chargés dans Amazon S3, mais ils ne sont pas visibles dans Gateway2, car une version des fichiers mis en cache localement dans S3 est utilisée. Pour rendre les fichiers visibles dans Gateway2, utilisez le [NotifyWhenUploaded](#) Opération d'API pour demander une notification de chargement de fichiers à Gateway1, pour vous avertir lorsque le chargement du jeu de fichiers de travail est terminé. Vous pouvez ensuite utiliser CloudWatch Events pour émettre automatiquement un [RefreshCache](#) Demande de partage de fichiers sur Gateway2. Lorsque [RefreshCache](#) La requête est terminée, les nouveaux fichiers sont visibles dans Gateway2. Cette opération n'importe pas de fichiers dans le stockage du cache de la passerelle de fichiers. Il met uniquement à jour l'inventaire mis en cache pour refléter les modifications apportées à l'inventaire des objets du compartiment S3.

Exemple Exemple : notification de téléchargement de jeux de fichiers de travail

L'exemple suivant montre une notification de chargement d'ensemble de fichiers de travail qui vous est envoyée via CloudWatch lorsque l'événement correspond à la règle que vous avez créée. Cette notification est au format JSON. Vous pouvez configurer cette notification pour qu'elle soit envoyée à la cible en tant que SMS. Le `detail-type` est `Storage Gateway File Upload Event`.

```
{
  "version": "2012-10-17",
  "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
  "detail-type": "Storage Gateway Upload Notification Event",
  "source": "aws.storagegateway",
  "account": "123456789012",
  "time": "2017-11-06T21:34:42Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
    "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
  ]
}
```

```

    ],
    "detail": {
      "event-type": "upload-complete",
      "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
      "request-received": "2018-02-06T21:34:42Z",
      "completed": "2018-02-06T21:34:53Z"
    }
  }
}

```

Noms de champ	Description
version ;	Version actuelle de la stratégie IAM.
id	ID qui identifie la stratégie IAM.
detail-type	Description de l'événement qui a déclenché la notification qui a été envoyée.
source	LeAWSqui est la source de la demande et de la notification.
compte	ID duAWSà partir duquel la demande et la notification ont été générées.
time	Moment où la demande de chargement des fichiers sur Amazon S3 a été effectuée.
Région	LeAWSRégion à partir de laquelle la demande et la notification ont été envoyées.
resources	Ressources Storage Gateway auxquelles la stratégie s'applique.
event-type	CloudWatch Events ayant déclenché la notification.
notification-id	ID généré de façon aléatoire pour la notification qui a été envoyée. Cet ID est au format UUID. ID de notification qui est renvoyé lorsque <code>NotifyWhenUploaded</code> est appelé.

Noms de champ	Description
request-received	Moment où la passerelle a reçu la demande <code>NotifyWhenUploaded</code> .
terminé	Lorsque tous les fichiers contenus dans l'ensemble de travail ont été chargés sur Amazon S3.

Recevoir une notification de cache d'actualisation

Pour le cas d'utilisation d'actualisation du cache, vous pouvez avoir deux passerelles de fichiers mappée au même compartiment Amazon S3 et le client NFS pour Gateway1 qui charge les nouveaux fichiers dans le compartiment S3. Les fichiers sont chargés dans Amazon S3, mais n'apparaissent dans Gateway2 que lorsque vous actualisez le cache. Cela est dû au fait que Gateway2 utilise une version mise en cache localement des fichiers dans Amazon S3. Vous pouvez utiliser les fichiers figurant dans Gateway2 après l'actualisation du cache. Les fichiers volumineux peuvent mettre un certain temps avant d'apparaître dans Gateway2, de sorte que vous pouvez choisir de recevoir une notification lorsque l'actualisation du cache est terminée. Vous pouvez demander une notification d'actualisation du cache à partir de Gateway2 pour être averti lorsque tous les fichiers sont visibles dans Gateway2.

Exemple Exemple — Notification d'actualisation du cache

L'exemple suivant montre une notification d'actualisation du cache qui vous est envoyée via CloudWatch lorsque l'événement correspond à la règle que vous avez créée. Cette notification est au format JSON. Vous pouvez configurer cette notification pour qu'elle soit envoyée à la cible en tant que SMS. Le `detail-type` est `Storage Gateway Refresh Cache Event`.

```
{
  "version": "2012-10-17",
  "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
  "detail-type": "Storage Gateway Refresh Cache Event",
  "source": "aws.storagegateway",
  "account": "209870788375",
  "time": "2017-11-06T21:34:42Z",
  "region": "us-east-2",
  "resources": [
    "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
```

```

    "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
  ],
  "detail": {
    "event-type": "refresh-complete",
    "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
    "started": "2018-02-06T21:34:42Z",
    "completed": "2018-02-06T21:34:53Z",
    "folderList": [
      "/"
    ]
  }
}

```

Noms de champ	Description
version ;	Version actuelle de la stratégie IAM.
id	ID qui identifie la stratégie IAM.
detail-type	Description du type d'événement qui a déclenché la notification ayant été envoyée.
source	LeAWSqui est la source de la demande et de la notification.
compte	ID duAWSà partir duquel la demande et la notification ont été générées.
time	Moment où la demande d'actualisation des fichiers dans l'ensemble de travail a été effectuée.
Région	LeAWSRégion à partir de laquelle la demande et la notification ont été envoyées.
resources	Ressources Storage Gateway auxquelles la stratégie s'applique.
event-type	CloudWatch Events ayant déclenché la notification.

Noms de champ	Description
notification-id	ID généré de façon aléatoire pour la notification qui a été envoyée. Cet ID est au format UUID. ID de notification qui est renvoyé lorsque vous appelez RefreshCache .
démarré	lorsque la passerelle a reçu l'RefreshCache et l'actualisation a été démarrée.
terminé	Moment où l'actualisation de l'ensemble de travail a été terminée.
folderList	Liste séparée par des virgules des chemins d'accès des dossiers qui ont été actualisés dans le cache. La valeur par défaut est [« / »].

Présentation des métriques de la passerelle

Le tableau suivant décrit les métriques couvrant les passerelles de fichiers S3. Chaque passerelle est associée à un ensemble de métriques. Certaines métriques propres à la passerelle ont le même nom que certaines métriques propres au partage de fichiers. Ces métriques représentent les mêmes types de mesures, mais s'appliquent à la passerelle plutôt qu'au partage de fichiers.

Précisez toujours si vous souhaitez utiliser une passerelle ou un partage de fichiers lorsque vous utilisez une métrique particulière. Plus précisément, lorsque vous utilisez les métriques de passerelle, vous devez spécifier laGateway Namepour la passerelle dont vous souhaitez afficher les données de métrique. Pour plus d'informations, consultez [Utilisation des métriques Amazon CloudWatch](#).

Le tableau suivant décrit les métriques d'que vous pouvez utiliser pour obtenir des informations sur votrePasserelle de fichiers S3Les

Métrique	Description
AvailabilityNotifications	Cette métrique indique le nombre de notifications d'intégrité liées à la disponibilité et générées par la passerelle au cours de la période de génération de rapport.

Métrique	Description
	Unités: Nombre
CacheFileSize	<p>Cette métrique analyse la taille des fichiers dans le cache de la passerelle.</p> <p>Utilisez cette mesure avec leAveragestatistique pour mesurer la taille moyenne d'un fichier dans le cache de passerelle. Utilisez cette mesure avec leMaxstatistique pour mesurer la taille maximale d'un fichier dans le cache de passerelle.</p> <p>Unités: Octets</p>
CacheFree	<p>Cette métrique indique le nombre d'octets disponibles dans le cache de la passerelle.</p> <p>Unités: Octets</p>
CacheHitPercent	<p>Pourcentage des opérations de lecture d'application à partir de la passerelle, qui sont fournies par le cache. L'exemple est pris à la fin de la période de génération de rapport.</p> <p>Lorsqu'il n'y a aucune demande d'opération de lecture à partir de la passerelle, cette métrique indique 100 %.</p> <p>Unités: Pourcentage</p>
CachePercentDirty	<p>Le pourcentage global de cache de passerelle n'est pas permanent dansAWS. L'exemple est pris à la fin de la période de génération de rapport.</p> <p>Unités: Pourcentage</p>

Métrique	Description
CachePercentUsed	<p>Pourcentage global du stockage de cache de passerelle utilisé. L'exemple est pris à la fin de la période de génération de rapport.</p> <p>Unités: Pourcentage</p>
CacheUsed	<p>Cette métrique indique le nombre d'octets utilisés dans le cache de passerelle.</p> <p>Unités: Octets</p>
CloudBytesDownloaded	<p>Nombre total d'octets que la passerelle a téléchargés versAWSpendant la période visée par le rapport.</p> <p>Utilisez cette métrique avec la statistique Sum pour mesurer le débit et avec la statistique Samples pour mesurer les opérations d'entrée/ de sortie par seconde (E/S par seconde).</p> <p>Unités: Octets</p>
CloudBytesUploaded	<p>Nombre total d'octets que la passerelle a téléchargés depuisAWSpendant la période visée par le rapport.</p> <p>Utilisez cette métrique avec la statistique Sum pour mesurer le débit et avec la statistique Samples pour mesurer les E/S par seconde.</p> <p>Unités: Octets</p>

Métrique	Description
FilesFailingUpload	<p>Cette métrique effectue le suivi du nombre de fichiers qui ne sont pas en cours de chargement dans AWS. Ces fichiers généreront des notifications de santé contenant plus d'informations sur le problème.</p> <p>Utilisez cette mesure avec le Sumstatistique pour indiquer le nombre de fichiers qui ne parviennent pas actuellement à être téléchargés dans AWS.</p> <p>Unités: Nombre</p>
FileSharesUnavailable	<p>Cette mesure indique le nombre de partages de fichiers sur ces passerelles qui se trouvent dans le Unavailable état.</p> <p>Si cette mesure indique que des partages de fichiers ne sont pas disponibles, il est probable qu'il y ait un problème avec la passerelle, ce qui peut perturber votre flux de travail. Il est recommandé de créer une alarme lorsque cette métrique indique une valeur différente de zéro.</p> <p>Unités: Nombre</p>
FilesRenamed	<p>Cette métrique effectue le suivi du nombre de fichiers renommés au cours de la période de génération du rapport.</p> <p>Unités: Nombre</p>
HealthNotifications	<p>Cette mesure indique le nombre de notifications d'intégrité générées par cette passerelle au cours de la période de reporting.</p> <p>Unités: Nombre</p>

Métrique	Description
IoWaitPercent	<p>Cette métrique indique le pourcentage de temps pendant lequel l'UC attend une réponse du disque local.</p> <p>Unités: Pourcentage</p>
MemTotalBytes	<p>Cette mesure indique la quantité totale de mémoire sur la passerelle.</p> <p>Unités: Octets</p>
MemUsedBytes	<p>Cette mesure indique la quantité de mémoire utilisée sur la passerelle.</p> <p>Unités: Octets</p>
NfsSessions	<p>Cette métrique indique le nombre de sessions NFS qui sont actives sur la passerelle.</p> <p>Unités: Nombre</p>
RootDiskFreeBytes	<p>Cette métrique indique le nombre d'octets disponibles sur le disque racine de la passerelle.</p> <p>Si cette mesure indique que moins de 20 Go sont libres, vous devez augmenter la taille du disque racine.</p> <p>Unités: Octets</p>
S3GetObjectRequestTime	<p>Cette mesure indique le temps que la passerelle doit terminer les demandes d'objets S3 Get.</p> <p>Unités: Millisecondes</p>

Métrique	Description
S3PutObjectRequestTime	<p>Cette mesure indique le temps que la passerelle doit terminer les demandes d'objet S3 put.</p> <p>Unités: Millisecondes</p>
S3UploadPartRequestTime	<p>Cette mesure indique le temps que la passerelle doit terminer les demandes d'article de chargement S3.</p> <p>Unités: Millisecondes</p>
SmbV1Sessions	<p>Cette métrique indique le nombre de sessions SMBv1 qui sont actives sur la passerelle.</p> <p>Unités: Nombre</p>
SmbV2Sessions	<p>Cette métrique indique le nombre de sessions SMBv2 qui sont actives sur la passerelle.</p> <p>Unités: Nombre</p>
SmbV3Sessions	<p>Cette métrique indique le nombre de sessions SMBv3 qui sont actives sur la passerelle.</p> <p>Unités: Nombre</p>
TotalCacheSize	<p>Cette métrique indique la taille totale du cache.</p> <p>Unités: Octets</p>
UserCpuPercent	<p>Cette mesure indique le pourcentage de temps consacré au traitement de la passerelle.</p> <p>Unités: Pourcentage</p>

Comprendre les mesures de partage de fichiers

Vous trouverez, ci-après, des informations sur les métriques de Storage Gateway qui couvrent les partages de fichiers. Chaque partage de fichiers est associé à un ensemble de métriques. Certaines métriques propres au partage de fichiers ont le même nom que certaines métriques propres à la passerelle. Ces métriques représentent les mêmes types de mesures, mais s'appliquent au partage de fichiers.

Précisez toujours si vous souhaitez travailler avec une métrique de passerelle ou de partage de fichiers avant d'utiliser une métrique. Plus précisément, lorsque vous travaillez avec des métriques de partage de fichiers, vous devez spécifier l'`File share ID` qui identifie le partage de fichiers pour lequel vous souhaitez afficher des métriques. Pour plus d'informations, consultez [Utilisation des métriques Amazon CloudWatch](#).

Le tableau suivant décrit les métriques de Storage Gateway que vous pouvez utiliser pour obtenir des informations sur les partages de fichiers.

Métrique	Description
<code>CacheHitPercent</code>	<p>Pourcentage des opérations de lecture d'application à partir des partages de fichiers qui sont servis à partir du cache. L'exemple est pris à la fin de la période de génération de rapport.</p> <p>Lorsqu'il n'y a aucune demande d'opération de lecture à partir du partage de fichiers, cette métrique indique 100 %.</p> <p>Unités: Pourcentage</p>
<code>CachePercentDirty</code>	<p>Contribution du partage de fichiers pour le pourcentage global de cache de la passerelle qui n'est pas conservé dans AWS. L'exemple est pris à la fin de la période de génération de rapport.</p> <p>Utilisation de l'<code>CachePercentDirty</code> métrique de la passerelle pour afficher le pourcentage</p>

Métrique	Description
	<p>global de cache de la passerelle qui n'est pas conservé dansAWS.</p> <p>Unités: Pourcentage</p>
CachePercentUsed	<p>Contribution du partage de fichiers à l'utilisation en pourcentage global du stockage de cache de la passerelle. L'exemple est pris à la fin de la période de génération de rapport.</p> <p>Utilisez la métrique CachePercentUsed de la passerelle pour afficher l'utilisation en pourcentage global du stockage de cache de la passerelle.</p> <p>Unités: Pourcentage</p>
CloudBytesUploaded	<p>Nombre total d'octets que la passerelle a téléchargés versAWSpendant la période visée par le rapport.</p> <p>Utilisez cette métrique avec la statistique Sum pour mesurer le débit et avec la statistique Samples pour mesurer les E/S par seconde.</p> <p>Unités: Octets</p>
CloudBytesDownloaded	<p>Nombre total d'octets que la passerelle a téléchargés depuisAWSpendant la période visée par le rapport.</p> <p>Utilisez cette métrique avec la statistique Sum pour mesurer le débit et avec la statistique Samples pour mesurer les opérations d'entrée/ de sortie par seconde (E/S par seconde).</p> <p>Unités: Octets</p>

Métrique	Description
ReadBytes	<p>Nombre total d'octets lus depuis vos applications sur site au cours de la période de génération de rapport pour un partage de fichiers.</p> <p>Utilisez cette métrique avec la statistique Sum pour mesurer le débit et avec la statistique Samples pour mesurer les E/S par seconde.</p> <p>Unités: Octets</p>
WriteBytes	<p>Nombre total d'octets écrits dans vos applications sur site au cours de la période de génération de rapport.</p> <p>Utilisez cette métrique avec la statistique Sum pour mesurer le débit et avec la statistique Samples pour mesurer les E/S par seconde.</p> <p>Unités: Octets</p>

Comprendre les journaux d'audit de passerelle de fichiers

Les journaux d'audit Amazon S3 File Gateway (S3 File Gateway) fournissent des détails sur l'accès des utilisateurs aux fichiers et dossiers dans un partage de fichiers. Vous pouvez les utiliser pour surveiller les activités des utilisateurs et prendre des mesures si des modèles d'activité inappropriés sont identifiés.

Opérations

Le tableau suivant décrit les opérations d'accès aux fichiers journaux d'audit de la passerelle de fichiers.

Nom de l'opération	Définition
Lire des données	Lire le contenu d'un fichier.

Nom de l'opération	Définition
Écrire des données	Modifier le contenu d'un fichier.
Création	Créer un nouveau fichier ou dossier.
Rename	Renommer un fichier ou un dossier existant.
Delete	Supprimer un fichier ou un dossier.
Écrire des attributs	Mettre à jour les métadonnées de fichiers ou de dossiers (ACL, propriétaire, groupe, autorisations).

Attributs

Le tableau suivant décrit les attributs d'accès aux fichiers journaux d'audit S3 File Gateway.

Attribut	Définition
accessMode	Paramètre d'autorisation pour l'objet.
accountDomain (PME uniquement)	Domaine Active Directory (AD) auquel appartient le compte du client.
accountName (PME uniquement)	Le nom d'utilisateur Active Directory du client.
bucket	Nom du compartiment S3.
clientGid (NFS uniquement)	Identifiant du groupe utilisateur qui accède à l'objet.
clientUid (NFS uniquement)	Identifiant de l'utilisateur accédant à l'objet.
ctime	Moment où le contenu ou les métadonnées de l'objet a été modifié, défini par le client.
groupId	Identifiant du propriétaire du groupe de l'objet.

Attribut	Définition
<code>fileSizeInBytes</code>	Taille du fichier en octets, définie par le client au moment de la création du fichier.
<code>gateway</code>	ID de la passerelle de stockage.
<code>mtime</code>	Moment où le contenu de l'objet a été modifié, défini par le client.
<code>newObjectName</code>	Chemin d'accès complet au nouvel objet après qu'il a été renommé.
<code>objectName</code>	Chemin d'accès complet à l'objet.
<code>objectType</code>	Définit si l'objet est un fichier ou un dossier.
<code>operation</code>	Nom de l'opération d'accès à l'objet.
<code>ownerId</code>	Identifiant du propriétaire de l'objet.
<code>securityDescriptor</code> (PME uniquement)	Affiche la liste ACL discrétionnaire (DACL) définie sur un objet, au format SDDL.
<code>shareName</code>	Nom du partage auquel vous accédez.
<code>source</code>	ID du partage de fichiers en cours d'audit.
<code>sourceAddress</code>	Adresse IP de la machine cliente de partage de fichiers.
<code>status</code>	L'état de l'opération. Seules les réussites sont enregistrées (les échecs sont consignés à l'exception des échecs résultant des autorisations refusées).
<code>timestamp</code>	Moment où l'opération s'est produite en fonction de l'horodatage du système d'exploitation de la passerelle.

Attribut	Définition
version	Version du format du journal d'audit.

Attributs enregistrés par opération

Le tableau suivant décrit les attributs du journal d'audit de la passerelle de fichiers S3 enregistrés dans chaque opération d'accès aux fichiers.

	Lire des données	Écrire des données	Créer un dossier	Créer un fichier	Renommer fichier/dossier	Supprimer un fichier/dossier	Attributs d'écriture (modifier l'ACL -SMB uniquement)	Attributs d'écriture (chown)	Attributs d'écriture (chmod)	Attributs d'écriture (chgrp)
access			X	X					X	
account main (PME uniquement)	X	X	X	X	X	X	X	X	X	X
account me (PME uniquement)	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (NFS)	X	X	X	X	X	X		X	X	X

	Lire des données	Écrire des données	Créer un dossier	Créer un fichier	Renommer le fichier/dossier	Supprimer un fichier/dossier	Attributs d'écriture (modifier l'ACL -SMB uniquement)	Attributs d'écriture (chown)	Attributs d'écriture (chmod)	Attributs d'écriture (chgrp)
client (NFS uniquement)	X	X	X	X	X	X		X	X	X
ctime			X	X						
groupID			X	X						
fileSize				X						
gateway	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObjectName					X					
objecte	X	X	X	X	X	X	X	X	X	X
objecte	X	X	X	X	X	X	X	X	X	X

	Lire des données	Écrire des données	Créer un dossier	Créer un fichier	Renommer le fichier/dossier	Supprimer un fichier/dossier	Attributs d'écriture (modifier l'ACL -SMB uniquement)	Attributs d'écriture (chown)	Attributs d'écriture (chmod)	Attributs d'écriture (chgrp)
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securi escrip (PME uniquen t)							X	X		
shareM	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
source ress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timest	X	X	X	X	X	X	X	X	X	X
versic	X	X	X	X	X	X	X	X	X	X

Maintenance de votre passerelle

La maintenance de votre passerelle inclut des tâches telles que la configuration de l'espace de stockage en cache et du tampon de chargement et la maintenance générale des performances de votre passerelle. Ces tâches sont communes à tous les types de passerelle.

Rubriques

- [Arrêt de la machine virtuelle de la passerelle](#)
- [Gestion des disques locaux pour votre Storage Gateway](#)
- [Gestion de bande passante pour votre passerelle de fichiers Amazon S3](#)
- [Gestion des mises à jour de la passerelle à l'aide de la Console AWS Storage Gateway](#)
- [Exécution des tâches de maintenance sur la console locale](#)
- [Suppression de votre passerelle à l'aide de la Console AWS Storage Gateway et suppression des ressources associées](#)

Arrêt de la machine virtuelle de la passerelle

Par exemple, vous devrez peut-être arrêter ou redémarrer la machine virtuelle pour les opérations de maintenance, comme lors de l'application d'un correctif à votre hyperviseur. Avant d'arrêter la machine virtuelle, vous devez d'abord arrêter la passerelle. Pour la passerelle de fichiers, vous devez juste arrêter votre machine virtuelle. Bien que cette section se concentre sur le démarrage et l'arrêt de la passerelle à l'aide de la console de gestion Storage Gateway, vous pouvez également arrêter et démarrer la passerelle à l'aide de la console locale de votre machine virtuelle ou de l'API Storage Gateway. Lorsque vous mettez votre machine virtuelle sous tension, n'oubliez pas de redémarrer votre passerelle.

Par exemple, vous devrez peut-être arrêter ou redémarrer la machine virtuelle pour les opérations de maintenance, comme lors de l'application d'un correctif à votre hyperviseur. Pour la passerelle de fichiers, vous devez juste arrêter votre machine virtuelle. Vous n'arrêtez pas la passerelle. Bien que cette section se concentre sur le démarrage et l'arrêt de la passerelle à l'aide de la console de gestion Storage Gateway, vous pouvez également arrêter et démarrer la passerelle à l'aide de la console locale de votre machine virtuelle ou de l'API Storage Gateway. Lorsque vous mettez votre machine virtuelle sous tension, n'oubliez pas de redémarrer votre passerelle.

- Console locale de la machine virtuelle de la passerelle : [Exécution des tâches de maintenance sur la console locale](#).
- API Storage Gateway : voir [ShutdownGateway](#)

Gestion des disques locaux pour votre Storage Gateway

L'ordinateur virtuel de la passerelle utilise les disques locaux que vous allouez sur site pour le tampon et le stockage. Les passerelles créées sur des instances Amazon EC2 utilisent des volumes Amazon EBS en tant que disques locaux.

Rubriques

- [Décider de la quantité de stockage sur disque local](#)
- [Détermination de la taille du stockage en cache à allouer](#)
- [Ajouter du stockage de cache](#)
- [Utilisation du stockage éphémère avec des passerelles EC2](#)

Décider de la quantité de stockage sur disque local

Vous décidez du nombre et de la taille des disques que vous souhaitez allouer à la passerelle. La passerelle nécessite le stockage supplémentaire suivant :

Les passerelles de fichiers requièrent au moins un disque qui sera utilisé en tant que cache. Le tableau suivant recommande des tailles pour le stockage du disque local associé à la passerelle déployée. Vous pouvez ajouter ultérieurement plus de stockage local une fois que vous avez configuré la passerelle et en fonction de l'augmentation de vos demandes de charge de travail.

Stockage local	Description	Type de passerelle
Stockage de cache	Le stockage du cache fait office de stockage sur site durable des données en attente de chargement sur Amazon S3 ou sur un système de fichiers.	<ul style="list-style-type: none"> • Passerelles de fichiers

Note

Les ressources de stockage physique sous-jacentes sont représentées sous la forme de banque de données dans VMware. Lorsque vous déployez l'ordinateur virtuel de la passerelle, vous choisissez une banque de données sur laquelle stocker les fichiers de l'ordinateur virtuel. Lorsque vous mettez en service un disque local (par exemple, pour l'utiliser comme stockage de cache), vous avez la possibilité de stocker le disque virtuel dans la même banque de données en tant qu'ordinateur virtuel ou dans une banque de données différente.

Si vous avez plusieurs banques de données, nous vous recommandons vivement de choisir une banque de données pour le stockage de cache. Un stockage de données qui est basé sur un seul disque physique sous-jacent peut entraîner des performances médiocres dans certains cas si elle est utilisée pour soutenir les deux disques de cache. C'est également le cas si la sauvegarde est une configuration RAID moins performante telle que RAID1.

Après la configuration initiale et le déploiement de votre passerelle, vous pouvez ajuster le stockage local en ajoutant des disques pour le stockage de cache.

Détermination de la taille du stockage en cache à allouer

Votre passerelle utilise son stockage de cache pour fournir un accès à faible latence aux données récemment consultées. Le stockage de cache fait office de stockage sur site durable des données en attente de chargement sur Amazon S3 ou sur un système de fichiers. Pour plus d'informations sur l'estimation de la taille du stockage de cache, consultez [Gestion des disques locaux pour votre Storage Gateway](#).

Vous pouvez d'abord utiliser cette approximation pour mettre en service les disques du stockage de cache. Vous pouvez ensuite utiliser les métriques opérationnelles Amazon CloudWatch pour surveiller l'utilisation du stockage de cache et mettre en service plus de stockage en fonction des besoins à l'aide de la console. Pour plus d'informations sur les métriques et la configuration des alarmes, consultez [Performances](#).

Ajouter du stockage de cache

Les besoins de votre application évoluant, vous pouvez accroître la capacité de stockage de cache de la passerelle. Vous pouvez ajouter plus de capacité de cache à la passerelle sans interrompre les

fonctions de passerelle existantes. Lorsque vous ajoutez plus de capacité de stockage, vous le faites avec l'ordinateur virtuel de la passerelle activé.

Important

Lorsque vous ajoutez un cache à une passerelle existante, il est important de créer des disques sur votre hôte (hyperviseur ou instance Amazon EC2). Ne modifiez pas la taille des disques existants si les disques ont été alloués antérieurement en tant que cache. Ne supprimez pas les disques mis en cache alloués comme stockage de cache.

La procédure suivante vous montre comment configurer ou mettre en cache le stockage pour votre passerelle.

Pour ajouter et configurer ou mettre en cache du stockage

1. Allouez un nouveau disque dans votre hôte (hyperviseur ou instance Amazon EC2). Pour plus d'informations sur la façon d'allouer un disque dans un hyperviseur, consultez le manuel d'utilisation de votre hyperviseur. Vous configurez ce disque en tant que stockage de cache.
2. Ouvrez la console Storage Gateway à l'adresse <https://console.aws.amazon.com/storagegateway/home>.
3. Dans le volet de navigation, choisissez Passerelles.
4. Dans le menu Actions, choisissez Modifier les disques locaux.
5. Dans la boîte de dialogue Modifier les disques locaux, identifiez les disques que vous avez alloués et choisissez celui que vous souhaitez utiliser pour le stockage mis en cache.

Si vous ne voyez pas vos disques, choisissez le bouton Actualiser.

6. Choisissez Enregistrer pour enregistrer les paramètres de configuration.

Utilisation du stockage éphémère avec des passerelles EC2

Cette section décrit les étapes à suivre pour éviter de perdre des données lorsque vous choisissez un disque éphémère pour le stockage du cache de votre passerelle.

Les disques éphémères assurent un stockage temporaire de niveau bloc pour votre instance Amazon EC2. Les disques éphémères sont idéaux pour le stockage temporaire de données qui changent fréquemment, telles que les données contenues dans le stockage de cache d'une passerelle.

Lorsque vous lancez votre passerelle avec une Amazon EC2 Amazon Machine Image et que le type d'instance que vous sélectionnez prend en charge le stockage éphémère, les disques s'affichent automatiquement. Vous pouvez alors en sélectionner un pour stocker des données dans le cache de votre passerelle. Pour de plus amples informations, veuillez consulter [Stockage d'instance Amazon EC2](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

Les écritures d'application sur les disques sont stockées dans le cache de manière synchrone et chargées de manière asynchrone vers un stockage durable dans Amazon S3. Si les données stockées dans le stockage éphémère sont perdues suite à l'arrêt d'une instance Amazon EC2 avant la fin du chargement des données, les données résidant encore dans le cache et non encore chargées vers Amazon S3 risquent d'être perdues. Vous pouvez éviter la perte de données en suivant les étapes nécessaires avant de redémarrer ou d'arrêter l'instance EC2 qui héberge votre passerelle.

 Note

Si vous utilisez un stockage éphémère et que vous arrêtez et démarrez votre passerelle, la passerelle sera définitivement hors ligne. Cela se produit parce que le disque de stockage physique est remplacé. Il n'est pas possible de contourner ce problème, c'est pourquoi vous devrez supprimer la passerelle et en activer une nouvelle sur une nouvelle instance EC2.

Les étapes de la procédure ci-dessous sont propres aux passerelles de fichiers.

Pour éviter une perte de données dans les passerelles de fichiers qui utilisent des disques éphémères

1. Arrêtez tous les processus qui écrivent dans le partage de fichiers.
2. Abonnez-vous pour recevoir des notifications de CloudWatch Events. Pour plus d'informations, veuillez consulter [Réception de notifications sur les opérations de fichiers](#).
3. Appelez le [NotifyWhenUploaded de l'API](#) pour recevoir une notification lorsque les données écrites jusqu'au moment de la perte du stockage éphémère sont stockées durablement dans Amazon S3.
4. Attendez que l'API ait terminé. Vous recevez alors un ID de notification.

Vous recevez un événement CloudWatch avec le même ID de notification.

5. Vérifiez que la métrique `CachePercentDirty` correspondant à votre partage de fichiers a la valeur 0. Cette valeur signifie que toutes vos données ont été écrites sur Amazon S3. Pour plus

d'informations sur les métriques de partage de fichiers, consultez [Comprendre les mesures de partage de fichiers](#).

6. Vous pouvez à présent redémarrer ou arrêter la passerelle de fichiers sans risque de perdre des données.

Gestion de bande passante pour votre passerelle de fichiers Amazon S3

Vous pouvez limiter le débit de chargement depuis votre passerelle vers AWS. Pour contrôler la quantité de bande passante réseau utilisée par la passerelle. Par défaut, une passerelle activée n'a pas de limites de taux.

Vous pouvez configurer un programme de limite de bande passante à l'aide de la AWS Management Console, un AWS Software Development Kit (SDK) ou le AWS Storage Gateway API (voir [Mettre à jour le calendrier de limite de débit de bande passante](#) dans le AWS Référence des API Storage Gateway). À l'aide d'un calendrier de limite de débit de bande passante, vous pouvez configurer les limites pour qu'elles soient modifiées automatiquement tout au long de la journée ou de Pour plus d'informations, consultez [Afficher et modifier le calendrier limite de débit de bande passante pour votre passerelle à l'aide de la console Storage Gateway](#).

Note

La configuration des limites de débit de bande passante et des programmes n'est actuellement pas prise en charge pour le type Amazon FSx File Gateway.

Rubriques

- [Afficher et modifier le calendrier limite de débit de bande passante pour votre passerelle à l'aide de la console Storage Gateway](#)
- [Mise à jour des limites de taux de bande passante des passerelles à l'aide AWS SDK for Java](#)
- [Mise à jour des limites de taux de bande passante des passerelles à l'aide AWS SDK for .NET](#)
- [Mise à jour des limites de taux de bande passante des passerelles à l'aide AWS Tools for Windows PowerShell](#)

Afficher et modifier le calendrier limite de débit de bande passante pour votre passerelle à l'aide de la console Storage Gateway

Cette section explique comment afficher et modifier le programme de limite de taux de bande passante pour votre passerelle.

Pour afficher et modifier le calendrier de limite de taux de bande passante

1. Ouvrez la console Storage Gateway à l'adresse <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le volet de navigation de gauche, choisissez Passerelles, puis choisissez la passerelle que vous voulez gérer.
3. Pour Actions, choisissez Modifier le calendrier limite de débit de bande passante.

La planification actuelle de la limite de débit de bande passante de la passerelle est affichée sur le Modifier le calendrier limite de débit de bande passante. Par défaut, une nouvelle passerelle n'a aucune limite de débit de bande passante définie.

4. (Facultatif) Choisissez Ajouter une nouvelle limite de débit de bande passante pour ajouter un nouvel intervalle configurable à la planification. Pour chaque intervalle que vous ajoutez, entrez les informations suivantes :
 - Taux de téléchargement— Entrez la limite de taux de téléchargement, en mégabits par seconde (Mbps). La valeur minimale est de 100 Mbps.
 - Jours de la semaine— Sélectionnez le jour ou les jours de chaque semaine où vous souhaitez que l'intervalle s'applique. Vous pouvez appliquer cet intervalle les jours de semaine (du lundi au vendredi), les week-ends (samedi et dimanche), tous les jours de la semaine ou un jour spécifique chaque semaine. Pour appliquer la limite de débit de bande passante de manière uniforme et constante tous les jours et à tout moment, choisissez Pas d'horaire.
 - L'heure de début— Entrez l'heure de début de l'intervalle de bande passante, en utilisant le format HH:MM et le décalage du fuseau horaire par rapport à l'UTC pour votre passerelle.

Note

Votre intervalle limite de bande passante commence au début de la minute que vous spécifiez ici.

- **Heure de fin**— Entrez l'heure de fin de l'intervalle de bande passante, en utilisant le format HH:MM et le décalage du fuseau horaire par rapport à GMT pour votre passerelle.

⚠ Important

L'intervalle limite de bande passante se termine à la fin de la minute spécifiée ici. Pour programmer un intervalle qui se termine à la fin d'une heure, entrez**59**. Pour programmer des intervalles continus consécutifs, en transition au début de l'heure, sans interruption entre les intervalles, entrez**59**pour la minute de fin du premier intervalle. Saisissez**00**pour la minute de début de l'intervalle suivant.

5. (Facultatif) Répétez l'étape précédente si nécessaire jusqu'à ce que votre programme de taux de bande passante limite soit terminé. Si vous devez supprimer un intervalle de votre programme, choisissezSupprimez.

⚠ Important

Les intervalles limites de bande passante ne peuvent pas se chevaucher. L'heure de début d'un intervalle doit se produire après l'heure de fin d'un intervalle précédent et avant l'heure de début d'un intervalle suivant.

6. Lorsque vous avez terminé, choisissezEnregistrez les modifications.

Mise à jour des limites de taux de bande passante des passerelles à l'aideAWS SDK for Java

En mettant à jour les limites de débit de bande passante par programmation, vous pouvez ajuster automatiquement ces limites sur une période donnée, par exemple à l'aide de tâches planifiées. L'exemple suivant montre comment mettre à jour les limites de taux de bande passante à l'aide d'.AWS SDK for Java. Pour utiliser l'exemple de code, vous devez maîtriser l'exécution d'une application de console Java. Pour plus d'informations, consultez [Mise en route](#) dans le Manuel du développeur AWS SDK for Java.

Exemple Mise à jour des limites de taux de bande passante des passerelles à l'aide d'AWS SDK for Java

L'exemple de code Java suivant met à jour les limites de taux de bande passante d'une passerelle. Pour utiliser cet exemple de code, vous devez fournir le point de terminaison du service, le

nom Amazon Resource Name (ARN) de la passerelle et la limite de chargement. Pour une liste de AWS points de terminaison de service que vous pouvez utiliser avec Storage Gateway, voir [AWS Storage Gateway Points de terminaison et quotas](#) dans le AWS Référence générale.

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

import java.util.Arrays;
import java.util.Collections;
import java.util.List;

public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

    // The gatewayARN
    public static String gatewayARN = "**** provide gateway ARN ****";

    // The endpoint
    static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

    // Rates
    static long uploadRate = 100 * 1024 * 1024; // Bits per second, minimum 100
Megabits/second

    public static void main(String[] args) throws IOException {

        // Create a storage gateway client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
        sgClient.setEndpoint(serviceURL);

        UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File gateways
```

```
    }

    private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
        try
        {
            BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
            BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                .withBandwidthRateLimit(bandwidthRateLimit)
                .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                .withStartHourOfDay(0)
                .withStartMinuteOfHour(0)
                .withEndHourOfDay(23)
                .withEndMinuteOfHour(59);
            UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                new UpdateBandwidthRateLimitScheduleRequest()
                .withGatewayARN(gatewayArn)
                .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

            UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

            String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
            System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
        }
        catch (AmazonClientException ex)
        {
            System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
        }
    }
}
```

Mise à jour des limites de taux de bande passante des passerelles à l'aide d'AWS SDK for .NET

En mettant à jour les limites de débit de bande passante par programmation, vous pouvez ajuster automatiquement ces limites sur une période donnée, par exemple à l'aide de tâches planifiées. L'exemple suivant montre comment mettre à jour les limites de taux de bande passante à l'aide d'AWSKit de développement logiciel (SDK) pour .NET. Pour utiliser l'exemple de code, vous devez maîtriser l'exécution d'une application de console .NET. Pour plus d'informations, consultez [Mise en route](#) dans le Manuel du développeur AWS SDK for .NET.

Exemple Mise à jour des limites de taux de bande passante de la passerelle à l'aide d'AWS SDK for .NET

L'exemple de code C# suivant met à jour les limites de taux de bande passante d'une passerelle. Pour utiliser cet exemple de code, vous devez fournir le point de terminaison du service, le nom Amazon Resource Name (ARN) de la passerelle et la limite de chargement. Pour une liste de AWS points de terminaison de service que vous pouvez utiliser avec Storage Gateway, voir [AWS Storage Gateway Points de terminaison et quotas](#) dans le AWS Référence générale.

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Amazon.StorageGateway;
using Amazon.StorageGateway.Model;

namespace AWSStorageGateway
{
    class UpdateBandwidthExample
    {
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

        // The gatewayARN
        public static String gatewayARN = "**** provide gateway ARN ****";

        // The endpoint
        static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";

        // Rates
```

```
static long uploadRate = 100 * 1024 * 1024; // Bits per second, minimum
100 Megabits/second

public static void Main(string[] args)
{
    // Create a storage gateway client
    sgConfig = new AmazonStorageGatewayConfig();
    sgConfig.ServiceURL = serviceURL;
    sgClient = new AmazonStorageGatewayClient(sgConfig);

    UpdateBandwidth(gatewayARN, uploadRate, null);

    Console.WriteLine("\nTo continue, press Enter.");
    Console.Read();
}

public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
{
    try
    {
        BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
        BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
            .withBandwidthRateLimit(bandwidthRateLimit)
            .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
            .withStartHourOfDay(0)
            .withStartMinuteOfHour(0)
            .withEndHourOfDay(23)
            .withEndMinuteOfHour(59);
        List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
        bandwidthRateLimitIntervals.Add(noScheduleInterval);
        UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
            new UpdateBandwidthRateLimitScheduleRequest()
                .withGatewayARN(gatewayARN)
                .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

        UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheduduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
```

```

        String returnGatewayARN =
updateBandwidthRateLimitScheduleResponse.GatewayARN;
        Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
        Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
    }
    catch (AmazonStorageGatewayException ex)
    {
        Console.WriteLine("Error updating gateway bandwidth.\n" +
ex.ToString());
    }
}
}
}

```

Mise à jour des limites de taux de bande passante des passerelles à l'aide d'AWS Tools for Windows PowerShell

En mettant à jour les limites de débit de bande passante par programmation, vous pouvez ajuster automatiquement ces limites sur une période donnée, par exemple à l'aide de tâches planifiées. L'exemple suivant montre comment mettre à jour les limites de taux de bande passante à l'aide d'AWS Tools for Windows PowerShell. Pour utiliser l'exemple de code, vous devez connaître l'exécution d'un script PowerShell. Pour plus d'informations, consultez [Démarrer](#) dans le Guide de l'utilisateur AWS Tools for Windows PowerShell.

Exemple Mise à jour des limites de taux de bande passante de la passerelle à l'aide d'AWS Tools for Windows PowerShell

L'exemple suivant de script PowerShell met à jour les limites de taux de bande passante d'une passerelle. Pour utiliser cet exemple de script, vous devez fournir le nom Amazon Resource Name (ARN) de la passerelle et la limite de chargement.

```

<#
.DESCRIPTION
    Update Gateway bandwidth limits schedule

.NOTES
    PREREQUISITES:
    1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and region stored in session using Initialize-AWSDefault.

```

For more info, see <https://docs.aws.amazon.com/powershell/latest/userguide/specifying-your-aws-credentials.html>

.EXAMPLE

```
powershell.exe .\SG_UpdateBandwidth.ps1
#>

$UploadBandwidthRate = 100 * 1024 * 1024
$gatewayARN = "**** provide gateway ARN ****"

$bandwidthRateLimitInterval = New-Object
Amazon.StorageGateway.Model.BandwidthRateLimitInterval
$bandwidthRateLimitInterval.StartHourOfDay = 0
$bandwidthRateLimitInterval.StartMinuteOfHour = 0
$bandwidthRateLimitInterval.EndHourOfDay = 23
$bandwidthRateLimitInterval.EndMinuteOfHour = 59
$bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
$bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
$UploadBandwidthRate

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                     -BandwidthRateLimitInterval
@($bandwidthRateLimitInterval)

$schedule = Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew bandwidth throttle schedule: " +
$schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

Gestion des mises à jour de la passerelle à l'aide de la Console AWS Storage Gateway

Storage Gateway publie régulièrement d'importantes mises à jour logicielles pour votre passerelle. Vous pouvez appliquer manuellement les mises à jour dans la console de gestion Storage Gateway ou automatiquement pendant le programme de maintenance configuré. Bien que Storage Gateway vérifie les mises à jour chaque minute, les opérations de maintenance et de redémarrage ne sont effectuées qu'en cas de mises à jour.

Les versions logicielles de la passerelle incluent régulièrement des mises à jour du système d'exploitation et des correctifs de sécurité validés par AWS. Ces mises à jour sont généralement publiées tous les six mois et sont appliquées dans le cadre du processus normal de mise à jour de la passerelle pendant les fenêtres de maintenance planifiées.

Note

Vous devez traiter le dispositif Storage Gateway comme un périphérique intégré géré et ne pas tenter d'accéder ou de modifier son installation de quelque manière que ce soit. La tentative d'installation ou de mise à jour de logiciels à l'aide de méthodes autres que le mécanisme normal de mise à jour de passerelle (par exemple, les outils SSM ou hyperviseur) peut entraîner un dysfonctionnement de la passerelle.

Avant d'appliquer une mise à jour à votre passerelle, AWS vous informe par un message sur la console Storage Gateway et sur votre AWS Health Dashboard. Pour plus d'informations, consultez [AWS Health Dashboard](#). La machine virtuelle ne redémarre pas, mais la passerelle est indisponible pendant une courte période lors de sa mise à jour et son redémarrage.

Lorsque vous déployez et activez votre passerelle, un programme de maintenance hebdomadaire par défaut est défini. Vous pouvez modifier le programme de maintenance à tout moment. Lorsque des mises à jour sont disponibles, l'onglet Détails affiche un message de maintenance. Dans l'onglet Détails, vous pouvez voir la date et l'heure auxquelles la dernière mise à jour réussie a été appliquée à votre passerelle.

Pour modifier le programme de maintenance

1. Ouvrez la console Storage Gateway à l'adresse <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le panneau de navigation, choisissez Passerelles, puis choisissez la passerelle dont vous souhaitez modifier le programme de mise à jour.
3. Dans le menu Actions choisissez Edit maintenance window (Modifier la fenêtre de maintenance) pour ouvrir la boîte de dialogue Edit maintenance start time (Modifier le commencement de la fenêtre de maintenance).
4. Pour Programme, choisissez Hebdomadaire ou Mensuel afin de planifier des mises à jour.
5. Si vous choisissez Hebdomadaire, modifiez les valeurs de Jour de la semaine et de Temps.

Si vous choisissez Mensuel, modifiez les valeurs de Jour du mois et de Temps. Si vous choisissez cette option et que vous obtenez une erreur, cela signifie que votre passerelle est une version plus ancienne et n'a pas encore été mise à niveau vers une version plus récente.

Note

La valeur maximale pouvant être définie pour le jour du mois est 28. Si 28 est sélectionné, l'heure de début de la maintenance sera le 28e jour de chaque mois.

L'heure de début de la maintenance apparaît sur le **Détails** pour la passerelle la prochaine fois que vous ouvrirez le **Détails** onglet.

Exécution des tâches de maintenance sur la console locale

Vous pouvez exécuter les tâches de maintenance suivantes à l'aide de la console locale de l'hôte. Les tâches de la console locale peuvent être effectuées sur l'hôte de l'ordinateur virtuel ou sur l'instance Amazon EC2. La plupart des tâches sont communes aux différents hôtes, mais il existe également quelques différences.

Rubriques

- [Exécution de tâches sur la console locale de la machine virtuelle \(passerelle de fichiers\)](#)
- [Exécution de tâches sur la console locale Amazon EC2 \(passerelle de fichiers\)](#)
- [Accès à la console locale de la passerelle](#)
- [Configuration des cartes réseau pour la passerelle](#)

Exécution de tâches sur la console locale de la machine virtuelle (passerelle de fichiers)

Pour une passerelle de fichiers déployée sur site, vous pouvez exécuter les tâches de maintenance suivantes à l'aide de la console locale de l'hôte de l'ordinateur virtuel. Ces tâches sont communes aux hyperviseurs VMware, Microsoft Hyper-V et KVM (machine virtuelle basée sur le noyau Linux).

Rubriques

- [Connexion à la console locale de la passerelle de fichiers](#)

- [Configuration d'un proxy HTTP](#)
- [Configuration des paramètres réseau de votre passerelle](#)
- [Test de la connectivité réseau de votre passerelle](#)
- [Affichage de l'état des ressources système de votre passerelle](#)
- [Configuration d'un serveur NTP \(Network Time Protocol\) pour votre passerelle](#)
- [Exécution de commandes Storage Gateway sur la console locale](#)
- [Configuration des cartes réseau pour votre passerelle](#)

Connexion à la console locale de la passerelle de fichiers

Lorsque l'ordinateur virtuel est prêt pour que vous puissiez vous connecter, l'écran de connexion s'affiche. Si c'est la première fois que vous vous connectez à la console locale, vous utilisez le nom d'utilisateur et le mot de passe par défaut pour vous connecter. Ces informations d'identification par défaut vous donnent accès aux menus dans lesquels vous pouvez configurer les paramètres réseau de la passerelle et changer le mot de passe à partir de la console locale. AWS Storage Gateway vous permet de définir votre propre mot de passe à partir de la console Storage Gateway au lieu de modifier le mot de passe à partir de la console locale. Vous n'avez pas besoin de connaître le mot de passe par défaut pour définir un nouveau mot de passe. Pour plus d'informations, consultez [Connexion à la console locale de la passerelle de fichiers](#).

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

Pour vous connecter à la console locale de la passerelle

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

Note

Nous vous recommandons de changer le mot de passe par défaut. Pour cela, exécutez la commande `passwd` dans le menu de la console locale (point 6 du menu principal). Pour plus d'informations sur l'exécution de la commande, consultez [Exécution de commandes Storage Gateway sur la console locale](#). Vous pouvez également définir le mot de passe à partir de la console Storage Gateway. Pour plus d'informations, consultez [Connexion à la console locale de la passerelle de fichiers](#).

Définition du mot de passe de la console locale depuis la console Storage Gateway

Lors de la première connexion à la console locale, connectez-vous à l'ordinateur virtuel avec les informations d'identification par défaut. Pour tous les types de passerelle, utilisez les informations d'identification par défaut. Le nom d'utilisateur est `admin`, et le mot de passe est `password`.

Nous vous recommandons de définir toujours un nouveau mot de passe immédiatement après avoir créé votre nouvelle passerelle. Vous pouvez définir ce mot de passe à partir de la console AWS Storage Gateway au lieu de la console locale si vous le souhaitez. Vous n'avez pas besoin de connaître le mot de passe par défaut pour définir un nouveau mot de passe.

Pour définir le mot de passe de la console locale sur la console Storage Gateway

1. Ouvrez la console Storage Gateway à l'adresse <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le volet de navigation, choisissez Gateways (Passerelles), puis sélectionnez la passerelle pour laquelle vous souhaitez définir un nouveau mot de passe.
3. Pour Actions, choisissez Set Local Console Password (Définir le mot de passe de la console locale).
4. Dans la boîte de dialogue Set Local Console Password (Définir le mot de passe de la console locale), entrez un nouveau mot de passe, confirmez-le, puis choisissez Save (Enregistrer).

Le nouveau mot de passe remplace le mot de passe par défaut. Storage Gateway n'enregistre pas le mot de passe, mais le transmet en toute sécurité à l'ordinateur virtuel.

Note

Le mot de passe peut être constitué de n'importe quel caractère sur le clavier et peut comporter de 1 à 512 caractères.

Configuration d'un proxy HTTP

Les passerelles de fichiers prennent en charge la configuration d'un proxy HTTP.

Note

La seule configuration proxy prise en charge par la passerelle de fichiers est HTTP.

Si votre passerelle doit utiliser un serveur proxy pour communiquer avec Internet, vous devez configurer les paramètres de proxy HTTP de la passerelle. Pour cela, spécifiez un numéro de port et une adresse IP pour l'hôte exécutant le proxy. Ensuite, Storage Gateway achemine tous les AWSTrafic des points de terminaison via le serveur proxy. Les communications entre la passerelle et les points de terminaison sont chiffrées, même lorsque vous utilisez le proxy HTTP. Pour plus d'informations sur les exigences en matière de réseau pour votre passerelle, consultez [Exigences pour le réseau et le pare-feu](#).

Pour configurer un proxy HTTP pour une passerelle de fichiers

1. Connectez-vous à la console locale de la passerelle :
 - Pour plus d'informations sur la journalisation dans la console locale VMware ESXi, consultez [Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Pour plus d'informations sur la journalisation dans la console locale Microsoft Hyper-V, consultez [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).
 - Pour plus d'informations sur la connexion à la console locale pour la machine virtuelle basée sur le noyau Linux (KVM), consultez [Accès à la console locale de la passerelle avec Linux KVM](#).
2. Dans la page AWSActivation de l'appliance - ConfigurationMenu principal, saisissez1Pour commencer à configurer le proxy HTTP.

```

AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: 192.168.1.100
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: Command Prompt

Press "x" to exit session

Enter command: _

```

3. Dans le menu de configuration de proxy HTTP, entrez **1** et indiquez le nom d'hôte du serveur proxy HTTP.

```

AWS Appliance Activation HTTP Proxy Configuration

Note: setting is only applicable to AWS Storage Gateway

1: Configure HTTP Proxy
2: View Current HTTP Proxy Configuration
3: Remove HTTP Proxy Configuration

Press "x" to exit

Enter command: _

```

Vous pouvez configurer d'autres paramètres HTTP à partir de ce menu comme indiqué ci-après.

Pour	Faire ceci
Configurer un proxy HTTP	Saisissez 1 .

Pour	Faire ceci
	Vous devez fournir un nom d'hôte et un port pour finaliser la configuration.
Afficher la configuration actuelle du proxy HTTP	<p>Saisissez 2.</p> <p>Si aucun proxy HTTP n'est configuré, le message HTTP Proxy not configured s'affiche. Si un proxy HTTP est configuré, le nom d'hôte et le port du proxy s'affichent.</p>
Supprimer une configuration de proxy HTTP	<p>Saisissez 3.</p> <p>Le message HTTP Proxy Configuration Removed s'affiche.</p>

- Redémarrez votre ordinateur virtuel pour appliquer vos paramètres de configuration HTTP.

Configuration des paramètres réseau de votre passerelle

La configuration du réseau par défaut de la passerelle est le protocole de DHCP (Dynamic Host Configuration Protocol). Avec le protocole DHCP, votre passerelle reçoit automatiquement une adresse IP. Dans certains cas, vous devrez peut-être affecter manuellement l'IP de votre passerelle comme adresse IP statique, tel que décrit ci-après.

Pour configurer votre passerelle de façon à utiliser des adresses IP statiques

- Connectez-vous à la console locale de la passerelle :
 - Pour plus d'informations sur la journalisation dans la console locale VMware ESXi, consultez [Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Pour plus d'informations sur la journalisation dans la console locale Microsoft Hyper-V, consultez [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).
 - Pour plus d'informations sur la journalisation dans la console locale KVM, consultez [Accès à la console locale de la passerelle avec Linux KVM](#).

2. Dans la page AWS Activation de l'appliance - Configuration Menu principal, saisissez 2 pour commencer à configurer votre réseau.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: Command Prompt

Press "x" to exit session

Enter command: _
```

3. Choisissez l'une des options suivantes dans le menu Network Configuration (Configuration du réseau).

```
AWS Appliance Activation - Network Configuration

1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: Edit DNS Configuration
7: View DNS Configuration
8: View Routes

Press "x" to exit

Enter command: _
```

Pour	Faire ceci
Collecter des informations sur votre carte réseau	<p>Saisissez 1.</p> <p>Une liste de noms de cartes apparaît et vous êtes invité à entrer un nom d'adaptateur, par exemple, eth0. Si la carte que vous spécifiez est en cours d'utilisation, les informations suivantes sur la carte sont affichées :</p> <ul style="list-style-type: none">• Adresse MAC• Adresse IP• Masque réseau• Adresse IP de la passerelle• État activé DHCP <p>Vous utilisez le même nom de carte lorsque vous configurez une adresse IP statique (option 3) que lorsque vous définissez la carte de routage par défaut de votre passerelle (option 5).</p>

Pour	Faire ceci
Configurer DHCP	<p>Saisissez 2.</p> <p>Vous êtes invité à configurer l'interface réseau pour utiliser le protocole DHCP.</p> <pre data-bbox="829 470 1507 905">AWS Storage Gateway Network Configuration 1: Describe Adapter 2: Configure DHCP 3: Configure Static IP 4: Reset all to DHCP 5: Set Default Adapter 6: View DNS Configuration 7: View Routes Press "x" to exit Enter command: 2 Available adapters: eth0 Enter Network Adapter: eth0 Reset to DHCP [y/n]: y Adapter eth0 set to use DHCP You must exit Network Configuration to complete this configuration. Press Return to Continue_</pre>

Pour	Faire ceci
Configurer une adresse IP statique pour la passerelle	<p>Saisissez 3.</p> <p>Vous êtes invité à entrer les informations suivantes pour configurer une adresse IP statique :</p> <ul style="list-style-type: none">• Nom de la carte réseau• Adresse IP• Masque réseau• Adresse de la passerelle par défaut• Adresse DNS principale• Adresse DNS secondaire <div data-bbox="829 1161 1511 1619" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Si votre passerelle a déjà été activée, vous devez l'arrêter et la redémarrer à partir de la console Storage Gateway pour que les paramètres prennent effet. Pour plus d'informations, consultez Arrêt de la machine virtuelle de la passerelle.</p></div> <p>Si votre passerelle utilise plusieurs interfaces réseau, vous devez définir toutes les interfaces</p>

Pour	Faire ceci
	<p>activées pour utiliser DHCP ou des adresses IP statiques.</p> <p>Par exemple, supposons que votre ordinateur virtuel de passerelle utilise deux interfaces configurées comme DHCP. Si vous définissez plus tard une interface à une adresse IP statique, l'autre interface est désactivée. Pour activer l'interface dans ce cas, vous devez la définir sur une adresse IP statique.</p> <p>Si les deux interfaces ont été définies au départ de façon à utiliser des adresses IP statiques et que vous définissez ensuite la passerelle de façon à utiliser le protocole DHCP, les deux interfaces utilisent DHCP.</p>
Réinitialiser la configuration du réseau de votre passerelle sur DHCP	<p>Saisissez 4.</p> <p>Toutes les interfaces réseau sont programmées pour utiliser le protocole DHCP.</p> <div data-bbox="829 1245 1507 1703" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Si votre passerelle a déjà été activée, vous devez l'arrêter et la redémarrer à partir de la console Storage Gateway pour que les paramètres prennent effet. Pour plus d'informations, consultez Arrêt de la machine virtuelle de la passerelle.</p></div>

Pour	Faire ceci
Définir la carte de routage par défaut de la passerelle	<p>Saisissez 5.</p> <p>Les cartes disponibles pour votre passerelle sont affichées et vous êtes invité à choisir l'une des cartes, par exemple, eth0.</p>
Modifier la configuration DNS de la passerelle	<p>Saisissez 6.</p> <p>Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent. Vous êtes invité à indiquer la nouvelle adresse IP.</p>
Afficher la configuration DNS de la passerelle	<p>Saisissez 7.</p> <p>Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent.</p> <div data-bbox="829 1041 1507 1304" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Pour certaines versions de l'hyperviseur VMware, vous pouvez modifier la configuration de la carte dans ce menu.</p></div>
Consultation des tables de routage	<p>Saisissez 8.</p> <p>La route par défaut de votre passerelle s'affiche</p> <p>.</p>

Test de la connectivité réseau de votre passerelle

Vous pouvez utiliser la console locale de la passerelle afin de tester la connectivité de votre réseau. Ce test peut être utile lorsque vous dépannez des problèmes de réseau avec votre passerelle.

Pour tester la connectivité réseau de la passerelle

1. Connectez-vous à la console locale de la passerelle :
 - Pour plus d'informations sur la journalisation dans la console locale VMware ESXi, consultez [Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Pour plus d'informations sur la journalisation dans la console locale Microsoft Hyper-V, consultez [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).
 - Pour plus d'informations sur la journalisation dans la console locale KVM, consultez [Accès à la console locale de la passerelle avec Linux KVM](#).
2. De l'AWSActivation de l'appliance - Configuration menu principal, entrez le chiffre correspondant à sélectionner Test de la connectivité réseau.

Si votre passerelle a déjà été activée, le test de connectivité commence immédiatement. Pour les passerelles qui n'ont pas encore été activées, vous devez spécifier le type de point de terminaison et Région AWS comme décrit dans les étapes suivantes.

3. Si votre passerelle n'est pas encore activée, entrez le chiffre correspondant pour sélectionner le type de point de terminaison de votre passerelle.
4. Si vous avez sélectionné le type de point de terminaison public, entrez le chiffre correspondant pour sélectionner la case Région AWS que vous souhaitez tester. Pour prise en charge Régions AWS et une liste de AWS points de terminaison de service que vous pouvez utiliser avec Storage Gateway, voir [AWS Storage Gateway Points de terminaison et quotas](#) dans le AWS Référence générale.

Au fur et à mesure que le test progresse, chaque point de terminaison affiche [REUSSITE] ou [ECHEC], indiquant l'état de la connexion comme suit :

Message	Description
[REUSSITE]	Storage Gateway possède une connectivité réseau.
[ECHEC]	Storage Gateway ne dispose pas de connectivité réseau.

Affichage de l'état des ressources système de votre passerelle

Lorsque votre passerelle démarre, elle vérifie les cœurs virtuels du processeur, la taille du volume racine et la RAM. Elle détermine ensuite si ces ressources système (cœurs virtuels du processeur, taille du volume racine et RAM) sont suffisantes pour que la passerelle fonctionne correctement. Vous pouvez afficher les résultats de ce contrôle sur la console locale de la passerelle.

Pour afficher le statut d'un contrôle de ressource du système

1. Connectez-vous à la console locale de la passerelle :
 - Pour plus d'informations sur la journalisation dans la console VMware ESXi, consultez [Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Pour plus d'informations sur la journalisation dans la console locale Microsoft Hyper-V, consultez [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).
 - Pour plus d'informations sur la journalisation dans la console locale KVM, consultez [Accès à la console locale de la passerelle avec Linux KVM](#).
2. Dans AWS Activation de l'appliance - Configuration Menu principal, saisissez 4 pour afficher les résultats de la vérification des ressources du système.

```

AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: Command Prompt

Press "x" to exit session

Enter command: _

```

La console affiche un message [OK], [Avertissement] ou [ECHEC] pour chaque ressource, comme décrit dans le tableau suivant.

Message	Description
[OK]	La ressource a réussi le contrôle des ressources système.
[AVERTISSEMENT]	La ressource ne respecte pas les exigences recommandées, mais la passerelle peut continuer à fonctionner. Storage Gateway affiche un message qui décrit les résultats de la vérification de la ressource.
[ECHEC]	La ressource ne répond pas à la configuration minimum requise. Il est possible que votre passerelle ne fonctionne pas correctement. Storage Gateway affiche un message qui décrit les résultats de la vérification de la ressource.

La console affiche également le nombre d'erreurs et d'avertissements en regard de l'option de menu de contrôle de la ressource.

Configuration d'un serveur NTP (Network Time Protocol) pour votre passerelle

Vous pouvez afficher et modifier les configurations de serveur NTP et synchroniser l'heure de l'ordinateur virtuel sur votre passerelle avec l'hôte de l'hyperviseur.

Pour gérer l'heure système

1. Connectez-vous à la console locale de la passerelle :
 - Pour plus d'informations sur la journalisation dans la console locale VMware ESXi, consultez [Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Pour plus d'informations sur la journalisation dans la console locale Microsoft Hyper-V, consultez [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).
 - Pour plus d'informations sur la journalisation dans la console locale KVM, consultez [Accès à la console locale de la passerelle avec Linux KVM](#).

2. Dans AWS Activation de l'apppliance - Configuration Menu principal, saisissez 5 pour gérer le temps de votre système.

```

AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: Command Prompt

Press "x" to exit session

Enter command: _

```

3. Dans le menu System Time Management (Gestion de l'heure système), choisissez l'une des options suivantes.

```

System Time Management

1: View and Synchronize System Time
2: Edit NTP Configuration
3: View NTP Configuration

Press "x" to exit
Enter command: _

```

Pour	Faire ceci
Afficher et synchroniser l'heure de votre ordinateur virtuel avec l'heure du serveur NTP.	Saisissez 1 . L'heure actuelle de votre ordinateur virtuel s'affiche. Votre passerelle de fichiers détermine la différence de temps à partir de votre

Pour	Faire ceci
	<p>ordinateur virtuel de passerelle, et l'heure du serveur NTP vous invite à synchroniser l'heure de l'ordinateur virtuel avec l'heure NTP.</p> <p>Une fois que votre passerelle a été déployée et qu'elle est en cours d'exécution, l'heure de l'ordinateur virtuel de la passerelle peut dériver dans certains scénarios. Par exemple, supposons qu'une panne de réseau prolongée se produise et que l'hôte de l'hyperviseur et la passerelle ne reçoivent pas de mises à jour de l'heure. Dans ce cas, l'heure de l'ordinateur virtuel de la passerelle est différente de l'heure réelle. Lorsqu'il y a une dérive de l'heure, un écart se produit entre l'heure indiquée pour une opération telle que la réalisation d'un instantané et l'heure à laquelle cette opération s'est réellement produite.</p> <p>Pour une passerelle déployée sur VMware ESXi, la définition de l'heure de l'hôte de l'hyperviseur et la synchronisation de l'heure de l'ordinateur virtuel sur l'hôte suffisent pour éviter la dérive de l'heure. Pour plus d'informations, consultez Synchronisation de l'heure de l'ordinateur virtuel et de celle de l'hôte.</p> <p>Pour une passerelle déployée sur Microsoft Hyper-V, vérifiez régulièrement l'heure de l'ordinateur virtuel. Pour plus d'informations, consultez Synchronisation de l'heure de l'ordinateur virtuel de la passerelle.</p> <p>Pour une passerelle déployée sur KVM, vous pouvez vérifier et synchroniser l'heure de la</p>

Pour	Faire ceci
	machine virtuelle à l'aide de l'interface de ligne de commande <code>virsh</code> pour KVM.
Modifier la configuration du serveur NTP	Saisissez 2 . Vous êtes invité à entrer un serveur NTP principal et secondaire.
Afficher la configuration du serveur NTP	Saisissez 3 . La configuration de votre serveur NTP s'affiche .

Exécution de commandes Storage Gateway sur la console locale

La console locale de l'ordinateur virtuel dans Storage Gateway permet de fournir un environnement sécurisé pour la configuration et le diagnostic des problèmes avec votre passerelle. En utilisant les commandes de la console locale, vous pouvez exécuter des tâches de maintenance telles que l'enregistrement des tables de routage, la connexion à Amazon Web Services Support, etc.

Pour exécuter une commande de configuration ou de diagnostic

1. Connectez-vous à la console locale de la passerelle :
 - Pour plus d'informations sur la journalisation dans la console locale VMware ESXi, consultez [Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Pour plus d'informations sur la journalisation dans la console locale Microsoft Hyper-V, consultez [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).
 - Pour plus d'informations sur la journalisation dans la console locale KVM, consultez [Accès à la console locale de la passerelle avec Linux KVM](#).
2. Dans la page AWS Activation de l'appliance - Configuration Menu principal, saisissez **6** pour Inviter de commande.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: Command Prompt

Press "x" to exit session

Enter command: _
```

3. Dans la pageAWSActivation de la solution matérielle-inviteconsole, entrezh, puis appuyez surRetourclé.

La console affiche le menu AVAILABLE COMMANDS (COMMANDES DISPONIBLES) avec la fonction des commandes, comme illustré dans la capture d'écran suivante.

```
AVAILABLE COMMANDS
ip Show / manipulate routing, devices, and tunnels
save-routing-table Save newly added routing table entry
ifconfig View or configure network interfaces
iptables Administration tool for IPv4 packet filtering and NAT
save-iptables Persist IP tables
passwd Update authentication tokens
open-support-channel Connect to AWS Support
h Display available command list
exit Return to Configuration menu

Command: _
```

4. À l'invite de commande, entrez la commande que vous souhaitez utiliser et suivez les instructions.

Pour en savoir plus sur une commande, entrez le nom de la commande à l'invite de commande.

Configuration des cartes réseau pour votre passerelle

Par défaut, Storage Gateway est configuré pour utiliser le type de carte réseau E1000, mais vous pouvez reconfigurer votre passerelle pour utiliser la carte réseau VMXNET3 (10 GbE). Vous pouvez également configurer Storage Gateway afin d'y accéder par plusieurs adresses IP. Pour cela, configurez votre passerelle de façon à utiliser plusieurs cartes réseau.

Rubriques

- [Configurer votre passerelle pour utiliser la carte réseau VMXNET3](#)

Configurer votre passerelle pour utiliser la carte réseau VMXNET3

Storage Gateway prend en charge le type de carte réseau E1000 chez les hôtes VMware ESXi et Microsoft Hyper-V Hypervisor. Toutefois, le type de carte réseau VMXNET3 (10 GbE) est pris en charge dans l'hyperviseur VMware ESXi uniquement. Si la passerelle est hébergée sur un hyperviseur VMware ESXi, vous pouvez reconfigurer la passerelle de façon à utiliser la carte VMXNET3 (10 GbE). Pour plus d'informations sur cette carte, consultez le [site Web de VMware](#).

Pour les hôtes de l'hyperviseur KVM, Storage Gateway prend en charge l'utilisation de `virtio` pilotes de périphériques réseau. L'utilisation du type de carte réseau E1000 pour les hôtes KVM n'est pas prise en charge.

Important

Pour sélectionner VMXNET3, votre type de système d'exploitation invité doit être Other Linux64 (Autre Linux64).

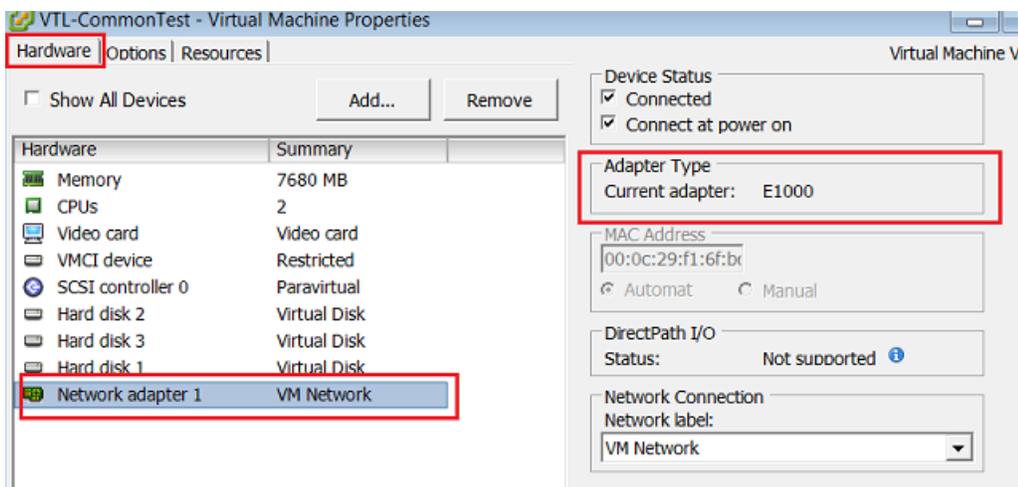
Voici les étapes à suivre pour configurer votre passerelle de façon à utiliser la carte VMXNET3 :

1. Supprimez la carte E1000 par défaut.
2. Ajoutez la carte VMXNET3.
3. Redémarrez la passerelle.
4. Configurez la carte pour le réseau.

Voici des détails sur chaque étape.

Pour supprimer la carte E1000 par défaut et configurer votre passerelle de façon à utiliser la carte VMXNET3

1. Dans VMware, ouvrez le menu contextuel (clic droit) pour la passerelle, puis choisissez Modifier les paramètres.
2. Dans la fenêtre Propriétés de l'ordinateur virtuel, choisissez l'onglet Matériel.
3. Pour Matériel, choisissez Carte réseau. Notez que la carte actuelle est E1000 dans la section Adapter Enter (Entrée de carte). Vous remplacez cette carte par la carte VMXNET3.



4. Sélectionnez la carte réseau E1000, puis choisissez Supprimer. Dans cet exemple, la carte réseau E1000 est Carte réseau 1.

Note

Bien que vous puissiez exécuter les cartes réseau E1000 et VMXNET3 dans votre passerelle en même temps, il est déconseillé de le faire, car cela peut entraîner des problèmes de réseau.

5. Choisissez Ajouter pour ouvrir l'assistant Ajouter du matériel.
6. Choisissez Carte Ethernet, puis sélectionnez Suivant.
7. Dans l'assistant d'entrée de réseau, sélectionnez **VMXNET3** pour Adapter Enter (Entrée de carte), puis choisissez Next (Suivant).
8. Dans l'assistant des propriétés de l'ordinateur virtuel, vérifiez dans la section Adapter Enter (Entrée de carte) que Current Adapter (Carte actuelle) est définie sur VMXNET3, puis choisissez OK.
9. Dans le client VMware VSphere, arrêtez votre passerelle.

10. Dans le client VMware VSphere, redémarrez votre passerelle.

Après le redémarrage de votre passerelle, reconfigurez la carte que vous venez d'ajouter pour vous assurer que la connectivité réseau à Internet est établie.

Pour configurer la carte pour le réseau

1. Dans le client VSphere, sélectionnez l'onglet Console pour démarrer la console locale. Utilisez les informations d'identification de connexion par défaut pour vous connecter à la console locale de la passerelle pour cette tâche de configuration. Pour obtenir plus d'informations sur la connexion à l'aide des informations d'identification par défaut, consultez [Connexion à la console locale de la passerelle de fichiers](#).

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: Command Prompt

Press "x" to exit session

Enter command: _
```

2. A l'invite, entrez **2** pour sélectionner Network Configuration (Configuration du réseau), puis appuyez sur **Enter** pour ouvrir le menu de configuration du réseau.

3. A l'invite, entrez **4** pour sélectionner Reset all to DHCP (Tout réinitialiser sur DHCP), puis entrez **y** (pour confirmer) à l'invite pour que toutes les cartes utilisent le protocole DHCP. Toutes les cartes disponibles sont définies pour utiliser le protocole DHCP.

```
AWS Storage Gateway Network Configuration
1: Describe Adapter
2: Configure DHCP
3: Configure Static IP
4: Reset all to DHCP
5: Set Default Adapter
6: View DNS Configuration
7: View Routes

Press "x" to exit

Enter command: 2

Available adapters: eth0
Enter Network Adapter: eth0

Reset to DHCP [y/n]: y

Adapter eth0 set to use DHCP

You must exit Network Configuration to complete this configuration.
Press Return to Continue_
```

Si votre passerelle a déjà été activée, vous devez l'arrêter et la redémarrer à partir de Storage Gateway Management Console. Après le redémarrage de la passerelle, vous devez tester la connectivité réseau à Internet. Pour plus d'informations sur le test de la connectivité réseau, consultez [Test de la connectivité réseau de votre passerelle](#).

Exécution de tâches sur la console locale Amazon EC2 (passerelle de fichiers)

Certaines tâches de maintenance nécessitent une connexion à la console locale lors de l'exécution d'une passerelle déployée sur une instance Amazon EC2. Dans cette section, vous trouverez des informations sur la connexion à la console locale et l'exécution des tâches de maintenance.

Rubriques

- [Connexion à la console locale de votre passerelle Amazon EC2](#)
- [Routage de votre passerelle déployée sur EC2 via un proxy HTTP](#)
- [Configuration des paramètres réseau de votre passerelle](#)
- [Test de la connectivité réseau de votre passerelle](#)
- [Affichage de l'état des ressources système de votre passerelle](#)

- [Exécution de commandes Storage Gateway sur la console locale](#)

Connexion à la console locale de votre passerelle Amazon EC2

Vous pouvez vous connecter à une instance Amazon EC2 à l'aide d'un client SSH (Secure Shell). Pour plus d'informations, consultez [Connectez-vous à votre instance](#) dans le Guide de l'utilisateur Amazon EC2. Pour ce type de connexion, vous avez besoin de la paire de clés SSH que vous avez spécifiée lorsque vous avez lancé votre instance. Pour en savoir plus sur les paires de clés Amazon EC2, consultez [Paires de clés Amazon EC2](#) dans le Guide de l'utilisateur Amazon EC2.

Pour se connecter à la console locale de la passerelle

1. Connectez-vous à votre console locale. Si vous vous connectez à votre instance EC2 à partir d'un ordinateur Windows, connectez-vous en tant qu'administrateur.
2. Une fois que vous connecté, vous voyez leAWSActivation de l'appliance - Configurationcomme illustré dans la capture d'écran suivante.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

Pour en savoir plus	Consultez cette rubrique
Configurer un proxy HTTP pour la passerelle	Routage de votre passerelle déployée sur EC2 via un proxy HTTP
Configurer les paramètres réseau pour votre passerelle	Test de la connectivité réseau de votre passerelle
Testez la connectivité réseau	Test de la connectivité réseau de votre passerelle
Consulter le contrôle d'une ressource système	Connexion à la console locale de votre passerelle Amazon EC2.
Exécutez les commandes de la console Storage	Exécution de commandes Storage Gateway sur la console locale

Pour arrêter la passerelle, entrez **0**.

Pour quitter la session de configuration, entrez **x** pour quitter le menu.

Routage de votre passerelle déployée sur EC2 via un proxy HTTP

Storage Gateway prend en charge la configuration d'un proxy Secure Socket 5 (SOCKS5) entre la passerelle déployée sur Amazon EC2 et AWS.

Si votre passerelle doit utiliser un serveur proxy pour communiquer avec Internet, vous devez configurer les paramètres de proxy HTTP de la passerelle. Pour cela, spécifiez un numéro de port et une adresse IP pour l'hôte exécutant le proxy. Ensuite, Storage Gateway achemine tous les AWSTrafic des points de terminaison via le serveur proxy. Les communications entre la passerelle et les points de terminaison sont chiffrées, même lorsque vous utilisez le proxy HTTP.

Pour acheminer le trafic Internet de la passerelle via un serveur proxy local

1. Connectez-vous à la console locale de la passerelle. Pour obtenir des instructions, consultez [Connexion à la console locale de votre passerelle Amazon EC2](#).
2. Dans la page AWSActivation de l'appliance - ConfigurationMenu principal, saisissez **1** Pour commencer à configurer le proxy HTTP.

```

AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █

```

3. Choisissez l'une des options suivantes dans laAWSActivation de l'appliance - ConfigurationConfiguration d'un proxy HTTPmenu.

```

AWS Appliance Activation HTTP Proxy Configuration

Note: setting is only applicable to AWS Storage Gateway

1: Configure HTTP Proxy
2: View Current HTTP Proxy Configuration
3: Remove HTTP Proxy Configuration

Press "x" to exit

Enter command: █

```

Pour	Procédez comme suit
Configurer un proxy HTTP	

Pour	Procédez comme suit
	<p>Saisissez 1.</p> <p>Vous devez fournir un nom d'hôte et un port pour finaliser la configuration.</p>
Afficher la configuration actuelle du proxy HTTP	<p>Saisissez 2.</p> <p>Si aucun proxy HTTP n'est configuré, le message HTTP Proxy not configured s'affiche. Si un proxy HTTP est configuré, le nom d'hôte et le port du proxy s'affichent.</p>
Supprimer une configuration de proxy HTTP	<p>Saisissez 3.</p> <p>Le message HTTP Proxy Configuration Removed s'affiche.</p>

Configuration des paramètres réseau de votre passerelle

Vous pouvez afficher et configurer les paramètres de votre DNS (Domain Name Server) via la console locale.

Pour configurer votre passerelle de façon à utiliser des adresses IP statiques

1. Connectez-vous à la console locale de la passerelle. Pour obtenir des instructions, consultez [Connexion à la console locale de votre passerelle Amazon EC2](#).
2. Dans la page AWS Activation de l'appliance - Configuration Menu principal, saisissez **2** pour commencer à configurer votre serveur DNS.

```

AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █

```

3. Choisissez l'une des options suivantes dans le menu Network Configuration (Configuration du réseau).

```

AWS Appliance Activation - Network Configuration

1: Edit DNS Configuration
2: View DNS Configuration

Press "x" to exit

Enter command: █

```

Pour	Procédez comme suit
Modifier la configuration DNS de la passerelle	Saisissez 1 .

Pour	Procédez comme suit
	Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent. Vous êtes invité à indiquer la nouvelle adresse IP.
Afficher la configuration DNS de la passerelle	Saisissez 2 . Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent.

Test de la connectivité réseau de votre passerelle

Vous pouvez utiliser la console locale de la passerelle afin de tester la connectivité de votre réseau. Ce test peut être utile lorsque vous dépannez des problèmes de réseau avec votre passerelle.

Pour tester la connectivité de la passerelle

1. Connectez-vous à la console locale de la passerelle. Pour obtenir des instructions, consultez [Connexion à la console locale de votre passerelle Amazon EC2](#).
2. De l'AWSActivation de l'appliance - Configurationmenu principal, entrez le chiffre correspondant à sélectionnerTest de la connectivité réseau.

Si votre passerelle a déjà été activée, le test de connectivité commence immédiatement. Pour les passerelles qui n'ont pas encore été activées, vous devez spécifier le type de point de terminaison etRégion AWScomme décrit dans les étapes suivantes.

3. Si votre passerelle n'est pas encore activée, entrez le chiffre correspondant pour sélectionner le type de point de terminaison de votre passerelle.
4. Si vous avez sélectionné le type de point de terminaison public, entrez le chiffre correspondant pour sélectionner la caseRégion AWSque vous souhaitez tester. Pour prise en chargeRégions AWSet une liste deAWSpoints de terminaison de service que vous pouvez utiliser avec Storage Gateway, voir[AWS Storage GatewayPoints de terminaison et quotas](#)dans leAWSRéférence générale.

Au fur et à mesure que le test progresse, chaque point de terminaison affiche[REUSSITE]ou[ECHEC], indiquant l'état de la connexion comme suit :

Message	Description
[REUSSITE]	Storage Gateway possède une connectivité réseau.
[ECHEC]	Storage Gateway ne dispose pas de connectivité réseau.

Affichage de l'état des ressources système de votre passerelle

Lorsque votre passerelle démarre, elle vérifie les cœurs virtuels du processeur, la taille du volume racine et la RAM. Elle détermine ensuite si ces ressources système (cœurs virtuels du processeur, taille du volume racine et RAM) sont suffisantes pour que la passerelle fonctionne correctement. Vous pouvez afficher les résultats de ce contrôle sur la console locale de la passerelle.

Pour afficher le statut d'un contrôle de ressource du système

1. Connectez-vous à la console locale de la passerelle. Pour obtenir des instructions, consultez [Connexion à la console locale de votre passerelle Amazon EC2](#).
2. Dans Configuration Storage Gateway Menu principal, saisissez **4** pour afficher les résultats de la vérification des ressources du système.

```

AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █

```

La console affiche un message [OK], [Avertissement] ou [ECHEC] pour chaque ressource, comme décrit dans le tableau suivant.

Message	Description
[OK]	La ressource a réussi le contrôle des ressources système.
[AVERTISSEMENT]	La ressource ne respecte pas les exigences recommandées, mais la passerelle peut continuer à fonctionner. Storage Gateway affiche un message qui décrit les résultats de la vérification de la ressource.
[ECHEC]	La ressource ne répond pas à la configuration minimum requise. Il est possible que votre passerelle ne fonctionne pas correctement. Storage Gateway affiche un message qui décrit les résultats de la vérification de la ressource.

La console affiche également le nombre d'erreurs et d'avertissements en regard de l'option de menu de contrôle de la ressource.

Exécution de commandes Storage Gateway sur la console locale

La console AWS Storage Gateway permet de fournir un environnement sécurisé pour la configuration et le diagnostic des problèmes avec votre passerelle. En utilisant les commandes de la console, vous pouvez exécuter des tâches de maintenance telles que l'enregistrement des tables de routage ou la connexion à Amazon Web Services Support.

Pour exécuter une commande de configuration ou de diagnostic

1. Connectez-vous à la console locale de la passerelle. Pour obtenir des instructions, consultez [Connexion à la console locale de votre passerelle Amazon EC2](#).
2. Dans AWS Configuration d'activation de l'appliance Menu principal, saisissez 5 pour Console passerelle.

```
AWS Appliance Activation - Configuration
#####
## Currently connected network adapters:
##
## eth0: [REDACTED]
#####

1: Configure HTTP Proxy
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: Command Prompt

Press "x" to exit session

Enter command: █
```

3. À l'invite de commande, entrez **h** et appuyez sur la touche Retour.

La console affiche le menu AVAILABLE COMMANDS (COMMANDES DISPONIBLES) avec les commandes disponibles. Après le menu, une invite de console de passerelle s'affiche, comme illustré dans la capture d'écran suivante.

```
AVAILABLE COMMANDS
ip                Show / manipulate routing, devices, and tunnels
save-routing-table Save newly added routing table entry
ifconfig         View or configure network interfaces
iptables        Administration tool for IPv4 packet filtering and NAT
save-iptables    Persist IP tables
open-support-channel Connect to AWS Support
h               Display available command list
exit            Return to Configuration menu

Command: █
```

4. À l'invite de commande, entrez la commande que vous souhaitez utiliser et suivez les instructions.

Pour en savoir plus sur une commande, entrez le nom de la commande à l'invite de commande.

Accès à la console locale de la passerelle

La manière dont vous accédez à la console locale de votre ordinateur virtuel dépend du type de l'hyperviseur sur lequel vous avez déployé votre ordinateur virtuel de passerelle. Dans cette section, vous trouverez des informations sur la façon d'accéder à la console locale de la machine virtuelle à l'aide de KVM (machine virtuelle basée sur le noyau Linux), VMware ESXi et de Microsoft Hyper-V Manager.

Rubriques

- [Accès à la console locale de la passerelle avec Linux KVM](#)
- [Accès à la console locale de la passerelle avec VMware ESXi](#)
- [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#)

Accès à la console locale de la passerelle avec Linux KVM

La configuration des machines virtuelles exécutées sur KVM varie en fonction de la distribution Linux utilisée. Suivez les instructions ci-dessous pour accéder aux options de configuration KVM à partir de la ligne de commande. Les instructions peuvent varier en fonction de votre implémentation KVM.

Pour accéder à la console locale de la passerelle avec KVM

1. Utilisez la commande suivante pour répertorier les machines virtuelles actuellement disponibles dans KVM.

```
# virsh list
```

Vous pouvez choisir les machines virtuelles disponibles par Id.

```
[[root@localhost vms]# virsh list
 Id   Name           State
-----
 7    SGW_KVM        running

[[root@localhost vms]# virsh console 7
```

2. Utilisez la commande suivante pour accéder à la console locale.

```
# virsh console VM_Id
```

```
[[root@localhost vms]# virsh console 7
Connected to domain SGW_KVM
Escape character is ^]

AWS Appliance

Login to change your network configuration and other settings.
localhost login: _
```

3. Pour obtenir les informations d'identification par défaut pour se connecter à la console locale, consultez [Connexion à la console locale de la passerelle de fichiers](#).
4. Une fois connecté, vous pouvez activer et configurer votre passerelle.

```
AWS Appliance Activation - Configuration

#####
## Currently connected network adapters:
##
## eth0: 10.0.3.32
#####

1: HTTP/SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: View System Resource Check (0 Errors)
5: System Time Management
6: License Information
7: Command Prompt

0: Get activation key

Press "x" to exit session

Enter command: _
```

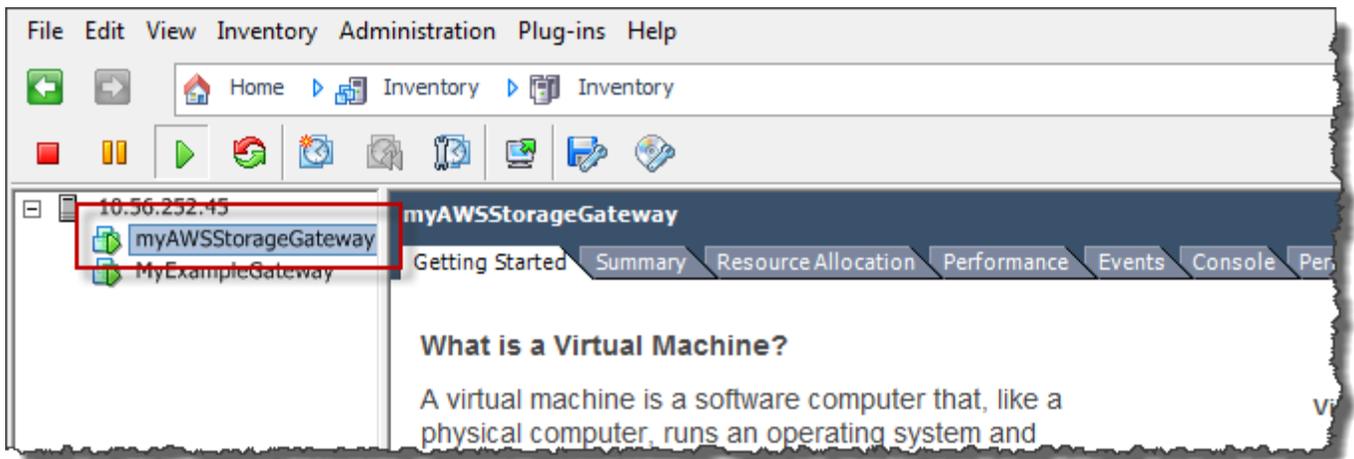
Accès à la console locale de la passerelle avec VMware ESXi

Pour accéder à la console locale de la passerelle avec VMware ESXi

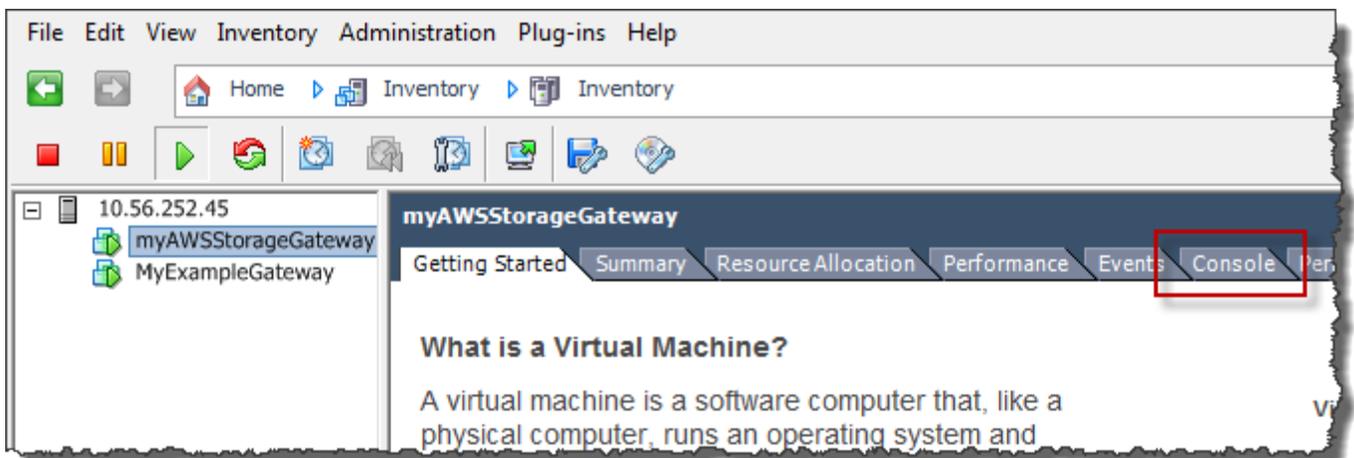
1. Dans le client VMware vSphere, sélectionnez l'ordinateur virtuel de la passerelle.
2. Vérifiez que la passerelle est activée.

Note

Si l'ordinateur virtuel de la passerelle est activé, une icône représentant une flèche verte s'affiche avec l'icône de l'ordinateur virtuel, comme illustré dans la capture d'écran suivante. Si l'ordinateur virtuel de la passerelle n'est pas activé, vous pouvez l'allumer en choisissant l'icône verte Marche sur le menu de la Barre d'outils.



3. Choisissez l'onglet Console.



Après quelques instants, l'ordinateur virtuel est prêt pour votre connexion.

Note

Pour libérer le curseur de la fenêtre de console, appuyez sur Ctrl+Alt.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Pour vous connecter à l'aide des informations d'identification par défaut, passez à la procédure [Connexion à la console locale de la passerelle de fichiers](#).

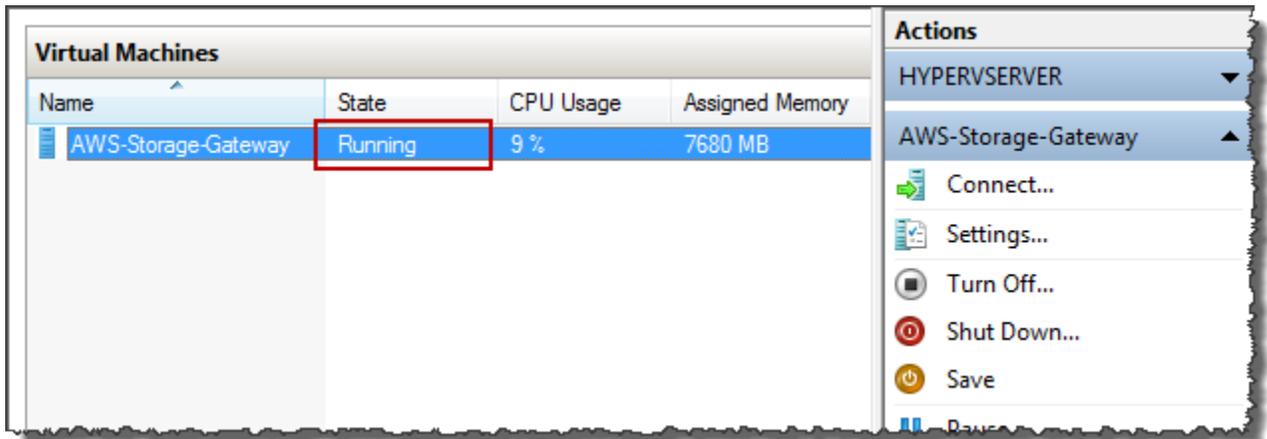
Accéder à la console locale de passerelle avec Microsoft Hyper-V

Pour accéder à la console locale de votre passerelle (Microsoft Hyper-V)

1. Dans la liste Ordinateurs virtuels de Microsoft Hyper-V Manager, sélectionnez l'ordinateur virtuel de la passerelle.
2. Vérifiez que la passerelle est activée.

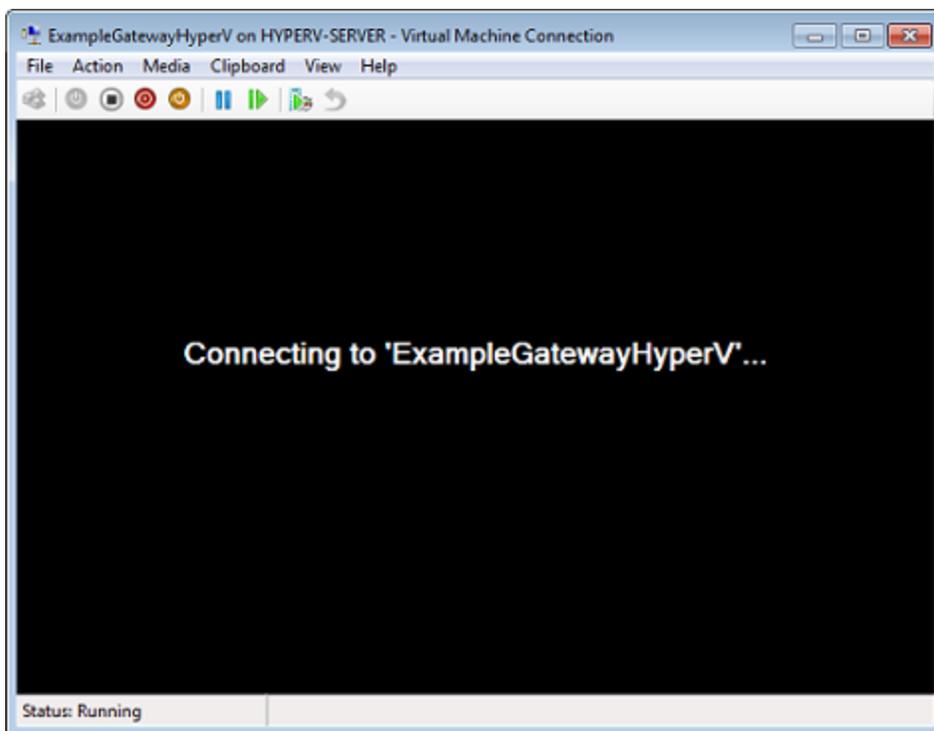
Note

Si l'ordinateur virtuel de la passerelle est activé, Running s'affiche afin d'indiquer l'état de l'ordinateur virtuel, comme illustré dans la capture d'écran suivante. Si l'ordinateur virtuel de la passerelle n'est pas activé, vous pouvez l'allumer en choisissant Démarrer dans le volet Actions.



3. Dans le volet Actions, choisissez Se connecter.

La fenêtre Connexion de l'ordinateur virtuel s'affiche. Si une fenêtre d'authentification s'affiche, tapez le nom d'utilisateur et le mot de passe qui vous ont été fournis par l'administrateur de l'hyperviseur.



Après quelques instants, l'ordinateur virtuel est prêt pour votre connexion.

```
AWS Storage Gateway

Login to change your network configuration and other gateway settings.

For more information, please see:
https://docs.aws.amazon.com/console/storagegateway/LocalConsole

localhost login: _
```

4. Pour vous connecter à l'aide des informations d'identification par défaut, passez à la procédure [Connexion à la console locale de la passerelle de fichiers](#).

Configuration des cartes réseau pour la passerelle

Dans cette section, vous trouverez des informations sur la manière de configurer plusieurs cartes réseau pour votre passerelle.

Rubriques

- [Configuration de votre passerelle pour plusieurs cartes réseau sur un hôte VMware ESXi](#)
- [Configuration de votre passerelle pour plusieurs cartes réseau sur un hôte Microsoft Hyper-V](#)

Configuration de votre passerelle pour plusieurs cartes réseau sur un hôte VMware ESXi

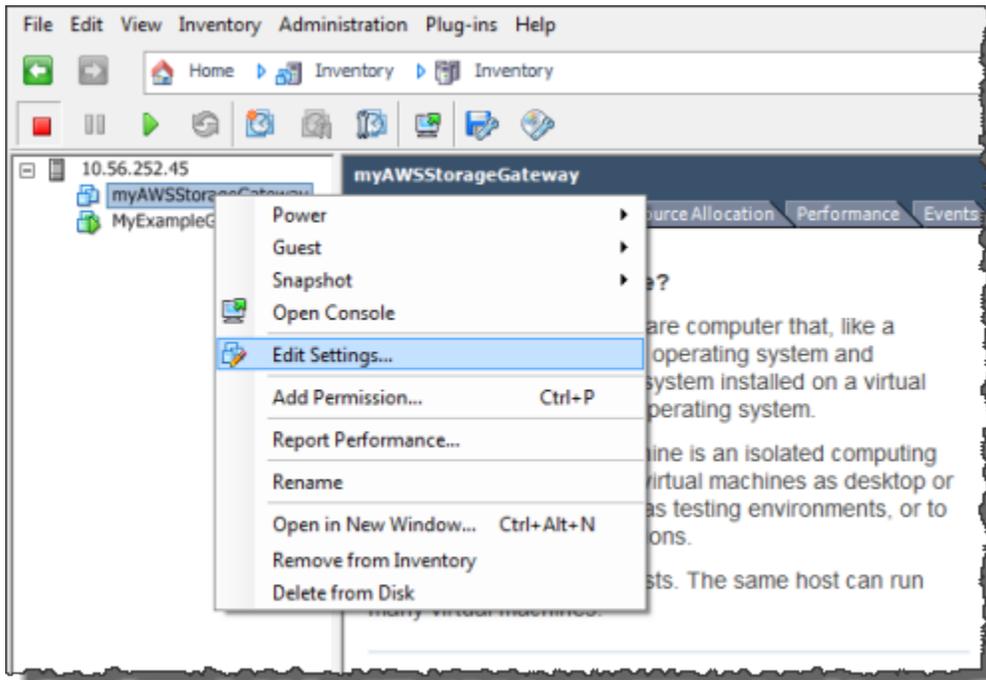
La procédure suivante suppose que l'ordinateur virtuel de la passerelle a déjà une carte réseau définie et que vous ajoutez une deuxième carte. La procédure suivante vous indique comment ajouter une carte pour VMware ESXi.

Pour configurer votre passerelle de façon à utiliser une carte réseau supplémentaire dans l'hôte VMware ESXi

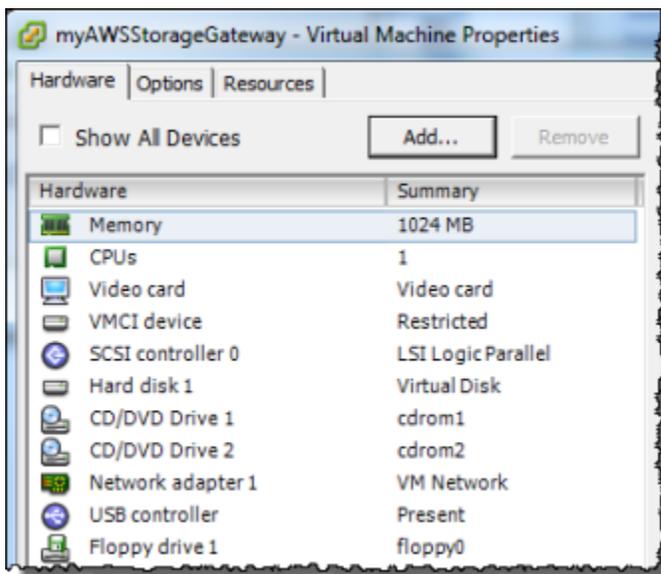
1. Arrêtez la passerelle.
2. Dans le client VMware vSphere, sélectionnez l'ordinateur virtuel de la passerelle.

L'ordinateur virtuel peut rester allumé pour cette procédure.

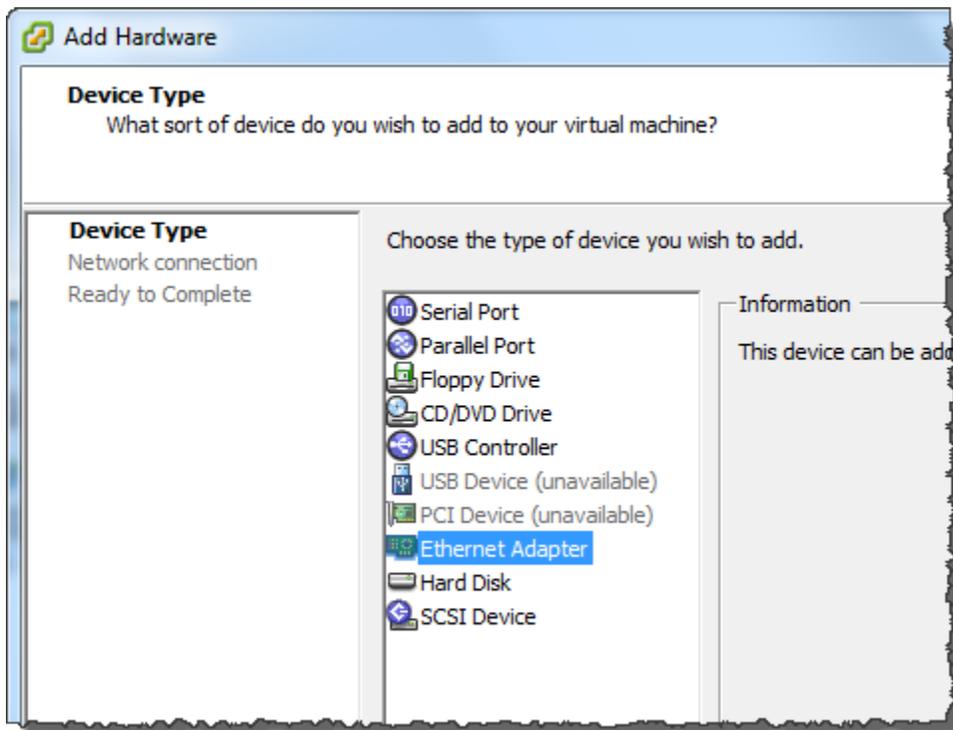
3. Dans le client, ouvrez le menu contextuel (clic droit) pour l'ordinateur virtuel de la passerelle, puis choisissez Modifier les paramètres.



4. Choisissez l'onglet Matériel de la boîte de dialogue Propriétés de l'ordinateur virtuel, puis choisissez Ajouter pour ajouter un appareil.



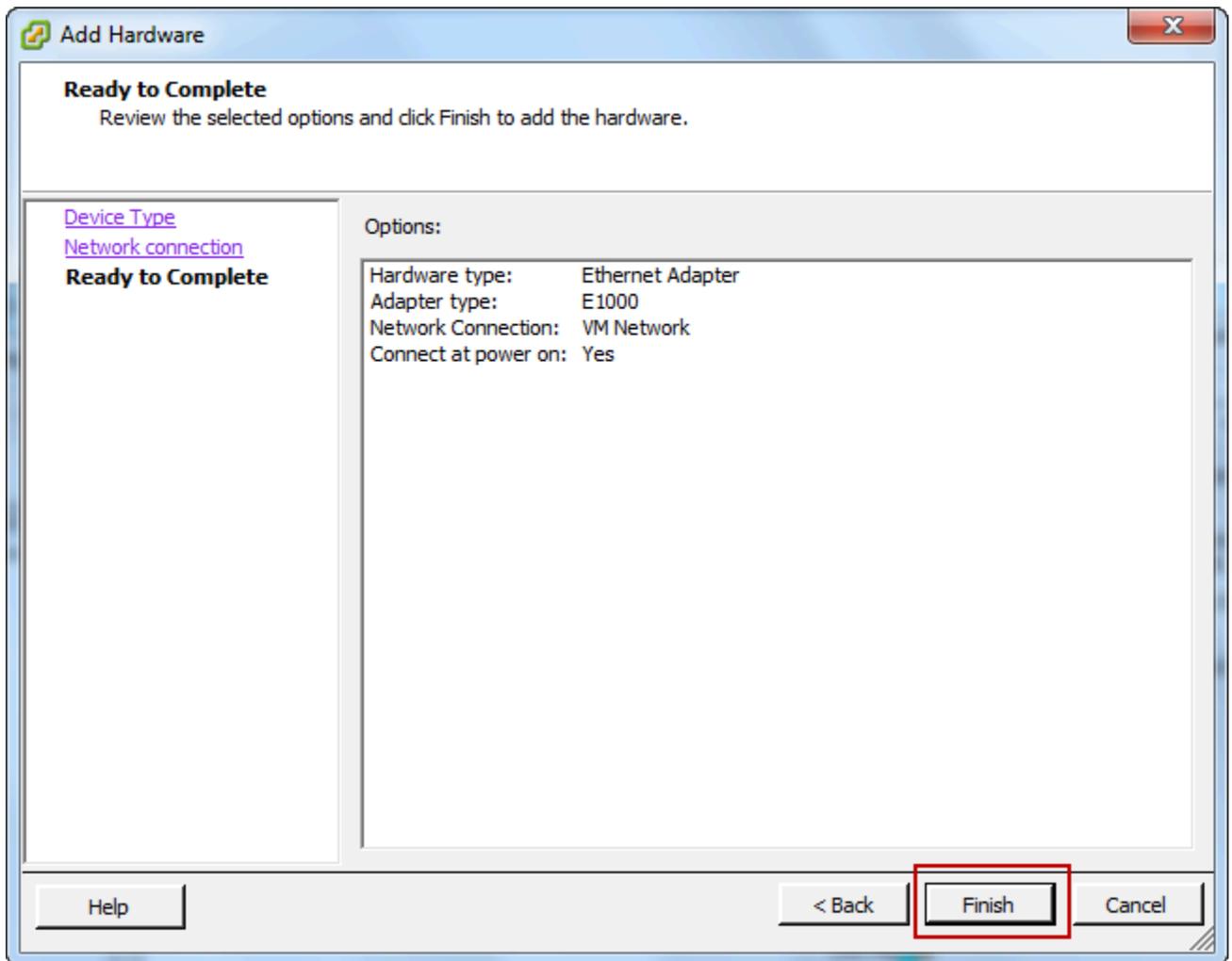
5. Suivez l'assistant Ajouter du matériel pour ajouter une carte réseau.
 - a. Dans le volet Type d'appareil, choisissez Carte Ethernet pour ajouter une carte, puis sélectionnez Suivant.



- b. Dans le volet Type de réseau, veillez à ce que l'option Se connecter lors de la mise sous tension soit sélectionnée pour Type, puis choisissez Suivant.

Nous vous recommandons d'utiliser la carte réseau E1000 avec Storage Gateway. Pour obtenir plus d'informations sur les types de cartes qui peuvent apparaître dans la liste des cartes, consultez Types de cartes réseau dans la [documentation sur ESXi et vCenter Server](#).

- c. Dans le volet Prêt à finaliser, vérifiez les informations, puis choisissez Terminer.

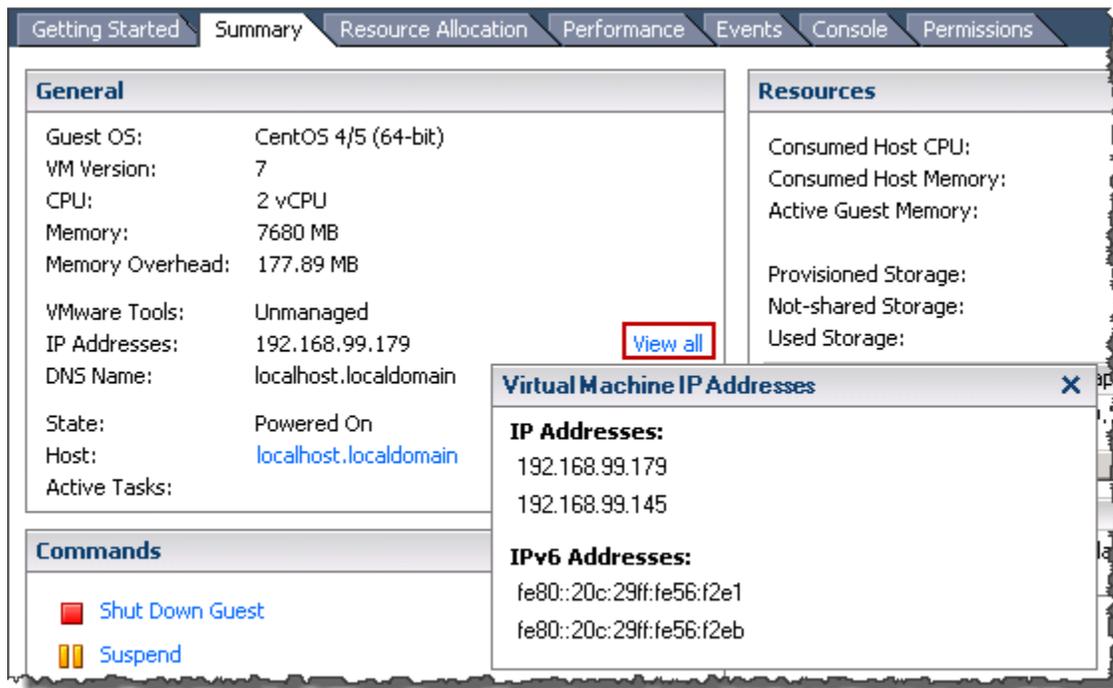


6. Choisissez l'onglet Résumé de l'ordinateur virtuel, puis sélectionnez Afficher tout en regard de la zone Adresse IP. Une fenêtre Adresses IP de l'ordinateur virtuel affiche toutes les adresses IP que vous pouvez utiliser pour accéder à la passerelle. Vérifiez qu'une deuxième adresse IP est répertoriée pour la passerelle.

Note

L'application des modifications de la carte et l'actualisation des informations de résumé de l'ordinateur virtuel peuvent prendre quelques instants.

L'image suivante est présentée à titre d'illustration uniquement. Dans la pratique, l'une des adresses IP sera l'adresse par laquelle la passerelle communique avec AWS et l'autre sera une adresse dans un autre sous-réseau.



7. Sur la console Storage Gateway, activez la passerelle.
8. Dans Navigation de la console Storage Gateway, choisissez Passerelles et choisissez la passerelle à laquelle vous avez ajouté la carte. Vérifiez que la deuxième adresse IP est répertoriée dans l'onglet Détails.

Pour plus d'informations sur les tâches de console locale communes aux hôtes VMware, Hyper-V et KVM, consultez [Exécution de tâches sur la console locale de la machine virtuelle \(passerelle de fichiers\)](#).

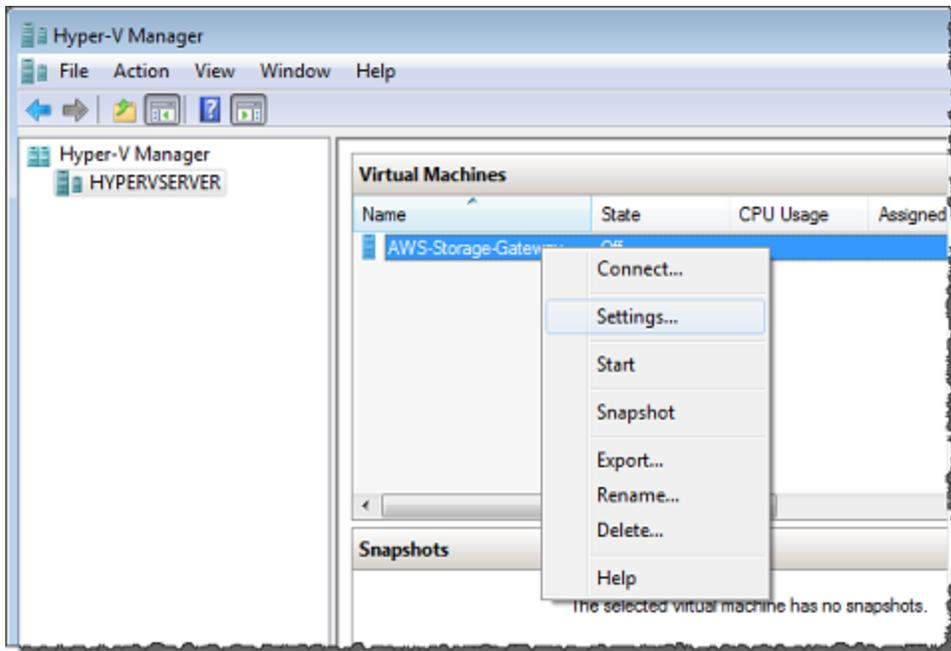
Configuration de votre passerelle pour plusieurs cartes réseau sur un hôte Microsoft Hyper-V

La procédure suivante suppose que l'ordinateur virtuel de la passerelle a déjà une carte réseau définie et que vous ajoutez une deuxième carte. Cette procédure montre comment ajouter une carte pour un hôte Microsoft Hyper-V.

Pour configurer votre passerelle afin d'utiliser une carte réseau supplémentaire dans un hôte Microsoft Hyper-V

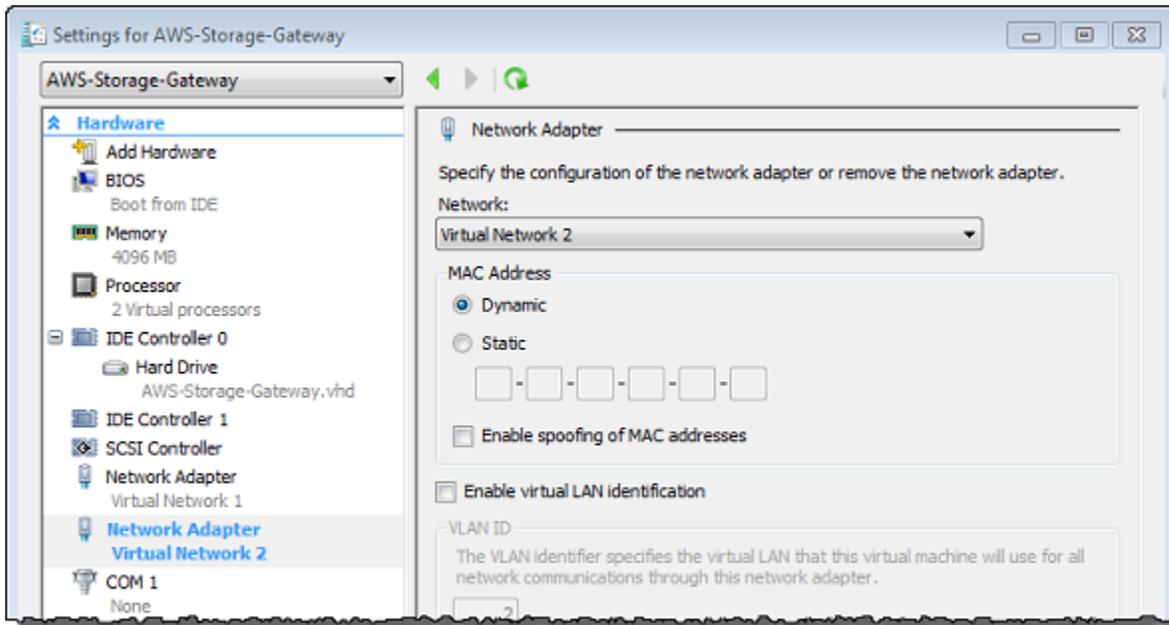
1. Sur la console Storage Gateway, désactivez la passerelle.
2. Dans Microsoft Hyper-V Manager, sélectionnez l'ordinateur virtuel de la passerelle.

3. Si l'ordinateur virtuel n'est pas encore éteint, ouvrez le menu contextuel (clic droit) pour votre passerelle et choisissez Eteindre.
4. Dans le client, ouvrez le menu contextuel de l'ordinateur virtuel de votre passerelle et choisissez Paramètres.



5. Dans la boîte de dialogue Paramètres pour l'ordinateur virtuel, pour Matériel, choisissez Ajouter du matériel.
6. Dans le volet Ajouter du matériel, choisissez Carte réseau, puis Ajouter pour ajouter un périphérique.
7. Configurez la carte réseau, puis choisissez Appliquer pour appliquer les paramètres.

Dans l'exemple suivant, Réseau virtuel 2 est sélectionné pour la nouvelle carte.



8. Dans la boîte de dialogue Paramètres, pour Matériel, vérifiez que la deuxième carte a été ajoutée, puis choisissez OK.
9. Sur la console Storage Gateway, activez la passerelle.
10. Dans le volet Navigation, choisissez Passerelles, puis sélectionnez la passerelle à laquelle vous avez ajouté la carte. Vérifiez que la deuxième adresse IP est répertoriée dans l'onglet Détails.

Pour plus d'informations sur les tâches de console locale communes aux hôtes VMware, Hyper-V et KVM, consultez [Exécution de tâches sur la console locale de la machine virtuelle \(passerelle de fichiers\)](#).

Suppression de votre passerelle à l'aide de la Console AWS Storage Gateway et suppression des ressources associées

Si vous n'avez l'intention de continuer à utiliser votre passerelle, pensez à supprimer la passerelle et ses ressources associées. La suppression des ressources évite la facturation de ressources que vous n'avez pas l'intention de continuer à utiliser et permet de réduire votre facture mensuelle.

Lorsque vous supprimez une passerelle, elle n'apparaît plus sur la console de gestion AWS Storage Gateway et sa connexion iSCSI à l'initiateur est fermée. La procédure de suppression d'une passerelle est identique pour tous les types de passerelle. Toutefois, en fonction du type de passerelle que vous souhaitez supprimer et de l'hôte sur lequel il est déployé, vous suivez les instructions de suppression des ressources associées.

Vous pouvez supprimer une passerelle à l'aide de la console Storage Gateway ou par programme. Vous trouverez ci-après des informations sur la suppression d'une passerelle à l'aide de la console Storage Gateway. Si vous souhaitez supprimer par programme votre passerelle, consultez [AWS Storage Gateway API Reference](#).

Rubriques

- [Suppression de votre passerelle à l'aide de la console Storage Gateway](#)
- [Suppression de ressources à partir d'une passerelle déployée sur site](#)
- [Suppression de ressources à partir d'une passerelle déployée sur une instance Amazon EC2](#)

Suppression de votre passerelle à l'aide de la console Storage Gateway

La procédure de suppression d'une passerelle est identique pour tous les types de passerelle. Toutefois, en fonction du type de passerelle que vous souhaitez supprimer et de l'hôte sur lequel la passerelle est déployée, vous devrez peut-être exécuter des tâches supplémentaires pour supprimer les ressources associées à la passerelle. La suppression de ces ressources vous aide à éviter de payer pour des ressources que vous n'avez pas l'intention d'utiliser.

Note

Pour les passerelles déployées sur une instance Amazon EC2, l'instance est conservée jusqu'à ce que vous la supprimiez.

Pour les passerelles déployés sur un ordinateur virtuel, une fois que vous avez supprimé la passerelle, l'ordinateur virtuel de la passerelle existe toujours dans votre environnement de virtualisation. Pour supprimer la machine virtuelle, utilisez le client VMware vSphere, Microsoft Hyper-V Manager ou le client KVM Linux pour vous connecter à l'hôte et supprimer la machine virtuelle. Notez que vous ne pouvez pas réutiliser l'ordinateur virtuel de la passerelle supprimée pour activer la nouvelle passerelle.

Supprimer une passerelle

1. Ouvrez la console Storage Gateway à l'adresse <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle que vous souhaitez supprimer.
3. Pour Actions, choisissez Delete stack (Supprimer la pile).

4.

⚠ Warning

Avant d'exécuter cette étape, veillez à ce qu'aucune application ne soit en train d'écrire sur les volumes de la passerelle. Si vous supprimez la passerelle alors qu'elle est en cours d'utilisation, une perte de données peut se produire.

Lorsqu'une passerelle est supprimée, il n'y a plus aucun moyen de la récupérer.

Dans la boîte de dialogue de confirmation qui s'affiche, activez la case à cocher afin de confirmer la suppression. Assurez-vous que l'ID de passerelle répertorié spécifie la passerelle à supprimer, puis choisissez Supprimer.

**⚠ Important**

Vous ne payez plus les frais de logiciels une fois que vous avez supprimé une passerelle, mais les ressources telles que les bandes virtuelles, les instantanés Amazon Elastic Block Store (Amazon EBS) et les instances Amazon EC2 restent. Vous continuerez à être facturé pour ces ressources. Vous pouvez choisir de supprimer des instances Amazon EC2 et des instantanés Amazon EBS en annulant votre abonnement Amazon EC2. Si vous souhaitez conserver votre abonnement Amazon EC2, vous pouvez supprimer vos instantanés Amazon EBS à l'aide de la console Amazon EC2.

Suppression de ressources à partir d'une passerelle déployée sur site

Vous pouvez utiliser les instructions suivantes pour supprimer les ressources à partir d'une passerelle déployée sur site.

Suppression de ressources à partir d'une passerelle de volume déployée sur un ordinateur virtuel

Si la passerelle à supprimer est déployée sur un ordinateur virtuel, nous vous recommandons de procéder comme suit pour nettoyer les ressources :

- Supprimez la passerelle.

Suppression de ressources à partir d'une passerelle déployée sur une instance Amazon EC2

Si vous souhaitez supprimer une passerelle que vous avez déployée sur une instance Amazon EC2, nous vous conseillons de nettoyer les ressources AWS qui ont été utilisées avec la passerelle, vous éviterez ainsi des coûts d'utilisation imprévus.

Suppression de ressources de vos volumes mis en cache déployés sur Amazon EC2

Si vous avez déployé une passerelle avec des volumes mis en cache sur EC2, nous vous recommandons de procéder comme suit pour supprimer votre passerelle, puis pour nettoyer ses ressources :

1. Sur la console Storage Gateway, supprimez la passerelle comme indiqué dans [Suppression de votre passerelle à l'aide de la console Storage Gateway](#).
2. Sur la console Amazon EC2, arrêtez votre instance EC2 si vous envisagez d'utiliser l'instance à nouveau. Sinon, mettez fin à l'instance. Si vous avez l'intention de supprimer des volumes, notez les appareils de bloc qui sont attachés à l'instance et les identificateurs des appareils avant de mettre fin à l'instance. Vous en aurez besoin pour identifier les volumes que vous souhaitez supprimer.
3. Dans la console Amazon EC2, supprimez tous les volumes Amazon EBS qui sont attachés à l'instance si vous ne prévoyez pas de les utiliser à nouveau. Pour de plus amples informations, veuillez consulter [Nettoyez votre instance et le volume](#) dans le Guide de l'utilisateur Amazon EC2 pour les instances Linux.

Remplacement de votre passerelle de fichiers existante par une nouvelle instance

Vous pouvez remplacer une passerelle de fichiers existante par une nouvelle instance à mesure que vos besoins en données et en performances augmentent, ou si vous recevez une notification AWS pour migrer votre passerelle. Cela peut être nécessaire si vous souhaitez déplacer votre passerelle vers une meilleure plateforme hôte ou des instances Amazon EC2 plus récentes, ou pour actualiser le matériel serveur sous-jacent.

Il existe deux méthodes pour remplacer une passerelle de fichiers existante. Le tableau suivant décrit les avantages et les inconvénients de chaque méthode. À l'aide de ces informations, sélectionnez la méthode la mieux adaptée à votre environnement de passerelle, puis reportez-vous aux étapes de la procédure dans la section correspondante ci-dessous.

	Méthode 1 : Migrer le disque cache et l'ID de passerelle vers une instance de remplacement	Méthode 2 : Instance de remplacement avec disque cache vide et nouvel ID de passerelle
Cache des données de disque	Les données du disque de cache sont conservées. Cette méthode est utile si votre passerelle possède un disque cache volumineux ou si vos applications sont sensibles au retard causé par les opérations de lecture hors cache.	Les données en cache sont téléchargées à partir du AWScloud. Cette méthode est optimale pour les charges de travail lourdes en écriture, si vos applications peuvent tolérer le retard causé par les lectures hors cache.
Temps d'arrêt	Votre passerelle sera hors ligne pendant 1 à 2 heures pendant le processus de migration.	Pas de temps d'arrêt. La passerelle existante peut être utilisée simultanément avec la passerelle de remplacement jusqu'à ce que vous décidiez de la supprimer. Plusieurs rédacteurs ne sont pas pris en charge lorsque les deux

	Méthode 1 : Migrer le disque cache et l'ID de passerelle vers une instance de remplacement	Méthode 2 : Instance de remplacement avec disque cache vide et nouvel ID de passerelle
		passerelles sont en cours d'utilisation.
ID de passerelle	La nouvelle passerelle hérite de l'ID de passerelle de la passerelle qu'elle remplace.	La passerelle existante et la passerelle de remplacement possèdent des ID de passerelle uniques et distincts.

 Note

Les données peuvent être déplacées uniquement entre des passerelles du même type.

Méthode 1 : Migrer le disque cache et l'ID de passerelle vers une instance de remplacement

Pour migrer le disque cache et l'ID de passerelle de votre passerelle File Gateway vers une instance de remplacement :

1. Arrêtez toutes les applications qui écrivent sur la passerelle de fichiers existante.
2. Vérifiez que le `CachePercentDirtyMetric` sur la surveillance pour la passerelle de fichiers existante est `0`.
3. Arrêtez la passerelle de fichiers existante en mettant hors tension la machine virtuelle hôte (VM) à l'aide de ses contrôles d'hyperviseur.

Pour plus d'informations sur l'arrêt d'une instance Amazon EC2, consultez [Arrêt et démarrage de votre instance](#) dans le Guide de l'utilisateur Amazon EC2.

Pour plus d'informations sur la fermeture d'une machine virtuelle KVM, VMware ou Hyper-V, consultez la documentation de votre hyperviseur.

- Détachez tous les disques, y compris le disque racine, les disques de cache et les disques tampons de chargement de l'ancienne machine virtuelle de passerelle.

 Note

Notez l'ID de volume du disque racine, ainsi que l'ID de passerelle associé à ce disque racine. Vous devrez détacher ce disque du nouvel hyperviseur Storage Gateway dans une étape ultérieure.

Si vous utilisez une instance Amazon EC2 en tant que machine virtuelle de votre passerelle de fichiers, consultez [Détachez un volume Amazon EBS d'une instance Windows](#) ou [Détachez un volume Amazon EBS d'une instance Linux](#) dans le Guide de l'utilisateur Amazon EC2.

Pour plus d'informations sur le détachement des disques d'une machine virtuelle KVM, VMware ou Hyper-V, consultez la documentation de votre hyperviseur.

- Création d'un nouveau AWS Instance de machine virtuelle de l'hyperviseur Storage Gateway, mais ne l'activez pas en tant que passerelle. Plus tard, cette nouvelle machine virtuelle assumera l'identité de l'ancienne passerelle.

Pour plus d'informations sur la création d'une nouvelle machine virtuelle hyperviseur Storage Gateway, consultez [Choix d'une plateforme hôte et téléchargement de la machine virtuelle](#).

 Note

N'ajoutez pas de disques de cache pour la nouvelle machine virtuelle. Cette machine virtuelle utilisera les mêmes disques de cache que ceux utilisés par l'ancienne machine virtuelle.

- Configurez votre nouvelle machine virtuelle Storage Gateway pour qu'elle utilise les mêmes paramètres réseau que l'ancienne machine virtuelle.

La configuration du réseau par défaut de la passerelle est le protocole de DHCP (Dynamic Host Configuration Protocol). Avec le protocole DHCP, votre passerelle reçoit automatiquement une adresse IP.

Si vous devez configurer manuellement une adresse IP statique pour votre machine virtuelle de passerelle, consultez [Configuration de votre passerelle réseau](#).

Si votre machine virtuelle de passerelle doit utiliser un proxy Secure Socket 5 (SOCKS5) pour se connecter à Internet, consultez [Routage de la passerelle sur site via un proxy](#).

7. Démarrez la nouvelle machine virtuelle Storage Gateway.
8. Attachez les disques que vous avez détachés de l'ancienne machine virtuelle de passerelle à la nouvelle machine virtuelle de passerelle. Ne détachez pas le disque racine existant de la nouvelle machine virtuelle de passerelle.

 Note

Pour réussir la migration, tous les disques doivent rester inchangés. La modification de la taille du disque ou d'autres valeurs entraîne des incohérences dans les métadonnées qui empêchent la migration réussie.

9. Lancez le processus de migration de passerelle en vous connectant à la nouvelle machine virtuelle à l'aide d'une URL qui utilise le format suivant :

`http://your-VM-IP-address/migrate?gatewayId=your-gateway-ID`

Vous pouvez utiliser la même adresse IP pour la nouvelle machine virtuelle de passerelle que celle utilisée pour l'ancienne machine virtuelle de passerelle. Votre URL doit être similaire à l'exemple suivant :

`http://198.51.100.123/migrate?gatewayId=sgw-12345678`

Utilisez cette URL depuis un navigateur ou depuis la ligne de commande à l'aide de cURL.

Lorsque la migration de la passerelle démarre correctement, le message suivant s'affiche :

```
Successfully imported Storage Gateway information. Please refer to Storage Gateway documentation to perform the next steps to complete the migration.
```

10. Attendez que l'état de la passerelle s'affiche sous forme *En cours d'exécution* dans le *AWSConsole Storage Gateway*. Selon la bande passante disponible, cette opération peut prendre jusqu'à 10 minutes.
11. Arrêtez la nouvelle VM Storage Gateway.
12. Détachez le disque racine de l'ancienne passerelle, dont vous avez noté l'ID de volume précédemment, de la nouvelle passerelle.
13. Démarrez la nouvelle machine virtuelle Storage Gateway.

14. Si votre passerelle a été jointe à un domaine Active Directory, rejoignez à nouveau le domaine. Pour obtenir des instructions, consultez [Configuration de l'accès à Microsoft Active Directory](#).

 Note

Vous devez effectuer cette étape même si l'état de la passerelle de fichiers apparaît comme suit :A rejoint.

15. Vérifiez que vos partages sont disponibles à l'adresse IP de la nouvelle machine virtuelle de passerelle, puis supprimez l'ancienne machine virtuelle de passerelle.

 Warning

Lorsqu'une passerelle est supprimée, il n'y a plus aucun moyen de la récupérer.

Pour plus d'informations sur la suppression d'une instance Amazon EC2, consultez [Résilier une instance](#) dans le Guide de l'utilisateur Amazon EC2. Pour plus d'informations sur la suppression d'une machine virtuelle KVM, VMware ou Hyper-V, consultez la documentation de votre hyperviseur.

Méthode 2 : Instance de remplacement avec disque cache vide et nouvel ID de passerelle

Pour configurer une instance de passerelle de fichiers de remplacement avec un disque cache vide et un nouvel ID de passerelle, procédez comme suit :

1. Arrêtez toutes les applications qui écrivent sur la passerelle de fichiers existante. Vérifiez que le `CachePercentDirtyMetric` sur la `SurveillanceTabulation` est `0` avant de configurer des partages de fichiers sur la nouvelle passerelle.
2. Utilisation de l'AWS Command Line Interface(AWS CLI) pour collecter et enregistrer les informations de configuration de votre passerelle de fichiers et de vos partages de fichiers existants en procédant comme suit :
 - a. Enregistrez les informations de configuration de la passerelle de la passerelle de fichiers.

```
aws storagegateway describe-gateway-information --gateway-arn
"arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Cette commande génère un bloc JSON contenant des métadonnées sur la passerelle telles que son nom, les interfaces réseau, le fuseau horaire configuré et son état (passerelle est en cours d'exécution).

- b. Enregistrez les paramètres SMB (Server Message Block) de la passerelle de fichiers.

```
aws storagegateway describe-smb-setting --gateway-arn
"arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Cette commande génère un bloc JSON contenant des métadonnées sur le partage de fichiers SMB, telles que son nom de domaine, l'état Microsoft Active Directory, si le mot de passe invité est défini et le type de stratégie de sécurité.

- c. Enregistrez les informations de partage de fichiers pour chaque partage de fichiers SMB et NFS (Network File System) de la passerelle de fichiers :
 - Utilisez la commande suivante pour les partages de fichiers SMB.

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
"arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

Cette commande génère un bloc JSON contenant des métadonnées sur le partage de fichiers NFS, telles que son nom, sa classe de stockage, son statut, son rôle Amazon Resource Name (ARN), une liste des clients autorisés à accéder à la passerelle de fichiers et le chemin d'accès utilisé par le client SMB pour identifier le point de montage.

- Utilisez la commande suivante pour les partages de fichiers NFS.

```
aws storagegateway describe-nfs-file-shares --file-share-arn-list
"arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

Cette commande génère un bloc JSON contenant des métadonnées sur le partage de fichiers NFS, telles que son nom, sa classe de stockage, son statut, son ARN de rôle IAM, une liste des clients autorisés à accéder à la passerelle de fichiers et le chemin d'accès utilisé par le client NFS pour identifier le point de montage.

3. Arrêtez la passerelle de fichiers existante en procédant comme suit :

- a. Arrêtez toutes les applications qui écrivent sur la passerelle de fichiers existante. Vérifiez que leCachePercentDirtyMetric sur laSurveillanceTabulation est0avant de configurer des partages de fichiers sur la nouvelle passerelle.
 - b. Arrêtez la passerelle de fichiers existante en mettant hors tension la machine virtuelle (VM) qui héberge la passerelle.
4. Créez une nouvelle passerelle de fichiers.
 5. Montez les partages de fichiers configurés sur l'ancienne passerelle.
 6. Vérifiez que votre nouvelle passerelle fonctionne correctement, puis supprimez l'ancienne passerelle de la console Storage Gateway.

 Important

Avant de supprimer une passerelle, assurez-vous qu'aucune application n'est en train d'écrire dans le cache de cette passerelle de fichiers. Si vous supprimez une passerelle de fichiers alors qu'elle est en cours d'utilisation, une perte de données peut se produire.

 Warning

Lorsqu'une passerelle est supprimée, il n'y a plus aucun moyen de la récupérer.

7. Supprimez l'ancienne machine virtuelle de passerelle ou l'instance EC2.

Performances

Dans cette section, vous trouverez des informations sur les performances de Storage Gateway.

Rubriques

- [Conseils sur les performances des passerelles de fichiers](#)
- [Optimisation des performances de la passerelle](#)
- [Utilisation de VMware vSphere High Availability avec Storage Gateway](#)

Conseils sur les performances des passerelles de fichiers

Dans cette section, vous trouverez des recommandations de configuration à des fins de mise en service du matériel pour la machine virtuelle de votre passerelle de fichiers. Les tailles et types d'instance Amazon EC2 répertoriés dans le tableau sont des exemples fournis à des fins de référence.

Pour obtenir les meilleures performances, la taille du disque de cache doit être adaptée à la taille de l'ensemble de travail actif. L'utilisation de plusieurs disques locaux pour le cache améliore les performances en écriture en mettant en parallèle l'accès aux données, ce qui entraîne une augmentation du nombre d'IOPS.

Dans les tableaux suivants, accès au cacheLes opérations de lecture sont des lectures à partir des partages de fichiers qui sont servis à partir du cache. Cache manquéLes opérations de lecture sont des lectures à partir des partages de fichiers qui sont servis depuis Amazon S3.

Note

Nous vous déconseillons d'utiliser le stockage éphémère. Pour de plus amples informations sur l'utilisation du stockage éphémère, veuillez consulter [Utilisation du stockage éphémère avec des passerelles EC2](#).

Voici des exemples de configurations de passerelle de fichiers.

Performances de passerelle de fichiers S3 sur les clients Linux

Exemples de configuration	Protocole	Débit d'écriture (taille de fichier 1 Go)	Débit de lecture d'accès au cache	Débit de lecture manquant du cache
Disque racine : 80 Go io1, 4 000 IOPS	NFSv3 - 1 filetage	110 Mib/sec (0,92 Gbit/s)	590 Mio/s (4,9 Gbit/s)	310 Mib/sec (2,6 Gbit/s)
	NFSv3 - 8 fils	160 Mio/s (1,3 Gbit/s)	590 Mio/s (4,9 Gbit/s)	335 Mio/s (2,8 Gbit/s)
Disque de cache : 512 GiB, io1, 1 500 E/S par seconde	NFSv4 - 1 filetage	130 Mib/sec (1,1 Gbit/s)	590 Mio/s (4,9 Gbit/s)	295 Mio/s (2,5 Gbit/s)
	NFSv4 - 8 fils	160 Mio/s (1,3 Gbit/s)	590 Mio/s (4,9 Gbit/s)	335 Mio/s (2,8 Gbit/s)
Performances réseau minimales : 10 Gbit/s	SMBv3 - 1 filetage	115 Mio/s (1,0 Gbit/s)	325 Mib/sec (2,7 Gbit/s)	255 Mib/sec (2,1 Gbit/s)
	SMBv3 - 8 fils	190 Mib/sec (1,6 Gbit/s)	590 Mio/s (4,9 Gbit/s)	335 Mio/s (2,8 Gbit/s)
UC : 16 vCPU RAM : 32 GO				
Protocole NFS recommandé pour Linux				
Appliance matérielle Storage Gateway	NFSv3 - 1 filetage	265 Mio/s (2,2 Gbit/s)	590 Mio/s (4,9 Gbit/s)	310 Mib/sec (2,6 Gbit/s)
	NFSv3 - 8 fils	385 Mib/sec (3,1 Gbit/s)	590 Mio/s (4,9 Gbit/s)	335 Mio/s (2,8 Gbit/s)
	NFSv4 - 1 filetage	310 Mib/sec (2,6 Gbit/s)	590 Mio/s (4,9 Gbit/s)	295 Mio/s (2,5 Gbit/s)
	NFSv4 - 8 fils	385 Mib/sec (3,1 Gbit/s)	590 Mio/s (4,9 Gbit/s)	335 Mio/s (2,8 Gbit/s)
Performances réseau minimales : 10 Gbit/s				

Exemples de configuration	Protocole	Débit d'écriture (taille de fichier 1 Go)	Débit de lecture d'accès au cache	Débit de lecture manquant du cache
	SMBV3 - 1 filetage	275 Mib/sec (2,4 Gbit/s)	325 Mib/sec (2,7 Gbit/s)	255 Mib/sec (2,1 Gbit/s)
	SMBV3 - 8 fils	455 Mio/s (3,8 Gbit/s)	590 Mio/s (4,9 Gbit/s)	335 Mio/s (2,8 Gbit/s)
Disque racine : SSD io1 80 Go, 4 000 E/S par seconde	NFSv3 - 1 filetage	300 Mio/s (2,5 Gbit/s)	590 Mio/s (4,9 Gbit/s)	325 Mib/sec (2,7 Gbit/s)
	NFSv3 - 8 fils	585 Mio/s (4,9 Gbit/s)	590 Mio/s (4,9 Gbit/s)	580 Mio/s (4,8 Gbit/s)
Disque de cache : 4 disques de cache NVME de 2 To	NFSv4 - 1 filetage	355 Mio/s (3,0 Gbit/s)	590 Mio/s (4,9 Gbit/s)	340 Mio/s (2,9 Gbit/s)
	NFSv4 - 8 fils	575 Mio/s (4,8 Gbit/s)	590 Mio/s (4,9 Gbit/s)	575 Mio/s (4,8 Gbit/s)
Performances réseau minimales : 10 Gbit/s	SMBV3 - 1 filetage	230 Mio/s (1,9 Gbit/s)	325 Mib/sec (2,7 Gbit/s)	245 Mio/s (2,0 Gbit/s)
	SMBV3 - 8 fils	585 Mio/s (4,9 Gbit/s)	590 Mio/s (4,9 Gbit/s)	580 Mio/s (4,8 Gbit/s)
UC : 32 vCPU RAM : 244 GO				
Protocole NFS recommandé pour Linux				

Performances de passerelle de fichiers sur les clients

Exemples de configuration	Protocole	Débit d'écriture (taille de fichier 1 Go)	Débit de lecture d'accès au cache	Débit de lecture manquant du cache
Disque racine : 80 Go io1, 4 000 E/S par seconde	SMBV3 - 1 filetage	150 Mio/s (1,3 Gbit/s)	180 Mio/s (1,5 Gbit/s)	20 Mio/s (0,2 Gbit/s)
	SMBV3 - 8 fils	190 Mib/sec (1,6 Gbit/s)	335 Mio/s (2,8 Gbit/s)	195 Mib/sec (1,6 Gbit/s)
Disque de cache : 512 GiB, io1, 1 500 E/S par seconde	NFSv3 - 1 filetage	95 Mio/s (0,8 Gbit/s)	130 Mib/sec (1,1 Gbit/s)	20 Mio/s (0,2 Gbit/s)
	NFSv3 - 8 fils	190 Mib/sec (1,6 Gbit/s)	330 Mio/s (2,8 Gbit/s)	190 Mib/sec (1,6 Gbit/s)
Performances réseau minimales : 10 Gbit/s				
UC : 16 vCPU RAM : 32 GO				
Protocole SMB recommandé pour Windows				
Appliance matérielle Storage Gateway	SMBV3 - 1 filetage	230 Mio/s (1,9 Gbit/s)	255 Mib/sec (2,1 Gbit/s)	20 Mio/s (0,2 Gbit/s)
	SMBV3 - 8 fils	835 Mio/s (7,0 Gbit/s)	475 Mio/s (4,0 Gbit/s)	195 Mib/sec (1,6 Gbit/s)
	NFSv3 - 1 filetage	135 Mib/sec (1,1 Gbit/s)	185 Mib/sec (1,6 Gbit/s)	20 Mio/s (0,2 Gbit/s)
	NFSv3 - 8 fils	545 Mib/sec (4,6 Gbit/s)	470 Mio/s (4,0 Gbit/s)	190 Mib/sec (1,6 Gbit/s)
Performances réseau minimales : 10 Gbit/s				

Exemples de configuration	Protocole	Débit d'écriture (taille de fichier 1 Go)	Débit de lecture d'accès au cache	Débit de lecture manquant du cache
Disque racine : SSD io1 80 Go, 4 000 E/S par seconde	SMBV3 - 1 filetage	230 Mio/s (1,9 Gbit/s)	265 Mio/s (2,2 Gbit/s)	30 Mio/s (0,3 Gbit/s)
	SMBV3 - 8 fils	835 Mio/s (7,0 Gbit/s)	780 Mio/s (6,5 Gbit/s)	250 Mib/sec (2,1 Gbit/s)
Disque de cache : 4 disques de cache NVME de 2 To	NFSv3 - 1 filetage	135 Mib/sec (1,1 Gb/s)	220 Mio/s (1,8 Gbit/s)	30 Mio/s (0,3 Gbit/s)
	NFSv3 - 8 fils	545 Mib/sec (4,6 Gbit/s)	570 Mio/s (4,8 Gbit/s)	240 Mio/s (2,0 Gbit/s)
Performances réseau minimales : 10 Gbit/s				
UC : 32 vCPU RAM : 244 GO				
Protocole SMB recommandé pour Windows				

 Note

Vos performances peuvent varier en fonction de la configuration de votre plateforme hôte et de la bande passante réseau.

Optimisation des performances de la passerelle

Vous trouverez ci-après des informations sur l'optimisation des performances de votre passerelle. Le conseil repose sur l'ajout de ressources à votre passerelle et l'ajout de ressources à votre serveur d'application.

Ajouter des ressources à la passerelle

Vous pouvez optimiser les performances de la passerelle en ajoutant des ressources à votre passerelle à l'aide de plusieurs façons.

Utiliser des disques hautes performances

Afin d'optimiser les performances de la passerelle, vous pouvez ajouter des disques hautes performances tels que les disques SSD et un contrôleur NVMe. Vous pouvez également attacher des disques virtuels directement à l'ordinateur virtuel à partir d'un réseau SAN au lieu d'avoir recours au système NTFS Microsoft Hyper-V. Les performances améliorées des disques entraînent généralement un débit plus élevé et un nombre plus élevé d'opérations d'entrée/sortie par seconde (IOPS). Pour en savoir plus sur l'ajout de disques, consultez [Ajouter du stockage de cache](#).

Pour mesurer le débit, utilisez les `ReadBytes` et `WriteBytes` métriques avec les `SampleStatistics` Amazon CloudWatch. Par exemple, la statistique `Sample` de la métrique `ReadBytes` pendant 5 minutes divisée par 300 secondes vous donne les IOPS. En règle générale, lorsque vous examinez ces métriques pour une passerelle, recherchez un débit faible et de faibles tendances IOPS pour indiquer les goulots d'étranglement liés aux disques.

Note

Les métriques CloudWatch ne sont pas disponibles pour toutes les passerelles. Pour plus d'informations sur les métriques de passerelle, consultez [Surveillance de la passerelle de fichiers](#).

Ajouter des ressources de processeur à votre hôte de passerelle

Un serveur hôte de passerelle doit avoir au moins quatre processeurs virtuels. Afin d'optimiser les performances de la passerelle, vérifiez que les quatre processeurs virtuels attribués à la machine virtuelle de la passerelle sont soutenus par quatre cœurs. En outre, vérifiez que vous ne surallegez pas les UC du serveur hôte.

Lorsque vous ajoutez des UC supplémentaires à votre serveur hôte de passerelle, vous augmentez la capacité de traitement de la passerelle. Cela permet à la passerelle de gérer, en parallèle, le stockage des données de votre application vers votre stockage local et le chargement de ces données vers Amazon S3. Les processeurs supplémentaires permettent également de

veiller à ce que votre passerelle obtienne suffisamment de ressources de processeur lorsque l'hôte est partagé avec d'autres ordinateurs virtuels. La présence d'une quantité suffisante de ressources de processeur permet généralement d'améliorer le débit.

Storage Gateway prend en charge l'utilisation de 24 processeurs sur votre serveur hôte de passerelle. Vous pouvez utiliser 24 processeurs pour améliorer nettement les performances de votre passerelle. Nous vous recommandons la configuration de passerelle suivante pour votre serveur hôte de passerelle :

- 24 UC.
- 16 GiB de mémoire RAM réservée pour les passerelles de fichiers
 - 16 GiB de RAM réservée pour les passerelles avec une taille de cache allant jusqu'à 16 TiB
 - 32 GiB de RAM réservée pour les passerelles avec une taille de cache de 16 à 32 TiB
 - 48 GiB de RAM réservée pour les passerelles avec une taille de cache de 32 à 64 TiB
- Disque 1 attaché au contrôleur paravirtuel 1, à utiliser comme cache de passerelle de la façon suivante :
 - SSD utilisant un contrôleur NVMe.
- Disque 1 attaché au contrôleur paravirtuel 2, à utiliser comme tampon de chargement de la passerelle de la façon suivante :
 - SSD utilisant un contrôleur NVMe.
- Disque 3 attaché au contrôleur paravirtuel 2, à utiliser comme tampon de chargement de la passerelle de la façon suivante :
 - SSD utilisant un contrôleur NVMe.
- Carte réseau 1 configurée sur le réseau d'ordinateur virtuel 1 :
 - Utilisez le réseau d'ordinateur virtuel 1 et ajoutez une carte VMXnet3 (10 Gbit/s) à utiliser pour l'intégration.
- Carte réseau 2 configurée sur le réseau d'ordinateur virtuel 2 :
 - Utilisez le réseau d'ordinateur virtuel 2 et ajoutez une carte VMXnet3 (10 Gbit/s) à utiliser pour la connexion à AWS.

Soutenir les disques virtuels de la passerelle avec des disques physiques distincts

Lorsque vous mettez en service les disques d'une passerelle, nous vous recommandons vivement de ne pas mettre en service des disques locaux pour le stockage local qui utilisent le même disque de stockage physique sous-jacente (c'est-à-dire, le même disque). Par exemple, pour VMware ESXi, les ressources de stockage physique sous-jacentes sont représentées comme une

banque de données. Lorsque vous déployez l'ordinateur virtuel de la passerelle, vous choisissez une banque de données sur laquelle stocker les fichiers de l'ordinateur virtuel. Lorsque vous mettez en service un disque virtuel (par exemple, en tant que tampon de chargement), vous pouvez stocker le disque virtuel dans la même banque de données en tant qu'ordinateur virtuel ou dans une banque de données différente.

Si vous avez plusieurs banques de données, nous vous recommandons vivement de choisir une banque de données pour chaque type de stockage local que vous créez. Un magasin de données soutenu par un seul disque physique sous-jacent peut entraîner des performances médiocres. Par exemple, lorsque vous utilisez un nouveau disque pour soutenir à la fois le stockage de cache et le tampon de chargement dans une configuration de passerelle. De la même façon, un magasin de données soutenu par une configuration RAID moins performante, comme RAID 1, peut entraîner des performances médiocres.

Ajouter des ressources à votre environnement d'application

Augmenter la bande passante entre le serveur d'application et la passerelle

Afin d'optimiser les performances de la passerelle, vérifiez que la bande passante réseau entre votre application et la passerelle peut supporter les besoins de votre application. Vous pouvez utiliser le plugin `ReadBytesetWriteBytes` mesures de la passerelle pour mesurer le débit total des données.

Pour votre application, comparez le débit mesuré avec le débit souhaité. Si le débit mesuré est inférieur au débit souhaité, l'augmentation de la bande passante entre votre application et la passerelle peut améliorer les performances si le réseau est le goulot d'étranglement. De même, vous pouvez augmenter la bande passante entre l'ordinateur virtuel et les disques locaux, s'ils ne sont pas attachés directement.

Ajouter des ressources de processeur à votre environnement d'application

Si votre application a besoin de ressources de processeur supplémentaires, l'ajout d'autres processeurs peut aider votre application à faire évoluer sa charge d'E/S.

Utilisation de VMware vSphere High Availability avec Storage Gateway

Storage Gateway offre une haute disponibilité sur VMware grâce à un ensemble de contrôles d'état au niveau de l'application, intégrés à VMware vSphere High Availability (VMware HA). Cette approche permet de protéger les charges de travail de stockage contre les défaillances de matériel, d'hyperviseur ou de réseau. Elle permet également de se protéger contre les erreurs logicielles, telles que les délais d'expiration de connexion et l'indisponibilité des volumes ou partages de fichiers.

Grâce à cette intégration, une passerelle déployée dans un environnement VMware sur site ou dans VMware Cloud sur AWS est automatiquement récupérée après la plupart des interruptions de service. Cette récupération s'effectue généralement en moins de 60 secondes, sans perte de données.

Pour utiliser VMware HA avec Storage Gateway, procédez comme suit.

Rubriques

- [Configurer votre cluster vSphere VMware HA](#)
- [Télécharger l'image .ova pour votre type de passerelle](#)
- [Déployer la passerelle](#)
- [\(Facultatif\) Ajouter des options de remplacement pour d'autres machines virtuelles de votre cluster](#)
- [Activer votre passerelle](#)
- [Tester votre configuration de VMware High Availability](#)

Configurer votre cluster vSphere VMware HA

Tout d'abord, si vous n'avez pas encore créé de cluster VMware, créez-en un. Pour plus d'informations sur la création d'un cluster VMware, consultez [Create a vSphere HA Cluster \(Créer un cluster vSphere HA\)](#) dans la documentation VMware.

Ensuite, configurez votre cluster VMware pour qu'il fonctionne avec Storage Gateway.

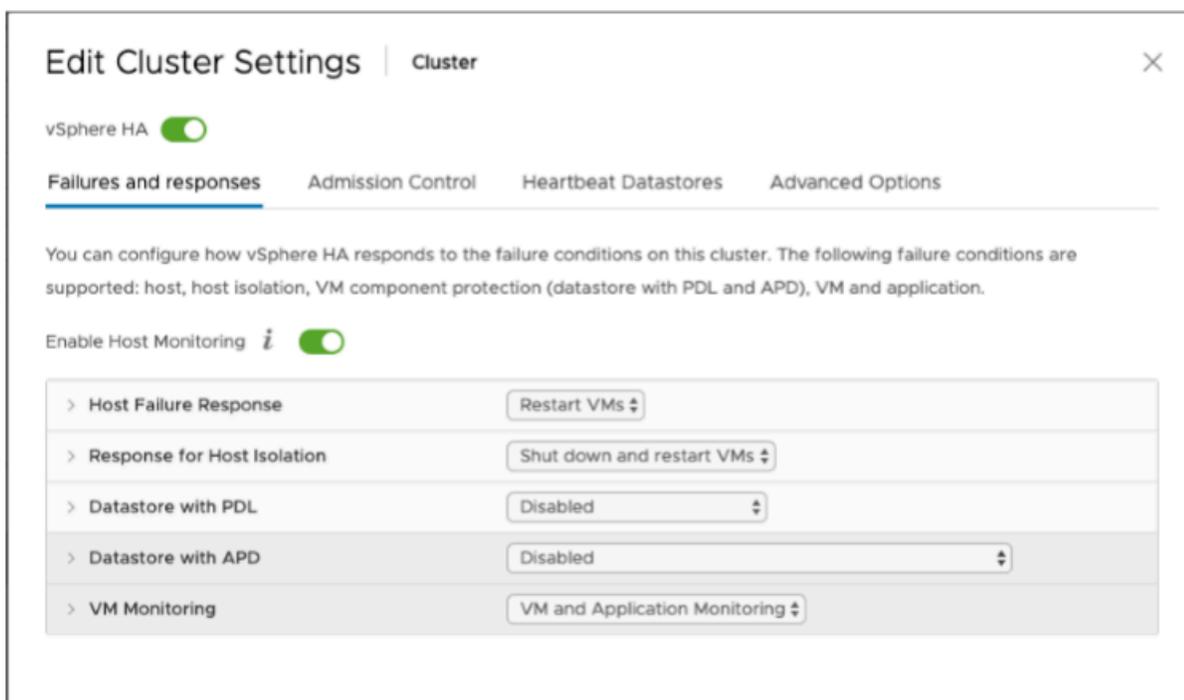
Pour configurer votre cluster VMware

1. Sur la page Edit Cluster Settings (Modifier les paramètres du cluster) dans VMware vSphere, assurez-vous que la surveillance des machines virtuelles est configurée pour la surveillance des

machines virtuelles et des applications. Pour ce faire, définissez les options suivantes comme indiqué :

- Host Failure Réponse : Redémarrer les machines virtuelles
- Réponse à l'isolement de l'hôte : Arrêter et redémarrer les machines virtuelles
- Datastore with PDL : Désactivé
- Datastore with APD : Désactivé
- VM Monitoring : Surveillance des machines virtuelles et des applications

Pour obtenir un exemple, consultez la capture d'écran suivante.



2. Affinez la sensibilité du cluster en ajustant les valeurs suivantes :

- Intervalle d'échec— Après cet intervalle, la VM est redémarrée si aucune pulsation de machine virtuelle n'est reçue.
- Temps de disponibilité minimum— Le cluster attend ce temps après le démarrage d'une machine virtuelle pour commencer à surveiller les pulsations des outils de machine virtuelle.
- Nombre maximum de réinitialisations par machine virtuelle: le cluster redémarre la machine virtuelle ce nombre de fois au maximum dans la fenêtre de temps des réinitialisations maximales.

- Fenêtre horaire maximum de réinitialisations— Fenêtre temporelle pendant laquelle compter le maximum de réinitialisations par machine virtuelle.

Si vous n'êtes pas sûr des valeurs à définir, utilisez les exemples de paramètres suivants :

- Failure interval (Intervalle d'échec) : **30** secondes
- Minimum uptime (Temps de disponibilité minimum) : **120** secondes
- Maximum per-VM resets (Nombre maximum de réinitialisations par machine virtuelle) : **3**
- Maximum resets time window (Fenêtre temporelle pour le maximum de réinitialisations) : **1** heure

Si vous avez d'autres machines virtuelles en cours d'exécution sur le cluster, vous pouvez définir ces valeurs spécifiquement pour votre machine virtuelle. Vous ne pouvez pas le faire tant que vous n'avez pas déployé la machine virtuelle à partir de .ova. Pour plus d'informations sur la définition de ces valeurs, consultez [\(Facultatif\) Ajouter des options de remplacement pour d'autres machines virtuelles de votre cluster](#).

Télécharger l'image .ova pour votre type de passerelle

Procédez comme suit pour télécharger l'image .ova.

Pour télécharger l'image .ova pour votre type de passerelle

- Téléchargez l'image .ova pour votre type de passerelle à partir de l'une des options suivantes :
 - Passerelle de fichiers —

Déployer la passerelle

Dans votre cluster configuré, déployez l'image .ova sur l'un des hôtes du cluster.

Pour déployer l'image .ova de la passerelle

1. Déployez l'image .ova sur l'un des hôtes du cluster.
2. Assurez-vous que les magasins de données que vous choisissez pour le disque racine et le cache sont disponibles pour tous les hôtes du cluster.

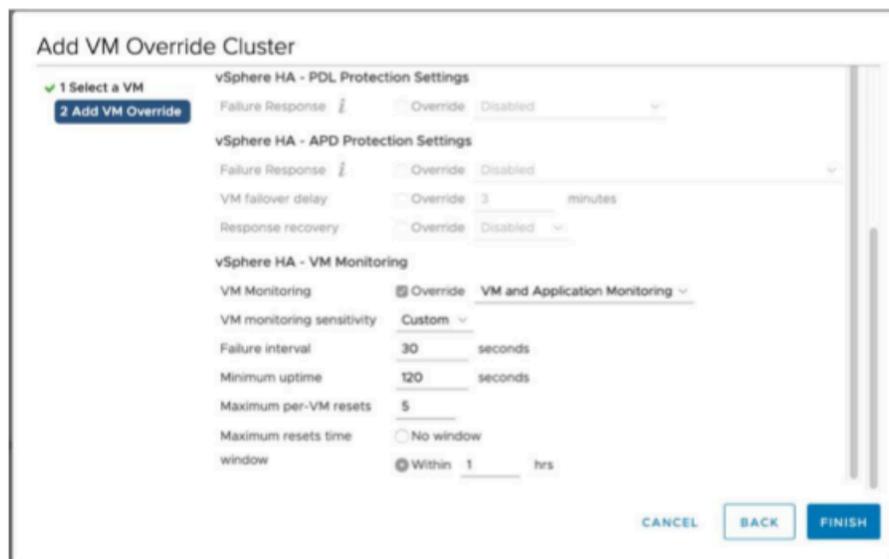
(Facultatif) Ajouter des options de remplacement pour d'autres machines virtuelles de votre cluster

Si vous avez d'autres machines virtuelles en cours d'exécution sur le cluster, vous pouvez définir les valeurs de cluster spécifiquement pour chaque machine virtuelle.

Pour ajouter des options de remplacement pour d'autres machines virtuelles de votre cluster

1. Sur la page Summary (Récapitulatif) de VMware vSphere, choisissez votre cluster pour ouvrir la page de cluster, puis choisissez Configure (Configurer).
2. Choisissez l'onglet Configuration puis choisissez VM Overrides (Remplacements de machines virtuelles).
3. Ajoutez une nouvelle option de remplacement de machine virtuelle pour modifier chaque valeur.

Pour les options de remplacement, consultez la capture d'écran suivante.



Activer votre passerelle

Une fois le .ova de votre passerelle déployé, activez votre passerelle. Les instructions sur la façon de procéder sont différentes pour chaque type de passerelle.

Pour activer la passerelle

- Choisissez des instructions d'activation en fonction de votre type de passerelle :

- Passerelle de fichiers —

Tester votre configuration de VMware High Availability

Après avoir activé votre passerelle, testez votre configuration.

Pour tester votre configuration de VMware HA

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le volet de navigation, choisissez Gateways (Passerelles), puis choisissez la passerelle que vous souhaitez tester pour VMware HA.
3. Dans Actions, choisissez Verify VMware HA (Vérifier VMware HA).
4. Dans la zone Verify VMware High Availability Configuration (Vérifier la configuration de VMware High Availability) qui s'affiche, choisissez OK.

Note

Le test de votre configuration de VMware HA redémarre votre machine virtuelle de passerelle et interrompt la connectivité à votre passerelle. Le test peut prendre quelques minutes.

Si le test réussit, l'état Verified (Vérifié) apparaît dans l'onglet Détails de la passerelle sur la console.

5. Choisissez Exit (Quitter).

Vous trouverez des informations sur les événements VMware HA dans les groupes de journaux Amazon CloudWatch. Pour de plus amples informations, veuillez consulter [Obtention des journaux d'intégrité de la passerelle de fichiers avec les groupes de journaux CloudWatch](#).

Sécurité dansAWSStorage Gateway

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous. Le [modèle de responsabilité partagée](#) décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des [AWS programmes de conformité](#). Pour de plus amples informations sur les programmes de conformité qui s'appliquent àAWSStorage Gateway, consultez[AWS Services concernés par le programme de conformité](#).
- Sécurité dans le cloud : votre responsabilité est déterminée par le service AWS que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utilisez Storage Gateway. Les rubriques suivantes vous montrent comment configurer Storage Gateway pour qu'elle réponde à vos objectifs de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autresAWSservices qui vous aident à surveiller et à sécuriser vos ressources Storage Gateway.

Rubriques

- [Protection des données dansAWSStorage Gateway](#)
- [authentification et contrôle d'accès pour Storage Gateway](#)
- [Journalisation et surveillance dans AWS Storage Gateway](#)
- [Validation de la conformité pourAWSStorage Gateway](#)
- [Résilience dansAWSStorage Gateway](#)
- [Sécurité de l'infrastructure dansAWSStorage Gateway](#)
- [Bonnes pratiques de sécurité pour Storage Gateway](#)

Protection des données dansAWSStorage Gateway

LeAWS [Modèle de responsabilité partagées](#)s'applique à la protection des données dansAWSStorage Gateway. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure globale sur laquelle l'ensemble du AWS Cloud s'exécute. La gestion du contrôle de votre contenu hébergé sur cette infrastructure est de votre responsabilité. Ce contenu comprend les tâches de configuration et de gestion de la sécurité des services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, veuillez consulter la [FAQ sur la confidentialité des données](#). Pour en savoir plus sur la protection des données en Europe, veuillez consulter le billet de blog [AWS Modèle de responsabilité partagée et RGPD](#) sur le AWSBlog de sécurité.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification Compte AWS et de configurer les comptes utilisateur individuels avec AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifacteur (MFA) avec chaque compte.
- Utilisez SSL/TLS pour communiquer avec les ressources AWS. Nous recommandons TLS 1.2 ou version ultérieure.
- Configurez une API et la journalisation des activités utilisateur avec AWS CloudTrail.
- Utilisez des solutions de chiffrement AWS, ainsi que tous les contrôles de sécurité par défaut au sein des services AWS.
- 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 disponibles, consultez [Norme de traitement de l'information fédérale \(Federal Information Processing Standard \(FIPS\)\) 140-2](#).

Nous vous recommandons vivement de ne jamais placer d'informations confidentielles ou sensibles, telles que des adresses e-mail, dans des balises ou des champs de format libre tels qu'un champ Nom. Cela s'applique aussi lorsque vous utilisez Storage Gateway ou d'autresAWSservices utilisant la console, l'API,AWS CLI, ouAWSKits SDK. Toutes les données que vous entrez dans des identifications ou des champs de format libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une URL à un serveur externe,

nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'URL pour valider votre demande au serveur.

Chiffrement des données avecAWS KMS

Storage Gateway utilise SSL/TLS (Secure Socket Layer/Transport Layer Security) pour chiffrer les données transférées entre votre appliance de passerelle etAWSstockage. Par défaut, Storage Gateway utilise des clés de chiffrement gérées par Amazon S3 (SSE-S3) pour chiffrer côté serveur toutes les données qu'elle stocke dans Amazon S3. Vous avez la possibilité d'utiliser l'API Storage Gateway pour configurer votre passerelle pour chiffrer les données stockées dans le cloud à l'aide du chiffrement côté serveur avecAWS Key Management Service(SSE-KMS) clés principales client (CMK).

Important

Lorsque vous utilisez unAWS KMSPour le chiffrement côté serveur, vous devez choisir une clé CMK symétrique. Storage Gateway ne prend pas en charge les clés CMK asymétriques. Pour en savoir plus, consultez [Utilisation des clés symétriques et asymétriques](#) dans le guide du développeur AWS Key Management Service.

Chiffrement d'un partage de fichiers

Pour un partage de fichiers, vous pouvez configurer votre passerelle pour chiffrer vos objets avecAWS KMS—clés gérées à l'aide de SSE-KMS. Pour plus d'informations sur l'utilisation de l'API Storage Gateway pour chiffrer les données écrites sur un partage de fichiers, consultez [CreateNFSFileShare](#) dans leAWS Storage GatewayAPI Reference.

Chiffrement d'un système de fichiers

Pour plus d'informations, consultez [Chiffrement des données dans Amazon FSx](#) dans leGuide de l'utilisateur Amazon FSx for Windows File Server.

Lorsque vous utilisez AWS KMS pour chiffrer vos données, gardez à l'esprit les points suivants :

- Vos données sont chiffrées lorsqu'elles sont au repos dans le cloud. En d'autres termes, elles sont chiffrées dans Amazon S3.
- Les utilisateurs IAM doivent disposer des autorisations requises pour appeler leAWS KMSOpérations d'API. Pour de plus amples informations, veuillez consulter [Utilisation des stratégies IAM avecAWS KMS](#) dans leAWS Key Management ServiceManuel du développeur.

- Si vous supprimez ou désactivez votre clé CMK ou que vous révoquez le jeton d'octroi, vous ne pouvez pas accéder aux données du volume ou de la bande. Pour de plus amples informations, veuillez consulter [Suppression des clés principales client](#) dans le [AWS Key Management Service Manuel du développeur](#).
- Si vous créez un instantané à partir d'un volume chiffré par KMS, l'instantané est chiffré. Si vous créez un instantané à partir d'un volume chiffré par KMS, l'instantané est chiffré.
- Si vous créez un nouveau volume à partir d'un instantané chiffré par KMS, le volume est chiffré. Vous pouvez spécifier une autre clé KMS pour le nouveau volume.

Note

Storage Gateway ne prend actuellement pas en charge la création d'un volume non chiffré à partir d'un point de récupération d'un volume chiffré par KMS ou d'un instantané chiffré par KMS.

Pour plus d'informations sur AWS KMS, consultez [Qu'est-ce que AWS Key Management Service ?](#)

authentification et contrôle d'accès pour Storage Gateway

L'accès à AWS Storage Gateway requiert des informations d'identification qu'AWS peut utiliser pour authentifier vos demandes. Ces informations d'identification doivent être autorisées à accéder à des ressources AWS, par exemple une passerelle, un partage de fichiers, un volume ou une bande. Les sections suivantes fournissent des détails sur la façon dont vous pouvez utiliser [AWS Identity and Access Management \(IAM\)](#) et Storage Gateway pour sécuriser vos ressources en contrôlant les personnes pouvant y accéder.

- [Authentification](#)
- [Contrôle d'accès](#)

Authentification

Vous pouvez utiliser les types d'identité suivants pour accéder à AWS :

- Utilisateur racine de Compte AWS-Lorsque vous créez dans un premier temps un Compte AWS, vous commencez avec une identité de connexion unique qui bénéficie d'un accès complet à

tous les services et ressources AWS du compte. Cette identité est appelée l'utilisateur racine du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide de l'adresse e-mail et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes, y compris pour les tâches administratives. Respectez plutôt la [bonne pratique qui consiste à avoir recours à l'utilisateur racine uniquement pour créer le premier utilisateur IAM](#). Ensuite, mettez en sécurité les informations d'identification de l'utilisateur racine et utilisez-les uniquement pour effectuer certaines tâches de gestion des comptes et des services.

- Utilisateur IAM— Un [Utilisateur IAM](#) est une identité au sein de votre Compte AWS qui dispose d'autorisations personnalisées spécifiques (par exemple, autorisation de créer une passerelle dans Storage Gateway). Vous pouvez utiliser un nom d'utilisateur et un mot de passe IAM pour vous connecter aux pages web AWS sécurisées telles que la [AWS Management Console](#), les [forums de discussion AWS](#) ou le [centre AWS Support](#).

En plus de générer un nom utilisateur et un mot de passe, vous pouvez générer des [clés d'accès](#) pour chaque utilisateur. Vous pouvez utiliser ces clés lorsque vous accédez aux services AWS par programmation, soit par le biais d'[un kit SDK](#) soit à l'aide d'[AWS Command Line Interface \(CLI\)](#). Les outils de la CLI et les kits SDK utilisent les clés d'accès pour signer de façon cryptographique votre demande. Si vous n'utilisez pas les outils AWS, vous devez signer la demande vous-même. Storage Gateway Signature Version 4, protocole permettant l'authentification des demandes d'API entrantes. Pour plus d'informations sur l'authentification des demandes, veuillez consulter [Processus de signature Signature Version 4](#) dans les Références générales AWS.

- Rôle IAM : un [rôle IAM](#) est une identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Un rôle IAM est similaire à un utilisateur IAM, car il s'agit d'une identité AWS avec des politiques d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être assumé par tout utilisateur qui en a besoin. En outre, un rôle ne dispose pas d'informations d'identification standard à long terme comme un mot de passe ou des clés d'accès associées. Au lieu de cela, lorsque vous adoptez un rôle, il vous fournit des informations d'identification de sécurité temporaires pour votre session de rôle. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès par des utilisateurs fédérés-Au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités existantes provenant d'AWS Directory Service, de votre répertoire d'utilisateurs d'entreprise ou d'un fournisseur d'identité web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un [fournisseur d'identité](#). Pour plus d'informations sur les utilisateurs fédérés, veuillez consulter [Utilisateurs fédérés et rôles](#) dans le Guide de l'utilisateur IAM.
- AWS Accès par un service -Un rôle de service est un [rôle IAM](#) qu'un service endosse pour effectuer des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, veuillez consulter [Création d'un rôle pour la délégation d'autorisations à un service AWS](#) dans le Guide de l'utilisateur IAM.
- Applications s'exécutant sur Amazon EC2-Vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant AWS CLI ou des requêtes AWS API. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour de plus amples informations, veuillez consulter [Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2](#) dans le Guide de l'utilisateur IAM.

Contrôle d'accès

Vous pouvez avoir des informations d'identification valides pour authentifier vos demandes, mais à moins d'avoir les autorisations requises, vous ne pouvez pas créer de ressources Storage Gateway ni y accéder. Par exemple, vous devez disposer des autorisations appropriées pour créer une passerelle dans Storage Gateway.

Les sections suivantes décrivent comment gérer les autorisations pour Storage Gateway. Nous vous recommandons de commencer par lire la présentation.

- [Présentation de la gestion des autorisations d'accès à votre Storage Gateway](#)

- [Politiques basées sur une identité \(politiques IAM\)](#)

Présentation de la gestion des autorisations d'accès à votre Storage Gateway

EVERYAWS appartient à un compte Amazon Web Services et les autorisations de créer des ressources et d'y accéder sont régies par des stratégies d'autorisation. Un administrateur de compte peut attacher des politiques d'autorisation aux identités IAM (c'est-à-dire aux utilisateurs, groupes et rôles), et certains services (tels que AWS Lambda) prennent également en charge l'attachement de politiques d'autorisation aux ressources.

Note

Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté des privilèges d'administrateur. Pour plus d'informations, consultez [Bonnes pratiques IAM](#) dans le Guide de l'utilisateur IAM.

Lorsque vous accordez des autorisations, vous décidez qui doit les obtenir, à quelles ressources ces autorisations s'appliquent et les actions spécifiques que vous souhaitez autoriser sur ces ressources.

Rubriques

- [Ressources et opérations Storage Gateway](#)
- [Présentation de la propriété des ressources](#)
- [Gestion de l'accès aux ressources](#)
- [Spécification des éléments de stratégie : Actions, effets, ressources et mandataires](#)
- [Spécification de conditions dans une politique](#)

Ressources et opérations Storage Gateway

Dans Storage Gateway, la principale ressource est un passerelle. Storage Gateway prend également en charge les types de ressources supplémentaires suivants : partage de fichiers, volume, bande virtuelle, cible iSCSI et appareil VTL. Ceux-ci sont appelés des sous-ressources, qui n'existent pas tant qu'elles n'ont pas été associées à une passerelle.

Ces ressources et sous-ressources ont des noms Amazon Resource Names (ARNs) uniques associés, comme cela est illustré dans le tableau suivant.

Type de ressource	Format ARN
ARN de passerelle	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
ARN de partage de fichiers	arn:aws:storagegateway: <i>region:account-id</i> :share/ <i>share-id</i>

Note

Les ID de ressource Storage Gateway sont en majuscules. Lorsque vous utilisez ces ID de ressource avec l'API Amazon EC2, Amazon EC2 attend des ID de ressource en minuscules. Vous devez modifier votre ID de ressource et utiliser des minuscules afin de pouvoir vous en servir avec l'API EC2. Par exemple, dans Storage Gateway, l'ID d'un volume peut être `vol-1122AABB`. Lorsque vous utilisez cet ID avec l'API EC2, vous devez le remplacer par `vol-1122aabb`. Sinon, l'API EC2 ne peut pas se comporter comme prévu.

Les ARN des passerelles activées avant le 2 septembre 2015, contiennent le nom de la passerelle au lieu de l'ID de la passerelle. Pour obtenir l'ARN votre passerelle, utilisez l'opération d'API `DescribeGatewayInformation`.

Pour accorder des autorisations pour des opérations spécifiques de l'API, par exemple la création d'une bande, Storage Gateway fournit un ensemble d'actions d'API vous permettant de créer et de gérer ces ressources et sous-ressources. Pour obtenir une liste d'actions d'API, consultez [Actions](#) dans le [AWS Storage Gateway API Reference](#).

Pour accorder des autorisations pour des opérations spécifiques d'API, par exemple la création d'une bande, Storage Gateway définit un ensemble d'actions que vous pouvez spécifier dans une stratégie d'autorisations afin d'accorder des autorisations pour certaines opérations d'API. Une opération d'API peut exiger des autorisations pour plusieurs actions. Pour visualiser un tableau répertoriant toutes les actions d'API Storage Gateway et les ressources auxquelles elles s'appliquent, consultez [Autorisations de Storage Gateway Référence des actions, ressources et conditions](#).

Présentation de la propriété des ressources

UNpropriétaire de ressourceest le compte Amazon Web Services qui a créé la ressource. En d'autres termes, le propriétaire de la ressource est le compte Amazon Web Services du.entité principale(le compte racine, un utilisateur IAM ou un rôle IAM) qui authentifie la demande créatrice de la ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification du compte racine de votre compte Amazon Web Services pour activer une passerelle, votre compte Amazon Web Services est le propriétaire de la ressource (dans Storage Gateway, la ressource est la passerelle).
- Si vous créez un utilisateur IAM dans votre compte Amazon Web Services et accordez des autorisations à `ActivateGateway` pour cet utilisateur, ce dernier peut activer une passerelle. Toutefois, votre compte Amazon Web Services, auquel l'utilisateur appartient, détient la ressource de passerelle.
- Si vous créez un rôle IAM dans votre compte Amazon Web Services avec des autorisations permettant l'activation d'une passerelle, toute personne capable d'exercer le rôle peut activer une passerelle. Votre compte Amazon Web Services, auquel le rôle appartient, détient la ressource de passerelle.

Gestion de l'accès aux ressources

Une politique d'autorisation décrit qui a accès à quoi. La section suivante explique les options disponibles pour créer des politiques d'autorisations.

Note

Cette section décrit l'utilisation d'IAM dans le contexte de Storage Gateway. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour accéder à la documentation complète d'IAM, consultez [En quoi consiste IAM](#) dans le IAM User Guide. Pour plus d'informations sur la syntaxe et les descriptions des stratégies IAM, consultez [Référence de stratégie AWS IAM](#) dans le Guide de l'utilisateur IAM.

Les stratégies attachées à une identité IAM sont appelées stratégies basées sur une entité (stratégies IAM) et les stratégies attachées à une ressource sont appelées stratégies basées sur une ressource. Storage Gateway prend en charge uniquement les stratégies basées sur une identité (stratégies IAM).

Rubriques

- [Politiques basées sur une identité \(politiques IAM\)](#)
- [politiques basées sur les ressources](#)

Politiques basées sur une identité (politiques IAM)

Vous pouvez attacher des politiques à des identités IAM. Par exemple, vous pouvez effectuer les opérations suivantes :

- Attacher une stratégie d'autorisation à un utilisateur ou à un groupe de votre compte: un administrateur de compte peut utiliser une stratégie d'autorisation associée à un utilisateur donné pour autoriser celui-ci à créer une ressource Storage Gateway, par exemple une passerelle, un volume ou une bande.
- Attacher une politique d'autorisations à un rôle (accorder des autorisations entre comptes)-Vous pouvez attacher une politique d'autorisation basée sur une identité à un rôle IAM afin d'accorder des autorisations entre comptes. Par exemple, l'administrateur dans le Compte A peut créer un rôle afin d'accorder des autorisations inter-comptes à un autre compte Amazon Web Services (par exemple, le Compte B) ou à unAWSservice comme suit :
 1. L'administrateur du Compte A crée un rôle IAM et attache une politique d'autorisation à ce rôle qui accorde des autorisations sur les ressources dans le Compte A.
 2. L'administrateur du Compte A attache une politique d'approbation au rôle identifiant le Compte B comme principal pouvant assumer ce rôle.
 3. L'administrateur du Compte B peut alors déléguer des autorisations pour assumer le rôle à tous les utilisateurs figurant dans le Compte B. Cela autorise les utilisateurs du Compte B à créer des ressources ou à y accéder dans le Compte A. Le principal dans la stratégie d'approbation peut également être un principal de service AWS si vous souhaitez accorder à un service AWS des autorisations pour assumer ce rôle.

Pour en savoir plus sur l'utilisation d'IAM pour déléguer des autorisations, consultez [Gestion des accès](#) dans le Guide de l'utilisateur IAM.

Voici un exemple de stratégie qui accorde les autorisations requises pour toutes les actions `List*` au niveau de toutes les ressources. Cette action est une action en lecture seule. Par conséquent, la stratégie ne permet pas à l'utilisateur de modifier l'état des ressources.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowAllListActionsOnAllResources",
    "Effect": "Allow",
    "Action": [
      "storagegateway:List*"
    ],
    "Resource": "*"
  }
]
```

Pour plus d'informations sur l'utilisation des stratégies basées sur une identité avec Storage Gateway, consultez [Utilisation des stratégies basées sur une identité \(stratégies IAM\) pour Storage Gateway](#).

Pour de plus amples informations sur les utilisateurs, les groupes, les rôles et les autorisations, veuillez consulter [Identités \(utilisateurs, groupes et rôles\)](#) dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

D'autres services, tels qu'Amazon S3, prennent également en charge les politiques d'autorisation basées sur une ressource. Par exemple, vous pouvez attacher une politique à un compartiment S3 pour gérer les autorisations d'accès à ce compartiment. Storage Gateway ne prend pas en charge les stratégies basées sur une ressource.

Spécification des éléments de stratégie : Actions, effets, ressources et mandataires

Pour chaque ressource Storage Gateway (voir [Autorisations de Storage Gateway Référence des actions, ressources et conditions](#)), le service définit un ensemble d'opérations d'API (voir [Actions](#)). Pour accorder des autorisations pour ces opérations d'API, Storage Gateway définit un ensemble d'actions que vous pouvez spécifier dans une stratégie. Par exemple, pour la ressource Storage Gateway, les actions suivantes sont définies : `ActivateGateway`, `DeleteGateway`, et `DescribeGatewayInformation`. Notez que l'exécution d'une opération d'API peut exiger des autorisations pour plusieurs actions.

Voici les éléments les plus élémentaires d'une politique :

- Ressource – dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour des ressources Storage Gateway, vous devez toujours utiliser le caractère générique. (*) dans les stratégies IAM. Pour plus d'informations, consultez [Ressources et opérations Storage Gateway](#).

- Action : vous utilisez des mots clés d'action pour identifier les opérations de ressource que vous voulez accorder ou refuser. Par exemple, en fonction de la valeur spécifiée `Effect`, le `storagegateway:ActivateGateway` accorde ou refuse à l'utilisateur les autorisations appropriées pour effectuer `Storage GatewayActivateGateway`.
- Effet – Vous spécifiez l'effet produit lorsque l'utilisateur demande l'action spécifique, qui peut être une autorisation ou un refus. Si vous n'accordez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez aussi explicitement refuser l'accès à une ressource, ce que vous pouvez faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une politique différente accorde l'accès.
- Principal – dans les stratégies basées sur une identité (stratégies IAM), l'utilisateur auquel la stratégie est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource). Storage Gateway ne prend pas en charge les stratégies basées sur une ressource.

Pour en savoir plus sur la syntaxe des stratégies IAM et pour obtenir des descriptions, consultez [Référence de stratégie IAM AWS](#) dans le Guide de l'utilisateur IAM.

Pour visualiser un tableau répertoriant toutes les actions d'API Storage Gateway, consultez [Autorisations de Storage Gateway Référence des actions, ressources et conditions](#).

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage de stratégie IAM pour spécifier les conditions définissant à quel moment une stratégie doit prendre effet lors de l'octroi des autorisations. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour de plus amples informations sur la spécification de conditions dans un langage de politique, veuillez consulter [Condition](#) dans le Guide de l'utilisateur IAM.

Pour exprimer des conditions, vous utilisez des clés de condition prédéfinies. Il n'existe pas de clés de condition spécifiques à Storage Gateway. Il existe, toutefois, des clés de condition à l'échelle d'AWS que vous pouvez utiliser selon vos besoins. Pour obtenir la liste complète des clés à l'échelle d'AWS, veuillez consulter [Clés disponibles](#) dans le Guide de l'utilisateur IAM.

Utilisation des stratégies basées sur une identité (stratégies IAM) pour Storage Gateway

Cette rubrique fournit des exemples de politiques basées sur une identité dans lesquelles un administrateur de compte peut attacher des politiques d'autorisation aux identités IAM (c'est-à-dire aux utilisateurs, groupes et rôles).

Important

Nous vous recommandons tout d'abord d'examiner les rubriques de présentation qui détaillent les concepts de base et les options disponibles pour gérer l'accès à vos ressources Storage Gateway. Pour plus d'informations, consultez [Présentation de la gestion des autorisations d'accès à votre Storage Gateway](#).

Les sections de cette rubrique couvrent les sujets suivants :

- [Autorisations requises pour utiliser la console Storage Gateway](#)
- [AWSstratégies gérées pour Storage Gateway](#)
- [Exemples de stratégies gérées par le client](#)

Un exemple de politique d'autorisation est exposé ci-dessous.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsSpecifiedActionsOnAllGateways",
      "Effect": "Allow",
      "Action": [
        "storagegateway:ActivateGateway",
        "storagegateway:ListGateways"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
    ],
    "Resource": "*"
}
]
```

La stratégie a deux instructions (notez les éléments Action et Resource dans les deux instructions) :

- La première instruction accorde des autorisations pour deux actions Storage Gateway (`storagegateway:ActivateGateway` et `storagegateway:ListGateways`) sur une ressource de passerelle.

Le caractère générique (*) signifie que cette instruction peut correspondre à toutes les ressources. Dans ce cas, l'énoncé autorise l'`storagegateway:ActivateGateway` et `storagegateway:ListGateways` actions sur n'importe quelle passerelle. Le caractère générique est utilisé ici, car vous ne connaissez pas l'ID de ressource tant que vous n'avez pas créé la passerelle. Pour plus d'informations sur l'utilisation d'un caractère générique (*) dans une stratégie, consultez [Exemple 2 : Autoriser l'accès en lecture seule à une passerelle](#).

Note

Les ARN identifient de façon unique AWS. Pour de plus amples informations, veuillez consulter [Amazon Resource Name \(ARN\) et espaces de noms du service AWS](#) dans la Référence générale AWS.

Pour limiter les autorisations relatives à une action particulière sur une passerelle spécifique uniquement, créez une instruction distincte pour cette action dans la stratégie et spécifiez l'ID de passerelle dans cette instruction.

- La deuxième instruction accorde des autorisations pour les actions `ec2:DescribeSnapshots` et `ec2:DeleteSnapshot`. Ces actions Amazon Elastic Compute Cloud (Amazon EC2) requièrent des autorisations dans la mesure où les instantanés générés à partir de Storage Gateway sont stockés dans Amazon Elastic Block Store (Amazon EBS) et gérés en tant que ressources Amazon

EC2. Pour de plus amples informations, veuillez consulter [Actions](#) dans le [Référence d'API Amazon EC2](#). Étant donné que ces actions Amazon EC2 ne prennent pas en charge les autorisations au niveau des ressources, la stratégie spécifie le caractère générique (*) en tant que `Resource` valeur au lieu de spécifier un ARN de passerelle.

Pour visualiser un tableau répertoriant toutes les actions d'API Storage Gateway et les ressources auxquelles elles s'appliquent, consultez [Autorisations de Storage Gateway Référence des actions, ressources et conditions](#).

Autorisations requises pour utiliser la console Storage Gateway

Pour utiliser la console Storage Gateway, vous devez accorder des autorisations en lecture seule. Si vous avez l'intention de décrire des instantanés, vous devez également accorder des autorisations pour des actions supplémentaires comme indiqué dans la stratégie d'autorisations suivante :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
    }
  ]
}
```

Cette autorisation supplémentaire est obligatoire dans la mesure où les instantanés Amazon EBS générés à partir de Storage Gateway sont gérés comme des ressources Amazon EC2.

Pour configurer les autorisations minimales requises pour parcourir la console Storage Gateway, consultez [Exemple 2 : Autoriser l'accès en lecture seule à une passerelle](#).

AWSstratégies gérées pour Storage Gateway

Amazon Web Services est approprié pour de nombreux cas d'utilisation courants et fournit des stratégies IAM autonomes qui sont créées et administrées par AWS. Les politiques gérées octroient les autorisations requises dans les cas d'utilisation courants et vous évitent d'avoir à

réfléchir aux autorisations qui sont requises. Pour plus d'informations surAWSstratégies gérées, consultez[AWSStratégies gérées par](#) dans leIAM User Guide.

Procédez comme suit :AWSLes stratégies gérées, que vous pouvez attacher aux utilisateurs dans votre compte, sont spécifiques à Storage Gateway :

- Accès en lecture seule AWS Storage Gateway— Attribue l'accès en lecture seule àAWS Storage GatewayAWS.
- Accès complet à AWS Storage Gateway— Accorde l'accès complet àAWS Storage GatewayAWS.

Note

Vous pouvez consulter ces politiques d'autorisations en vous connectant à la console IAM et en y recherchant des politiques spécifiques.

Vous pouvez également créer vos propres stratégies IAM personnalisées pour accorder des autorisations pour les actions d'API AWS Storage Gateway. Vous pouvez attacher ces stratégies personnalisées aux utilisateurs ou groupes IAM qui nécessitent ces autorisations.

Exemples de stratégies gérées par le client

Dans cette section, vous trouverez des exemples de stratégies utilisateur qui accordent des autorisations pour diverses actions Storage Gateway. Ces stratégies fonctionnent lorsque vous utilisezAWSKits SDK et leAWS CLI. Lorsque vous utilisez la console, vous devez accorder des autorisations supplémentaires spécifiques à la console, ce qui est détaillé dans [Autorisations requises pour utiliser la console Storage Gateway](#).

Note

Tous les exemples utilisent la région USA Ouest (Oregon) (us-west-2) et contiennent des ID de compte fictifs.

Rubriques

- [Exemple 1 : Autoriser toutes les actions Storage Gateway sur toutes les passerelles](#)

- [Exemple 2 : Autoriser l'accès en lecture seule à une passerelle](#)
- [Exemple 3 : Autoriser l'accès à une passerelle spécifique](#)
- [Exemple 4 : Autoriser un utilisateur à accéder à un volume spécifique](#)
- [Exemple 5 : Autoriser toutes les actions sur les passerelles avec un préfixe spécifique](#)

Exemple 1 : Autoriser toutes les actions Storage Gateway sur toutes les passerelles

La stratégie suivante permet à un utilisateur d'effectuer toutes les actions Storage Gateway. La stratégie permet également à l'utilisateur d'effectuer des actions Amazon EC2 ([DescribeSnapshot](#) et [DeleteSnapshot](#)) sur les instantanés Amazon EBS générés à partir de Storage Gateway.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsAllAWSStorageGatewayActions",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AllowsSpecifiedEC2Actions",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

{You can use Windows ACLs only with file shares that are enabled for Active Directory.

Exemple 2 : Autoriser l'accès en lecture seule à une passerelle

La stratégie suivante permet toutes les actions `List*` et `Describe*` sur toutes les ressources. Veuillez noter que ces actions sont en lecture seule. Par conséquent, la stratégie ne permet pas

à l'utilisateur de modifier l'état des ressources, ce qui signifie que la stratégie ne permet pas à l'utilisateur d'effectuer des actions comme par exemple :DeleteGateway,ActivateGateway, etShutdownGateway.

La stratégie permet également l'action Amazon EC2 DescribeSnapshots. Pour de plus amples informations, veuillez consulter [DescribeSnapshots](#) dans le Référence d'API Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToAllGateways",
      "Action": [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Dans la stratégie précédente, au lieu d'utiliser un caractère générique (*), vous pouvez parcourir les ressources couvertes par la stratégie pour une passerelle spécifique, comme illustré dans l'exemple suivant. La stratégie permet ensuite les actions uniquement sur la passerelle spécifique.

```
"Resource": [
  "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
  "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
]
```

Au sein d'une passerelle, vous pouvez restreindre davantage la portée des ressources aux volumes de la passerelle, comme illustré dans l'exemple suivant :

```
"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/*"
```

Exemple 3 : Autoriser l'accès à une passerelle spécifique

La stratégie suivante autorise toutes les actions sur une passerelle spécifique. L'utilisateur n'a pas le droit d'accéder à d'autres passerelles que vous auriez pu déployer.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToAllGateways",
      "Action": [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AllowsAllActionsOnSpecificGateway",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
        "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
      ]
    }
  ]
}
```

La stratégie précédente fonctionne si l'utilisateur auquel la stratégie est attachée utilise l'API ou un AWSSDK pour accéder à la passerelle. Toutefois, si l'utilisateur va utiliser la console Storage Gateway, vous devez également accorder des autorisations pour autoriser la `ListGateways` comme illustré dans l'exemple suivant.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsAllActionsOnSpecificGateway",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
        "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
      ]
    },
    {
      "Sid": "AllowsUserToUseAWSConsole",
      "Action": [
        "storagegateway:ListGateways"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Exemple 4 : Autoriser un utilisateur à accéder à un volume spécifique

La stratégie suivante permet à un utilisateur d'effectuer toutes les actions sur un volume spécifique d'une passerelle. Dans la mesure où un utilisateur ne reçoit aucune autorisation par défaut, la stratégie permet à l'utilisateur d'accéder uniquement à un volume spécifique.

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

```

        "storagegateway:*"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
  },
  {
    "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
    "Action": [
      "storagegateway:ListGateways"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

La stratégie précédente fonctionne si l'utilisateur auquel la stratégie est attachée utilise l'API ou un AWS SDK pour accéder au volume. Toutefois, si cet utilisateur doit utiliser le AWS Storage Gateway, vous devez également accorder les autorisations nécessaires pour autoriser l'ListGateways comme illustré dans l'exemple suivant.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantsPermissionsToSpecificVolume",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-
id/volume/volume-id"
    },
    {
      "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
      "Action": [
        "storagegateway:ListGateways"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}

```

```
    ]
  }
}
```

Exemple 5 : Autoriser toutes les actions sur les passerelles avec un préfixe spécifique

La stratégie suivante permet à un utilisateur d'effectuer toutes les actions Storage Gateway sur des passerelles avec des noms qui commencent par :DeptX. La stratégie permet également le `DescribeSnapshotsAction` Amazon EC2, qui est obligatoire si vous avez l'intention de décrire les instantanés.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsActionsGatewayWithPrefixDeptX",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
    },
    {
      "Sid": "GrantsPermissionsToSpecifiedAction",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

La stratégie précédente fonctionne si l'utilisateur auquel la stratégie est attachée utilise l'API ou un AWS SDK pour accéder à la passerelle. Toutefois, si cet utilisateur envisage d'utiliser le AWS Storage Gateway, vous devez accorder des autorisations supplémentaires comme décrit dans [Exemple 3 : Autoriser l'accès à une passerelle spécifique](#).

Utilisation de balises pour contrôler l'accès à votre passerelle et à vos ressources

Pour contrôler l'accès aux ressources et actions de passerelle, vous pouvez utiliser des stratégies AWS Identity and Access Management (IAM) basées sur des balises. Vous pouvez fournir le contrôle de deux manières :

1. Contrôlez l'accès aux ressources de la passerelle en fonction des balises de ces ressources.
2. Contrôlez quelles balises peuvent être transmises dans une condition de demande IAM.

Pour plus d'informations sur l'utilisation des balises pour contrôler l'accès, consultez [Contrôle de l'accès à l'aide des balises](#).

Contrôle de l'accès en fonction des balises sur une ressource

Pour contrôler les actions qu'un utilisateur ou un rôle peut effectuer sur la ressource, vous pouvez utiliser des balises sur une ressource de passerelle. Par exemple, vous pouvez autoriser ou refuser des opérations d'API spécifiques sur une ressource de passerelle de fichiers en fonction de la paire clé-valeur de la balise sur la ressource.

L'exemple suivant permet à un utilisateur ou à un rôle d'effectuer les actions `ListTagsForResource`, `ListFileShares` et `DescribeNFSFileShares` sur toutes les ressources. La stratégie s'applique uniquement si la balise sur la ressource a sa clé définie sur `allowListAndDescribe` et la valeur définie sur `yes`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:ListTagsForResource",
        "storagegateway:ListFileShares",
        "storagegateway:DescribeNFSFileShares"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/allowListAndDescribe": "yes"
        }
      }
    }
  ]
}
```

```

        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "storagegateway:*"
        ],
        "Resource": "arn:aws:storagegateway:region:account-id:*/*"
    }
]
}

```

Contrôle de l'accès en fonction des balises dans une demande IAM

Pour contrôler ce qu'un utilisateur IAM peut faire sur une ressource de passerelle, vous pouvez utiliser des conditions dans une stratégie IAM basée sur des balises. Par exemple, vous pouvez écrire une stratégie qui autorise ou refuse à un utilisateur IAM la possibilité d'effectuer des opérations d'API spécifiques en fonction de la balise qu'il a fournie lorsqu'il a créé la ressource.

Dans l'exemple suivant, la première déclaration permet à un utilisateur de créer une passerelle uniquement si la paire clé-valeur de la balise qu'il a fournie lors de la création de la passerelle est **Department** et **Finance**. Lorsque vous utilisez l'opération d'API, vous ajoutez cette balise à la demande d'activation.

La deuxième instruction permet à l'utilisateur de créer un partage de fichiers Network File System (NFS) ou SMB (Server Message Block) sur une passerelle uniquement si la paire clé-valeur de la balise sur la passerelle correspond à **:DepartmentetFinance**. De plus, l'utilisateur doit ajouter une balise au partage de fichiers et la paire clé-valeur de la balise doit être **Department** et **Finance**. Vous pouvez ajouter des balises à un partage de fichiers lors de la création du partage de fichiers. Il n'existe pas d'autorisations pour les opérations `RemoveTagsFromResource` ou `AddTagsToResource`, ce qui signifie que l'utilisateur ne peut pas effectuer ces opérations sur la passerelle ou le partage de fichiers.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:ActivateGateway"
      ],

```

```
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/Department": "Finance"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "storagegateway:CreateNFSFileShare",
      "storagegateway:CreateSMBFileShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Department": "Finance",
        "aws:RequestTag/Department": "Finance"
      }
    }
  }
]
```

Utilisation des listes ACL Microsoft Windows pour contrôler l'accès à un partage de fichiers SMB

Amazon S3 File Gateway prend en charge deux méthodes différentes pour contrôler l'accès aux fichiers et répertoires stockés via un partage de fichiers SMB : Autorisations POSIX ou ACL Windows.

Dans cette section, vous trouverez des informations sur la façon d'utiliser les listes ACL Microsoft Windows sur les partages de fichiers SMB activés avec Microsoft Active Directory (AD). En utilisant les ACL Windows, vous pouvez définir des autorisations précises sur les fichiers et les dossiers dans votre partage de fichiers SMB.

Voici quelques caractéristiques importantes des listes de contrôle d'accès (ACL) Windows sur les partages de fichiers SMB :

- Les listes ACL Windows sont sélectionnées par défaut pour les partages de fichiers SMB lorsque votre passerelle de fichiers est jointe à un domaine Active Directory.

- Lorsque les listes ACL sont activées, les informations sur les ACL sont conservées dans les métadonnées d'objet Amazon S3.
- La passerelle conserve jusqu'à 10 listes ACL par fichier ou dossier.
- Lorsque vous utilisez un partage de fichiers SMB activé avec les listes de contrôle d'accès (ACL) pour accéder aux objets S3 créés en dehors de votre passerelle, les objets héritent les informations ACL du dossier parent.
- L'ACL racine par défaut d'un partage de fichiers SMB accorde un accès complet à tout le monde, mais vous pouvez modifier les autorisations de la racine ACL. Vous pouvez utiliser les listes ACL racines pour contrôler l'accès au partage de fichiers. Vous pouvez définir les personnes qui peuvent monter le partage de fichiers (mapper le lecteur) et les autorisations accordées de façon récursive à l'utilisateur sur les fichiers et les dossiers du partage de fichiers. Cependant, nous vous recommandons de définir cette autorisation sur le dossier de niveau supérieur dans le compartiment S3 afin que votre liste ACL soit conservée.

Vous pouvez activer les listes ACL Windows lorsque vous créez un nouveau partage de fichiers SMB à l'aide de l'opération d'API [CreateSMBFileShare](#). Ou vous pouvez activer les listes ACL Windows ACL sur un partage de fichiers SMB existant à l'aide de l'opération d'API [UpdateSMBFileShare](#).

Activation des listes ACL Windows ACL sur un nouveau partage de fichiers SMB

Suivez les étapes ci-après pour activer les listes ACL Windows sur un nouveau partage de fichiers SMB.

Pour activer les listes ACL Windows lors de la création d'un nouveau partage de fichiers SMB

1. Créez une passerelle de fichiers si vous n'en avez pas déjà une. Pour plus d'informations, consultez .
2. Si la passerelle n'est pas jointes à un domaine, ajoutez-la à un domaine. Pour plus d'informations, consultez .
3. Créez un partage de fichiers SMB.
4. Activez la liste ACL Windows sur le partage de fichiers à partir de la console Storage Gateway.

Pour utiliser la console Storage Gateway, procédez comme suit :

- a. Choisissez le partage de fichiers, puis Edit file share (Modifier le partage de fichiers).
- b. Pour l'option File/directory access controlled by (Accès au fichier/répertoire contrôlé par), choisissez Windows Access Control List (Liste de contrôle d'accès ACL).

5. (Facultatif) Ajoutez un utilisateur administrateur à la liste [AdminUsersList](#), si vous voulez que l'utilisateur administrateur ait des privilèges pour mettre à jour les listes ACL de tous les fichiers et dossiers du partage de fichiers.
6. Mettez à jour les listes ACL des dossiers parents sous le dossier racine. Pour ce faire, utilisez l'Explorateur de fichiers Windows afin de configurer les listes de contrôle d'accès (ACL) sur les dossiers du partage de fichiers SMB.

 Note

Si vous configurez les listes de contrôle d'accès (ACL) sur la racine plutôt que sur le dossier parent sous la racine, les autorisations ACL ne sont pas conservées dans Amazon S3.

Nous vous recommandons de définir les listes ACL au dossier de niveau supérieur sous la racine de votre partage de fichiers, au lieu de définir les listes de contrôle d'accès (ACL) directement à la racine du partage de fichiers. Cette approche conserve les informations sous la forme de métadonnées d'objet dans Amazon S3.

7. Activez l'héritage, le cas échéant.

 Note

Vous pouvez activer l'héritage pour les partages de fichiers créés après le 8 mai 2019.

Si vous activez l'héritage et mettez à jour les autorisations de manière récursive, Storage Gateway met à jour tous les objets du compartiment S3. Selon le nombre d'objets dans le compartiment, la mise à jour peut prendre un peu de temps.

Activation des listes ACL Windows ACL sur un partage de fichiers SMB existant

Suivez les étapes ci-après pour activer les ACL Windows sur un partage de fichiers SMB existant qui dispose des autorisations POSIX.

Pour activer les listes ACL Windows sur un partage de fichiers SMB existant à l'aide de la console Storage Gateway

1. Choisissez le partage de fichiers, puis Edit file share (Modifier le partage de fichiers).

2. Pour l'option File/directory access controlled by (Accès au fichier/répertoire contrôlé par), choisissez Windows Access Control List (Liste de contrôle d'accès ACL).
3. Activez l'héritage, le cas échéant.

Note

Nous vous déconseillons de définir les listes de contrôle d'accès (ACL) à la racine, parce que si vous procédez ainsi et supprimez votre passerelle, vous devez réinitialiser à nouveau les listes de contrôle d'accès (ACL).

Si vous activez l'héritage et mettez à jour les autorisations de manière récursive, Storage Gateway met à jour tous les objets du compartiment S3. Selon le nombre d'objets dans le compartiment, la mise à jour peut prendre un peu de temps.

Limites lors de l'utilisation des listes ACL Windows

Gardez les limites suivantes à l'esprit lorsque vous utilisez les listes ACL Windows pour contrôler l'accès aux partages de fichiers SMB :

- Les listes ACL Windows sont prises en charge uniquement sur les partages de fichiers qui sont activés pour Active Directory lorsque vous utilisez les clients Windows SMB pour accéder aux partages de fichiers.
- Les passerelles de fichiers prennent en charge un maximum de 10 entrées ACL pour chaque fichier et répertoire.
- Les passerelles de fichiers ne prennent pas en charge `Audit` et `Alarm`, qui sont des entrées de liste ACL système (SACL). Les passerelles de fichiers prennent en charge les entrées `Deny` et `Allow`, qui sont des entrées de listes ACL discrétionnaires (DAACL).
- Les paramètres des listes ACL racine des partages de fichiers SMB ne se trouvent que sur la passerelle, et les paramètres sont conservés à travers les mises à jour et les redémarrages de la passerelle.

Note

Si vous configurez les listes de contrôle d'accès (ACL) sur la racine plutôt que sur le dossier parent sous la racine, les autorisations ACL ne sont pas conservées dans Amazon S3.

En raison de ces conditions, veuillez à effectuer les opérations suivantes :

- Si vous configurez plusieurs passerelles pour accéder au même compartiment Amazon S3, configurez la racine ACL sur chacune des passerelles pour que les autorisations demeurent cohérentes.
- Si vous supprimez un partage de fichiers et le recréez sur le même compartiment Amazon S3, assurez-vous d'utiliser le même ensemble de listes ACL racine.

Autorisations de Storage Gateway Référence des actions, ressources et conditions

Lorsque vous configurez un [contrôle d'accès](#) et écrivez des politiques d'autorisations que vous pouvez attacher à une identité IAM (politiques basées sur une identité), vous pouvez utiliser la table ci-dessous comme référence. Ce tableau répertorie chaque opération d'API Storage Gateway, les actions correspondantes pour lesquelles vous pouvez accorder des autorisations. AWS pour laquelle vous pouvez accorder les autorisations. Vous spécifiez les actions dans le champ `Action` de la politique ainsi que la valeur des ressources dans le champ `Resource` de la politique.

Vous pouvez utiliser AWS dans les stratégies Storage Gateway pour exprimer des conditions. Pour obtenir la liste complète des clés à l'échelle d'AWS, veuillez consulter [Clés disponibles](#) dans le Guide de l'utilisateur IAM.

Note

Pour spécifier une action, utilisez le préfixe `storagegateway:` suivi du nom de l'opération d'API (par exemple, `storagegateway:ActivateGateway`). Pour chaque action Storage Gateway, vous pouvez spécifier un caractère générique (*) en tant que la ressource.

Pour obtenir la liste des ressources Storage Gateway avec leur format ARN, consultez [Ressources et opérations Storage Gateway](#).

L'API Storage Gateway et les autorisations requises pour les actions sont les suivantes.

[ActivateGateway](#)

Action(s) : `storagegateway:ActivateGateway`

Ressource: *

[AddCache](#)

Action(s) : storagegateway:AddCache

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[AddTagsToResource](#)

Action(s) : storagegateway:AddTagsToResource

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ou

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

ou

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

[AddUploadBuffer](#)

Action(s) : storagegateway:AddUploadBuffer

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[AddWorkingStorage](#)

Action(s) : storagegateway:AddWorkingStorage

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[CancelArchival](#)

Action(s) : storagegateway:CancelArchival

Ressource: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

[CancelRetrieval](#)

Action(s) : storagegateway:CancelRetrieval

Ressource: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

Action(s) : storagegateway:CreateCachediSCSIVolume

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

Action(s) : storagegateway:CreateSnapshot

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

Action(s) : storagegateway:CreateSnapshotFromVolumeRecoveryPoint

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

CreateStorediSCSIVolume

Action(s) : storagegateway:CreateStorediSCSIVolume

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateTapes

Action(s) : storagegateway:CreateTapes

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteBandwidthRateLimit

Action(s) : storagegateway>DeleteBandwidthRateLimit

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteChapCredentials

Action(s) : storagegateway>DeleteChapCredentials

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
target/*iSCSITarget*

DeleteGateway

Action(s) : storagegateway>DeleteGateway

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteSnapshotSchedule

Action(s) : storagegateway>DeleteSnapshotSchedule

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

DeleteTape

Action(s) : storagegateway>DeleteTape

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

Action(s) : storagegateway>DeleteTapeArchive

Ressource: *

DeleteVolume

Action(s) : storagegateway>DeleteVolume

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

DescribeBandwidthRateLimit

Action(s) : storagegateway:DescribeBandwidthRateLimit

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCache

Action(s) : storagegateway:DescribeCache

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeCachediSCSIVolumes

Action(s) : storagegateway:DescribeCachediSCSIVolumes

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

DescribeChapCredentials

Action(s) : storagegateway:DescribeChapCredentials

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/target/*iSCSItarget*

DescribeGatewayInformation

Action(s) : storagegateway:DescribeGatewayInformation

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeMaintenanceStartTime

Action(s) : storagegateway:DescribeMaintenanceStartTime

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeSnapshotSchedule

Action(s) : storagegateway:DescribeSnapshotSchedule

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeStorediSCSIVolumes

Action(s) : storagegateway:DescribeStorediSCSIVolumes

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/volume/*volume-id*

DescribeTapeArchives

Action(s) : storagegateway:DescribeTapeArchives

Ressource: *

DescribeTapeRecoveryPoints

Action(s) : storagegateway:DescribeTapeRecoveryPoints

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeTapes

Action(s) : storagegateway:DescribeTapes

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[DescribeUploadBuffer](#)

Action(s) : storagegateway:DescribeUploadBuffer

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[DescribeVTLDevices](#)

Action(s) : storagegateway:DescribeVTLDevices

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[DescribeWorkingStorage](#)

Action(s) : storagegateway:DescribeWorkingStorage

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[DisableGateway](#)

Action(s) : storagegateway:DisableGateway

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[ListGateways](#)

Action(s) : storagegateway:ListGateways

Ressource: *

[ListLocalDisks](#)

Action(s) : storagegateway:ListLocalDisks

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[ListTagsForResource](#)

Action(s) : storagegateway:ListTagsForResource

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ou

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

ou

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ListTapes

Action(s) : storagegateway:ListTapes

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumeInitiators

Action(s) : storagegateway:ListVolumeInitiators

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

ListVolumeRecoveryPoints

Action(s) : storagegateway:ListVolumeRecoveryPoints

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumes

Action(s) : storagegateway:ListVolumes

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RemoveTagsFromResource

Action(s) : storagegateway:RemoveTagsFromResource

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ou

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

ou

ARN:AWS:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ResetCache

Action(s) : storagegateway:ResetCache

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeArchive

Action(s) : storagegateway:RetrieveTapeArchive

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeRecoveryPoint

Action(s) : storagegateway:RetrieveTapeRecoveryPoint

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ShutdownGateway

Action(s) : storagegateway:ShutdownGateway

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

StartGateway

Action(s) : storagegateway:StartGateway

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateBandwidthRateLimit

Action(s) : storagegateway:UpdateBandwidthRateLimit

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

UpdateChapCredentials

Action(s) : storagegateway:UpdateChapCredentials

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
target/*iSCSItarget*

UpdateGatewayInformation

Action(s) : storagegateway:UpdateGatewayInformation

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateGatewaySoftwareNow](#)

Action(s) : storagegateway:UpdateGatewaySoftwareNow

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateMaintenanceStartTime](#)

Action(s) : storagegateway:UpdateMaintenanceStartTime

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateSnapshotSchedule](#)

Action(s) : storagegateway:UpdateSnapshotSchedule

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

[UpdateVTLDeviceType](#)

Action(s) : storagegateway:UpdateVTLDeviceType

Ressource: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
device/*vtldevice*

Voir aussi

- [Contrôle d'accès](#)
- [Exemples de stratégies gérées par le client](#)

Utilisation des rôles liés à un service pour Storage Gateway

Utiliser Storage GatewayAWS Identity and Access Management(IAM)[rôles liés à un service](#). Un rôle lié à un service est un type unique de rôle IAM lié directement à Storage Gateway. Les rôles liés à un service sont prédéfinis par Storage Gateway et incluent toutes les autorisations requises par le service pour appeler d'autres.AWSservices en votre nom.

Un rôle lié à un service simplifie la configuration de Storage Gateway, car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. Storage Gateway définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul Storage Gateway peut assumer ses rôles. Les

autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez [AWS Services qui fonctionnent avec IAM](#) et recherchez les services avec un Oui dans la colonne rôle lié au service. Choisissez un Oui ayant un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés au service pour Storage Gateway

Storage Gateway utilise le rôle lié à un service nommé `Rôle de service AWS pour Storage Gateway`—`Rôle de service AWS pour Storage Gateway`.

Le rôle lié à un service `AWSRoleForStorageGateway` approuve les services suivants pour assumer le rôle :

- `storagegateway.amazonaws.com`

La stratégie d'autorisations liée au rôle permet à Storage Gateway de réaliser les actions suivantes sur les ressources spécifiées :

- Action : `fsx:ListTagsForResource` sur `arn:aws:fsx:*:*:backup/*`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer et modifier un rôle lié à un service. Pour plus d'informations, consultez [Autorisations de rôles liés à un service](#) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Storage Gateway

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez une `Storage GatewayAssociateFileSystem` Appel d'API dans le `AWS Management Console`, le `AWS CLI`, ou le `AWSAPI`, Storage Gateway crée le rôle lié à un service pour vous.

Important

Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. De plus, si vous utilisiez le service Storage Gateway avant le 31 mars 2021, date à laquelle il commençait à prendre en charge les rôles liés à un service, Storage Gateway a créé le rôle

AWSServiceRoleForStorageGateway dans votre compte. Pour plus d'informations, consultez [Un nouveau rôle est apparu dans mon compte IAM](#).

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez une Storage GatewayAssociateFileSystemAppel d'API, Storage Gateway crée à nouveau le rôle lié à un service pour vous.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec Rôle de service AWS pour Storage Gatewaycas d'utilisation. Dans l'AWS CLI ou l'API AWS, créez un rôle lié au service avec le nom de service `storagegateway.amazonaws.com`. Pour de plus amples informations, consultez [Création d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour Storage Gateway

Storage Gateway ne vous permet pas de modifier le rôle lié à au service AWSServiceRoleForStorageGateway. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas modifier le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour en savoir plus, consultez [Modification d'un rôle lié à un service](#) dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour Storage Gateway

Storage Gateway ne supprime pas automatiquement le rôle AWSServiceRoleForStorageGateway. Pour supprimer le rôle AWSServiceRoleForStorageGateway, vous devez appeler `iam:DeleteSLRAPI`. Si aucune ressource de passerelle de stockage ne dépend du rôle lié au service, la suppression réussira, sinon la suppression échouera. Si vous souhaitez supprimer le rôle lié au service, vous devez utiliser les API `iam:DeleteRole` ou `iam:DeleteServiceLinkedRole`. Dans ce cas, vous devez utiliser les API Storage Gateway pour supprimer d'abord toutes les passerelles ou associations de systèmes de fichiers dans le compte, puis supprimer le rôle lié au service en utilisant `iam:DeleteRole` ou `iam:DeleteServiceLinkedRoleAPI`. Lorsque vous supprimez le rôle lié au service à l'aide d'IAM, vous devez utiliser Storage GatewayDisassociateFileSystemAssociationAPI d'abord pour supprimer toutes les associations de systèmes de fichiers du compte. Sinon, l'opération de suppression échouera.

Note

Si le service Storage Gateway utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer des ressources Storage Gateway utilisées par `AWSServiceRoleForStorageGateway`

1. Utilisez notre console de service, notre interface de ligne de commande ou notre API pour passer un appel qui nettoie les ressources et supprime le rôle ou utilisez la console IAM, l'interface de ligne de commande ou l'API pour effectuer la suppression. Dans ce cas, vous devez utiliser les API Storage Gateway pour supprimer d'abord les passerelles et les associations de systèmes de fichiers du compte.
2. Si vous utilisez la console, l'interface de ligne de commande ou l'API IAM, supprimez le rôle lié à un service à l'aide d'`IAM.DeleteRole` ou `DeleteServiceLinkedRoleAPI`.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le `AWS CLI`, ou le `AWSAPI` pour supprimer le rôle lié au service `AWSServiceRoleForStorageGateway`. Pour plus d'informations, consultez [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service Storage Gateway

Storage Gateway prend en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez [Points de terminaison du service AWS](#).

Storage Gateway ne prend actuellement pas en charge l'utilisation des rôles liés à un service dans toutes les régions où le service est disponible. Vous pouvez utiliser le rôle `AWSServiceRoleForStorageGateway` dans les régions suivantes.

Nom de la région	Identité de la région	Support dans Storage Gateway
US East (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui

Nom de la région	Identité de la région	Support dans Storage Gateway
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asia Pacific (Osaka)	ap-northeast-3	Oui
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Canada (Centre)	ca-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Paris)	eu-west-3	Oui
Amérique du Sud (Sao Paulo)	sa-east-1	Oui
AWS GovCloud (US)	us-gov-west-2	Oui

Journalisation et surveillance dans AWS Storage Gateway

Storage Gateway est intégré à AWS CloudTrail, un service qui enregistre les actions réalisées par un utilisateur, un rôle ou un AWSservice dans Storage Gateway. CloudTrail capture tous les appels d'API pour Storage Gateway en tant qu'événements. Les appels capturés incluent des appels de la console Storage Gateway et les appels de code aux opérations d'API Storage Gateway. Si vous créez un journal de suivi, vous pouvez activer la livraison continue des événements CloudTrail

à un compartiment Amazon S3, y compris des événements pour Storage Gateway. Si vous ne configurez pas de journal d'activité, vous pouvez toujours afficher les événements les plus récents dans la console CloudTrail dans l'historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été envoyée à Storage Gateway, l'adresse IP source à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres détails.

Pour en savoir plus sur CloudTrail, consultez le [AWS CloudTrailGuide de l'utilisateur](#) .

Informations Storage Gateway dans CloudTrail

CloudTrail est activé dans votre compte AWS lors de la création de ce dernier. Lorsqu'une activité se produit dans Storage Gateway, celle-ci est enregistrée dans un événement CloudTrail avec d'autresAWSévénements de service dansHistorique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour de plus amples informations, veuillez consulter [Affichage des événements avec l'historique des événements CloudTrail](#).

Pour un registre permanent des événements dans votreAWS, y compris les événements pour Storage Gateway, crée une piste. Un journal de suivi permet à CloudTrail de livrer des fichiers journaux dans un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres services AWS pour analyser et agir sur les données d'événements collectées dans les journaux CloudTrail. Pour en savoir plus, consultez les ressources suivantes :

- [Présentation de la création d'un journal d'activité](#)
- [Intégrations et services pris en charge par CloudTrail](#)
- [Configuration des Notifications de Amazon SNS pour CloudTrail](#)
- [Réception des fichiers journaux CloudTrail de plusieurs régions](#) et [Réception des fichiers journaux CloudTrail de plusieurs comptes](#)

Toutes les actions Storage Gateway sont journalisées et documentées dans le [Actions](#) sujet. À titre d'exemple, les appels vers les actions ActivateGateway, ListGateways et ShutdownGateway génèrent des entrées dans les fichiers journaux CloudTrail.

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre service AWS.

Pour plus d'informations, veuillez consulter [l'élément `userIdentity` CloudTrail](#).

Présentation des entrées des fichiers journaux Storage Gateway

Un journal de suivi est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Les fichiers journaux CloudTrail peuvent contenir une ou plusieurs entrées. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la requête, etc. Les fichiers journaux CloudTrail ne constituent pas une série ordonnée retraçant les appels d'API publiques. Ils ne suivent aucun ordre précis.

L'exemple suivant montre une entrée de journal CloudTrail qui illustre l'action .

```
{ "Records": [{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAI15AUEPBH2M7JTNCV",
    "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "JohnDoe"
  },
  "eventTime": "2014-12-04T16:19:00Z",
  "eventSource": "storagegateway.amazonaws.com",
  "eventName": "ActivateGateway",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
  "requestParameters": {
    "gatewayTimezone": "GMT-5:00",
```

```

    "gatewayName": "cloudtrailgatewayv1",
    "gatewayRegion": "us-east-2",
    "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
    "gatewayType": "VTL"
  },
  "responseElements": {
    "gatewayARN":
"arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayv1"
  },
  "requestID":
"54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
  "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
  "eventType": "AwsApiCall",
  "apiVersion": "20130630",
  "recipientAccountId": "444455556666"
}
]]
}

```

L'exemple suivant montre une entrée de journal CloudTrail qui illustre l'action ListGateways.

```

{
  "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAI5AUPEBH2M7JTNVC",
      "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
      "accountId": "111122223333", "accessKeyId": "
AKIAIOSFODNN7EXAMPLE",
      "userName": "JohnDoe"
    },
    "eventTime": "2014-12-03T19:41:53Z",
    "eventSource": "storagegateway.amazonaws.com",
    "eventName": "ListGateways",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli / 1.6.2 Python / 2.7.6
Linux / 2.6.18 - 164.el5",
    "requestParameters": null,
  }
]
}

```

```
        " responseElements ":null,
        "requestID ":"
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QEUE3KPGG6F0KSTAUU0 ",
        " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
d203a189ec8d ",
        " eventType ":" AwsApiCall ",
        " apiVersion ":" 20130630 ",
        " recipientAccountId ":" 444455556666"
    ]}
}
```

Validation de la conformité pourAWSStorage Gateway

Les auditeurs tiers évaluent la sécurité et la conformité deAWSStorage Gateway dans le cadre de plusieursAWSprogrammes de conformité. Ceux-ci comprennent SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, K-ISMS, ENS High, OSPAR et HITRUST CSF.

Pour obtenir une liste des services AWS relevant de programmes de conformité spécifiques, veuillez consulter [Services AWS relevant de programme de conformité](#). Pour obtenir des renseignements généraux, consultez [Programmes de conformité AWS](#).

Vous pouvez télécharger les rapports de l'audit externe avec AWS Artifact. Pour de plus amples informations, veuillez consulter [Téléchargement de rapports dans AWS Artifact](#).

Votre responsabilité de conformité lors de l'utilisation de Storage Gateway est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables.AWSfournit les ressources suivantes pour faciliter la conformité :

- [Guides de Quick Start \(démarrage rapide\) de la sécurité et de la conformité](#). Ces guides de déploiement traitent des considérations architecturales et fournissent des étapes 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](#) – Le livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications conformes à HIPAA.
- [Ressources de conformité AWS](#) – Cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- [Évaluation des ressources à l'aide de règles](#) dans le Guide du développeur AWS Config : le service évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.

- [AWS Security Hub](#) : ce service AWS fournit une vue complète de votre état de sécurité au sein d'AWS qui vous permet de vérifier votre conformité aux normes du secteur et aux bonnes pratiques de sécurité.

Résilience dans AWSStorage Gateway

L'infrastructure mondiale AWS s'articule autour de régions et de zones de disponibilité AWS. AWS Les Régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, 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 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.

Pour plus d'informations sur les régions et les zones de disponibilité AWS, consultez [AWS Infrastructure mondiale](#).

En plus du AWSStorage Gateway propose plusieurs fonctionnalités qui contribuent à la prise en charge des vos besoins en matière de résilience et de sauvegarde de données.

- Utilisez VMware vSphere High Availability (VMware HA) pour protéger les charges de travail de stockage contre les défaillances de matériel, d'hyperviseur ou de réseau. Pour de plus amples informations, veuillez consulter [Utilisation de VMware vSphere High Availability avec Storage Gateway](#).
- Utilisez AWS Backup pour sauvegarder vos volumes. Pour de plus amples informations, veuillez consulter [Utilisation d'AWS Backup pour sauvegarder vos volumes](#).
- Clonez votre volume à partir d'un point de récupération. Pour de plus amples informations, veuillez consulter [Clonage d'un volume](#).
- Archivez les bandes virtuelles dans Amazon S3 Glacier. Pour de plus amples informations, veuillez consulter [Archivage des bandes virtuelles](#).

Sécurité de l'infrastructure dans AWSStorage Gateway

En tant que service géré, AWSStorage Gateway est protégé par les procédures de sécurité du réseau mondial qui sont décrites dans le [Amazon Web Services : Présentation des processus de sécurité](#) livre blanc.

Vous utilisez AWS appels d'API publiés pour accéder à Storage Gateway via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser [AWS Security Token Service](#) (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Bonnes pratiques de sécurité pour Storage Gateway

AWSStorage Gateway fournit différentes fonctions de sécurité à prendre en compte lorsque vous développez et implémentez vos propres stratégies de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations. Pour de plus amples informations, veuillez consulter [AWS Bonnes pratiques de sécurité](#).

Résolution des problèmes de passerelle

Vous trouverez ci-après des informations sur le dépannage des problèmes liés aux passerelles, partages de fichiers, volumes, bandes virtuelles et instantanés. Les informations de dépannage de la passerelle sur site couvrent les passerelles déployées sur les clients VMware ESXi et Microsoft Hyper-V. Les informations de dépannage pour les partages de fichiers s'appliquent au type de passerelle de fichiers Amazon S3. Les informations de dépannage pour les volumes s'appliquent au type de passerelle de volume. Les informations de dépannage pour les bandes s'appliquent au type de passerelle de bande. Les informations de dépannage pour les problèmes de passerelles s'appliquent à l'utilisation des métriques CloudWatch. Les informations de dépannage relatives aux problèmes de haute disponibilité couvrent les passerelles exécutées sur la plateforme VMware vSphere High Availability (HA).

Rubriques

- [Dépannage des problèmes de passerelle sur site](#)
- [Dépannage de la configuration de Microsoft Hyper-V](#)
- [Dépannage des problèmes liés à la passerelle Amazon EC2](#)
- [Dépannage des problèmes d'appliance matérielle](#)
- [Dépannage des problèmes de passerelle de fichiers](#)
- [Dépannage des problèmes de partage de fichiers](#)
- [Notifications d'intégrité relatives à la haute disponibilité](#)
- [Dépannage des problèmes de haute disponibilité](#)
- [Bonnes pratiques pour la récupération de vos données](#)

Dépannage des problèmes de passerelle sur site

Vous trouverez ci-après des informations sur les problèmes types que vous êtes susceptibles de rencontrer avec les passerelles sur site et sur la façon d'activer AWS Support pour résoudre les problèmes de votre passerelle.

Le tableau suivant répertorie les problèmes types que vous pourriez rencontrer avec les passerelles sur site.

Problème	Action à exécuter
<p>Vous ne pouvez pas trouver l'adresse IP de votre passerelle.</p>	<p>Utilisez le client de l'hyperviseur pour vous connecter à votre hôte afin de rechercher l'adresse IP de la passerelle.</p> <ul style="list-style-type: none"> • Pour VMware ESXi, l'adresse IP de l'ordinateur virtuel se trouve dans le client vSphere de l'onglet Résumé. • Pour Microsoft Hyper-V, vous pouvez trouver l'adresse IP de l'ordinateur virtuel en vous connectant à la console locale. <p>Si vous avez toujours du mal à trouver l'adresse IP de la passerelle :</p> <ul style="list-style-type: none"> • Vérifiez que l'ordinateur virtuel est activé. Une adresse IP est attribuée à votre passerelle uniquement lorsque l'ordinateur virtuel est activé. • Attendez que le démarrage de l'ordinateur virtuel soit terminé. Si vous venez d'allumer l'ordinateur virtuel, la passerelle peut mettre quelques minutes pour finaliser sa séquence de démarrage.
<p>Vous rencontrez des problèmes de réseau ou de pare-feu.</p>	<ul style="list-style-type: none"> • Autoriser les ports appropriés pour votre passerelle. • Si vous utilisez un pare-feu ou un routeur pour filtrer ou limiter le trafic réseau, vous devez les configurer afin de permettre les communications sortantes vers ces points de terminaison de service pour les communications sortantes vers AWS. Pour plus d'informations sur les exigences de réseau et de pare-feu, consultez Exigences pour le réseau et le pare-feu.
<p>L'activation de votre passerelle échoue lorsque vous cliquez sur le Passez à l'activation dans la console de gestion Storage Gateway.</p>	<ul style="list-style-type: none"> • Vérifiez que l'ordinateur virtuel de la passerelle est accessible en faisant un ping de l'ordinateur virtuel à partir du client. • Vérifiez que votre machine virtuelle dispose d'une connectivité réseau à Internet. Sinon, vous aurez besoin de configurer un proxy SOCKS. Pour plus d'informations sur la procédure à utiliser, consultez Test de la connectivité réseau de votre passerelle.

Problème	Action à exécuter
	<ul style="list-style-type: none">• Vérifiez que l'heure de l'hôte est correcte, que l'hôte est configuré pour synchroniser son heure automatiquement sur un serveur NTP (Network Time Protocol) et que l'heure de l'ordinateur virtuel de la passerelle est correcte. Pour plus d'informations sur la synchronisation de l'heure des hôtes et ordinateurs virtuels de l'hyperviseur, consultez Configuration d'un serveur NTP (Network Time Protocol) pour votre passerelle.• Après l'exécution de ces étapes, vous pouvez recommencer le déploiement de la passerelle à l'aide de la console Storage Gateway et du Configuration et activation de la passerelle Assistant.• Vérifiez que votre ordinateur virtuel dispose d'au moins 7,5 Go de RAM. L'attribution de la passerelle échoue s'il y a moins de 7,5 Go de RAM. Pour plus d'informations, consultez Configuration requise de la passerelle de fichiers.
<p>Vous devez supprimer un disque alloué en tant qu'espace de tampon de chargement. Par exemple, vous devrez peut-être réduire la quantité d'espace du tampon de chargement d'une passerelle ou remplacer un disque utilisé comme tampon de chargement qui a échoué.</p>	

Problème	Action à exécuter
Vous avez besoin d'améliorer la bande passante entre votre passerelle et AWS.	<p>Vous pouvez améliorer la bande passante de votre passerelle à AWS en configurant votre connexion Internet à AWS sur une carte d'interface réseau (NIC) distincte de celle qui relie vos applications et la machine virtuelle de la passerelle. Cette approche est utile si vous avez une connexion haut débit à AWS et que vous voulez éviter les conflits de bande passante, notamment lors d'une restauration de l'instantané. Pour les besoins de charge de travail à haut débit, vous pouvez utiliser AWS Direct Connect pour établir une connexion réseau dédiée entre votre passerelle sur site et AWS. Pour mesurer la bande passante de la connexion de votre passerelle à AWS, utilisez les métriques <code>CloudBytesDownloaded</code> et <code>CloudBytesUploaded</code> de la passerelle. Pour en savoir plus sur ce sujet, consultez Performances. L'amélioration de votre connexion Internet permet d'éviter le remplissage de votre tampon de chargement.</p>

Problème	Action à exécuter
<p>Le débit vers ou depuis votre passerelle tombe à zéro.</p>	<ul style="list-style-type: none">• Dans la page Passerelle de la console Storage Gateway, vérifiez que les adresses IP de votre machine virtuelle de passerelle sont les mêmes que celles qui apparaissent avec le logiciel client de l'hyperviseur (autrement dit, le client VMware Vsphere ou Microsoft Hyper-V Manager). Si vous trouvez un décalage, redémarrez votre passerelle à partir de la console Storage Gateway, comme illustré dans la section Arrêt de la machine virtuelle de la passerelle. Après le redémarrage, les adresses dans la zone Adresses IP dans la console Storage Gateway Passerelle doit correspondre aux adresses IP de votre passerelle, que vous déterminez à partir du client de l'hyperviseur.• Pour VMware ESXi, l'adresse IP de l'ordinateur virtuel se trouve dans le client vSphere de l'onglet Résumé.• Pour Microsoft Hyper-V, vous pouvez trouver l'adresse IP de l'ordinateur virtuel en vous connectant à la console locale.• Vérifiez la connectivité à AWS de votre passerelle, comme décrit dans Test de la connectivité réseau de votre passerelle.• Vérifiez la configuration de la carte réseau de votre passerelle et veillez à ce que toutes les interfaces qui doivent être activées pour la passerelle le soient réellement. Pour afficher la configuration de la carte réseau de votre passerelle, suivez les instructions de Configuration des cartes réseau pour votre passerelle et sélectionnez l'option d'affichage de la configuration du réseau de la passerelle. <p>Vous pouvez afficher le débit vers et depuis votre passerelle à partir de la console Amazon CloudWatch. Pour plus d'informations sur la mesure du débit de votre passerelle vers AWS, consultez Performances.</p>

Problème	Action à exécuter
Vous rencontrez des problèmes d'importation (déploiement) de Storage Gateway sur Microsoft Hyper-V.	Consultez Dépannage de la configuration de Microsoft Hyper-V , qui traite des problèmes les plus courants de déploiement d'une passerelle sur Microsoft Hyper-V.
Vous recevez un message indiquant : « Les données qui ont été écrites sur le volume dans votre passerelle ne sont pas stockées en toute sécurité surAWS».	Vous recevez ce message si l'ordinateur virtuel de la passerelle a été créé à partir d'un clone ou d'un instantané d'un autre ordinateur virtuel de passerelle. Si ce n'est pas le cas, contactezAWS Support.

Activation deAWS Supportpour résoudre les problèmes de votre passerelle hébergée sur site

Storage Gateway fournit une console locale que vous pouvez utiliser pour exécuter plusieurs tâches de maintenance, y compris l'activation de l'activationAWS Supportpour accéder à votre passerelle afin de vous aider à résoudre les problèmes de passerelle. Par défaut,AWS Supportl'accès à votre passerelle est désactivé. Vous activez cet accès par le biais de la console locale de l'hôte. Pour donnerAWS Supportaccès à votre passerelle, vous devez d'abord vous connecter à la console locale pour l'hôte, accéder à la console de la passerelle de stockage, puis vous connecter au serveur de support.

Pour activerAWS Supportaccès à votre passerelle

1. Connectez-vous à la console locale de l'hôte.
 - VMware ESXi — Pour plus d'informations, consultez[Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Microsoft Hyper-V : pour de plus amples informations, veuillez consulter[Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).

La console locale ressemble à ce qui suit.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

2. À l'invite, entrez **5** pour ouvrir **AWS Support Console Channel**.
3. Saisissez **h** pour ouvrir la fenêtre **AVAILABLE COMMANDS (COMMANDES DISPONIBLES)**.
4. Effectuez l'une des actions suivantes :
 - Si votre passerelle utilise un point de terminaison public, dans le **COMMANDES DISPONIBLES** fenêtre, saisissez **open-support-channel** pour se connecter au support client de Storage Gateway. Autorisez le port TCP 22 afin de pouvoir ouvrir un canal de support vers AWS. Lorsque vous vous connectez au support client, Storage Gateway vous attribue un numéro de support. Notez ce numéro.
 - Si votre passerelle utilise un point de terminaison de VPC, dans la fenêtre **AVAILABLE COMMANDS (COMMANDES DISPONIBLES)**, saisissez **open-support-channel**. Si votre passerelle n'est pas activée, indiquez le point de terminaison VPC ou l'adresse IP pour vous connecter au service clientèle pour Storage Gateway. Autorisez le port TCP 22 afin de pouvoir ouvrir un canal de support vers AWS. Lorsque vous vous connectez au support client, Storage Gateway vous attribue un numéro de support. Notez ce numéro.

```
AVAILABLE COMMANDS
type 'man <command name>' to find out more information about commands

ip                Show / manipulate routing, devices, and tunnels
save-routing-table Save newly added routing table entry
ifconfig          View or configure network interfaces
iptables          Administration tool for IPv4 packet filtering and NAT
save-iptables     Persist IP tables
testconn          Test network connectivity
man               Display command manual pages
open-support-channel Connect to Storage Gateway Support
h                 Display available command list
exit              Return to Storage Gateway Configuration menu

Gateway Console: open-support-channel
```

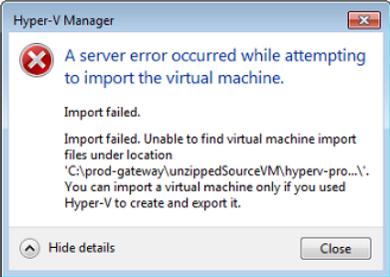
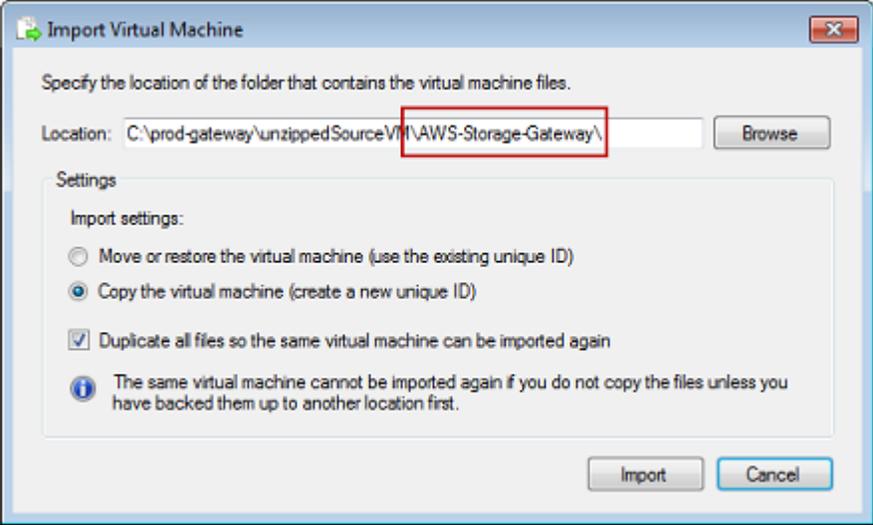
Note

Le numéro de canal n'est pas un numéro de port de TCP/UDP (Transmission Control Protocol/User Datagram Protocol). Au lieu de cela, la passerelle permet une connexion SSH (Secure Shell) (TCP 22) aux serveurs Storage Gateway et fournit le canal de support pour la connexion.

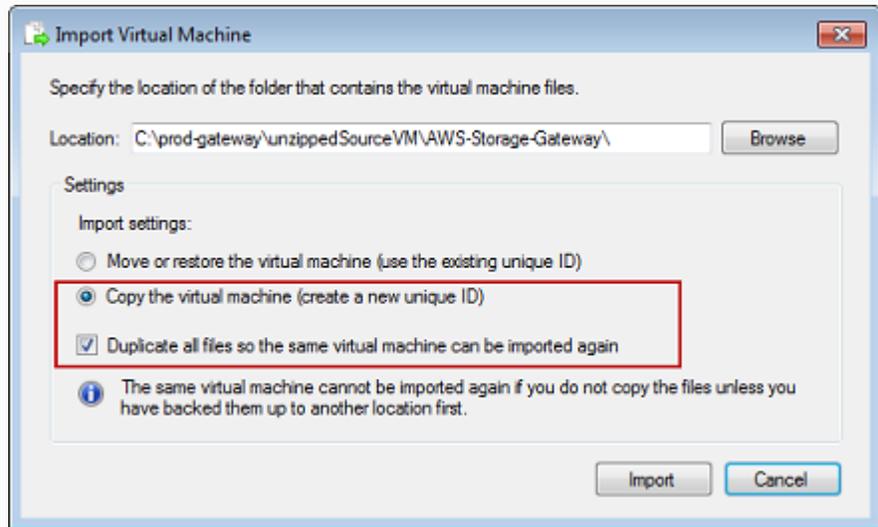
5. Une fois que le canal de support est établi, fournissez votre numéro de service de support àAWS SupportdoncAWS Supportpeuvent fournir une assistance au dépannage.
6. Une fois la session de support terminée, saisissez **q** pour y mettre fin. Ne fermez pas la session tant que le support Amazon Web Services ne vous a pas notifié que la session de support est terminée.
7. Saisissez**exit**pour vous déconnecter de la console Storage Gateway.
8. Suivez les invites pour quitter la console locale.

Dépannage de la configuration de Microsoft Hyper-V

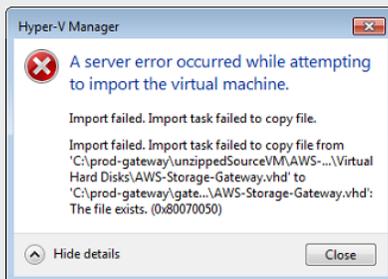
Le tableau suivant répertorie les problèmes types que vous êtes susceptibles de rencontrer lors du déploiement de Storage Gateway sur la plateforme Microsoft Hyper-V.

Problème	Action à exécuter
<p data-bbox="110 254 483 621">Vous essayez d'importer une passerelle et vous recevez le message d'erreur : « L'importation a échoué. Impossible de trouver le fichier d'importation de l'ordinateur virtuel sous l'emplacement... ».</p> 	<p data-bbox="542 254 1305 285">Cette erreur se produit dans les conditions suivantes :</p> <ul data-bbox="542 331 1495 558" style="list-style-type: none">• Si vous pointez pas vers la racine des fichiers source décompressés de la passerelle. La dernière partie de l'emplacement que vous spécifiez dans la boîte de dialogue Importer un ordinateur virtuel doit être <code>AWS-Storage-Gateway\</code>, comme le montre l'exemple suivant :  • Si vous avez déjà déployé une passerelle, mais n'avez pas sélectionné l'option Copier l'ordinateur virtuel et que vous avez activé l'option Dupliquer tous les fichiers dans la boîte de dialogue Importer un ordinateur virtuel, l'ordinateur virtuel a été créé à l'emplacement où vous avez décompressé les fichiers de la passerelle et vous ne pouvez pas réimporter à partir de cet emplacement. Pour résoudre ce problème, obtenez une nouvelle copie des fichiers source décompressés de la passerelle et copiez-les dans un nouvel emplacement. Utilisez le nouvel emplacement comme source de l'importation. L'exemple suivant montre les options que vous devez activer si vous avez l'intention de créer plusieurs passerelles à partir d'un emplacement de fichiers source décompressés.

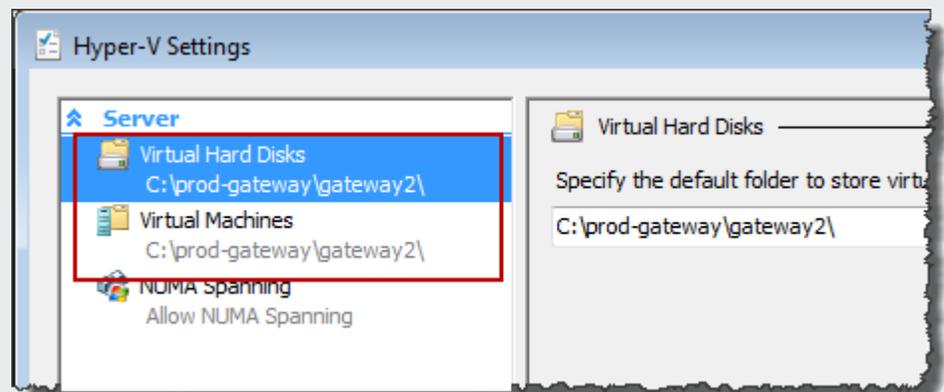
Problème	Action à exécuter
----------	-------------------



Vous essayez d'importer une passerelle et vous recevez le message d'erreur : « L'importation a échoué. La tâche d'importation n'a pas pu copier le fichier. »

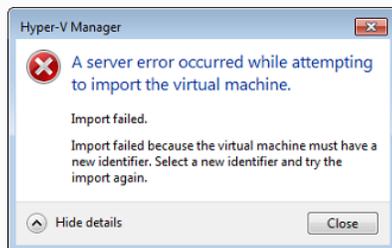


Si vous avez déjà déployé une passerelle et que vous essayez de réutiliser des dossiers par défaut qui stockent les fichiers du disque dur virtuel et les fichiers de configuration de l'ordinateur virtuel, cette erreur se produit. Pour résoudre ce problème, spécifiez les nouveaux emplacements dans la boîte de dialogue Paramètres Hyper-V.



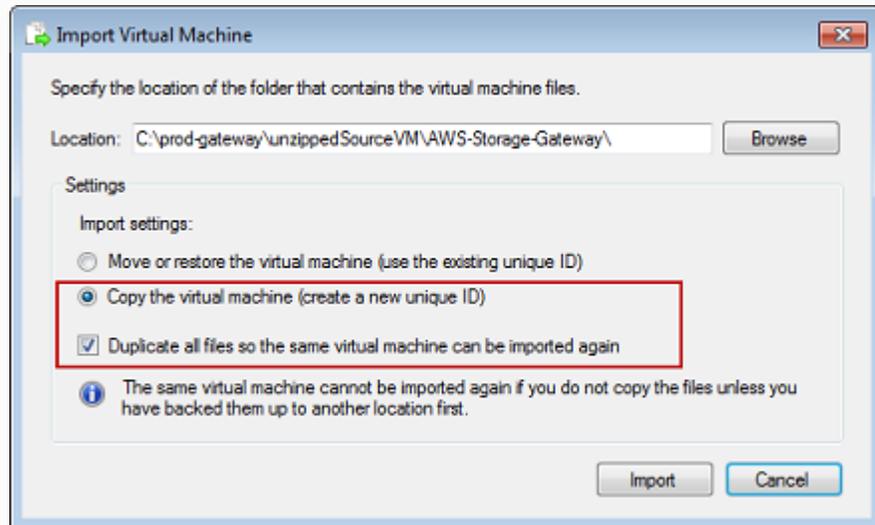
Problème

Vous essayez d'importer une passerelle et vous recevez un message d'erreur : « L'importation a échoué. L'importation a échoué car l'ordinateur virtuel doit avoir un nouvel identificateur. Sélectionnez un nouvel identificateur et réessayez l'importation. »



Action à exécuter

Lorsque vous importez la passerelle, veillez à sélectionner l'option Copier l'ordinateur virtuel et à cocher l'option Dupliquer tous les fichiers dans la boîte de dialogue Importer un ordinateur virtuel pour créer un ID unique pour l'ordinateur virtuel. L'exemple suivant montre les options de la boîte de dialogue Importer un ordinateur virtuel que vous devez utiliser.

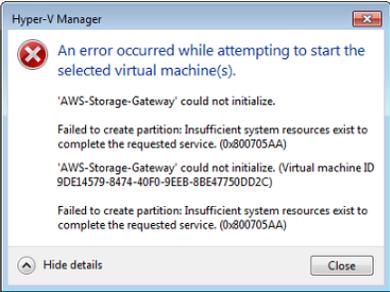


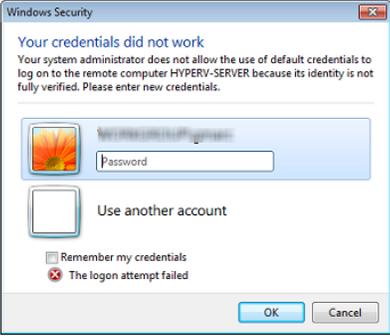
Vous essayez de démarrer un ordinateur virtuel de passerelle et vous recevez le message d'erreur : « Le paramètre de processeur de partition enfant est incompatible avec la partition parent. »



Cette erreur est probablement provoquée par une différence d'UC entre les processeurs obligatoires pour la passerelle et les processeurs disponibles sur l'hôte. Veillez à ce que le nombre d'UC de l'ordinateur virtuel soit pris en charge par l'hyperviseur sous-jacent.

Pour plus d'informations sur les exigences pour Storage Gateway, consultez [Configuration requise de la passerelle de fichiers](#).

Problème	Action à exécuter
<p>Vous essayez de démarrer une machine virtuelle de passerelle et vous recevez le message d'erreur : « Impossible de créer une partition : Les ressources sont insuffisantes pour terminer le service demandé. »</p> 	<p>Cette erreur est probablement provoquée par un écart de RAM entre la RAM obligatoire pour la passerelle et la RAM disponible sur l'hôte.</p> <p>Pour plus d'informations sur les exigences pour Storage Gateway, consultez Configuration requise de la passerelle de fichiers.</p>
<p>Les instantanés et les mises à jour logicielles de la passerelle se produisent à des moments qui diffèrent par rapport à ce qui était prévu.</p>	<p>L'horloge de l'ordinateur virtuel de la passerelle peut être décalée par rapport à l'heure réelle ; il s'agit d'une dérive de l'horloge. Vérifiez et corrigez l'heure de l'ordinateur virtuel à l'aide de l'option de synchronisation de l'heure de la console de passerelle. Pour plus d'informations, consultez Configuration d'un serveur NTP (Network Time Protocol) pour votre passerelle.</p>
<p>Vous devez placer les fichiers décompressés Microsoft Hyper-V Storage Gateway Gateway sur le système de fichiers hôte.</p>	<p>Accédez à l'hôte comme vous le feriez avec un serveur Microsoft Windows standard. Par exemple, si l'hôte de l'hyperviseur est nommé <code>hyperv-server</code> , vous pouvez utiliser le chemin UNC suivant <code>\\hyperv-server\c\$</code> , ce qui implique que le nom <code>hyperv-server</code> peut être résolu ou est défini dans votre fichier d'hôtes local.</p>

Problème	Action à exécuter
<p data-bbox="110 226 506 403">Vous êtes invité à saisir les informations d'identification lors de la connexion à l'hyperviseur.</p> 	<p data-bbox="539 226 1507 352">Ajoutez vos informations d'identification utilisateur en tant qu'administrateur local pour l'hôte de l'hyperviseur à l'aide de l'outil Sconfig.cmd.</p>

Dépannage des problèmes liés à la passerelle Amazon EC2

Les sections suivantes répertorient les problèmes types que vous êtes susceptibles de rencontrer avec votre passerelle déployée sur Amazon EC2. Pour plus d'informations sur la différence entre une passerelle sur site et une passerelle déployée dans Amazon EC2, consultez [Déploiement d'une passerelle de fichiers sur un hôte Amazon EC2](#).

Pour de plus amples informations sur l'utilisation du stockage éphémère, veuillez consulter [Utilisation du stockage éphémère avec des passerelles EC2](#).

Rubriques

- [L'activation de votre passerelle n'a pas eu lieu après quelques instants](#)
- [Vous ne trouvez pas votre instance de passerelle EC2 dans la liste des instances](#)
- [Vous voulez AWS Support pour résoudre les problèmes de votre passerelle EC2](#)

L'activation de votre passerelle n'a pas eu lieu après quelques instants

Vérifiez les points suivants dans la console Amazon EC2 :

- Le port 80 est activé dans le groupe de sécurité que vous avez associé à l'instance. Pour de plus amples informations sur l'ajout d'une règle au groupe de sécurité, veuillez consulter [Ajout d'une règle de groupe de sécurité](#) dans le Manuel de l'utilisateur Amazon EC2 pour les instances Linux.

- L'instance de passerelle est marquée comme étant en cours d'exécution. Dans la console Amazon EC2, l'état Pour l'instance doit être EN COURS D'EXÉCUTION.
- Assurez-vous que le type d'instance Amazon EC2 répond aux exigences minimales, comme décrit dans la section [Besoins de stockage](#).

Après avoir corrigé le problème, essayez à nouveau d'activer la passerelle. Pour cela, ouvrez la console Storage Gateway, choisissez Déploiement d'une nouvelle passerelle sur Amazon EC2, puis entrez à nouveau l'adresse IP de l'instance.

Vous ne trouvez pas votre instance de passerelle EC2 dans la liste des instances

Si vous n'avez pas attribué de balise de ressource à l'instance et que vous avez de nombreuses instances en cours d'exécution, il peut être difficile de savoir quelle instance vous avez lancée. Dans ce cas, vous pouvez procéder de la façon suivante pour rechercher l'instance de la passerelle :

- Vérifiez le nom de l'Amazon Machine Image (AMI) sur l'onglet Description de l'instance. Une instance basée sur l'AMI Storage Gateway doit commencer par le texte **aws-storage-gateway-ami**.
- Si vous avez plusieurs instances basées sur l'AMI Storage Gateway, vérifiez l'heure de lancement de l'instance afin de trouver l'instance appropriée.

Vous voulez AWS Support pour résoudre les problèmes de votre passerelle EC2

Storage Gateway fournit une console locale que vous pouvez utiliser pour exécuter plusieurs tâches de maintenance, y compris l'activation de l'activation AWS Support pour accéder à votre passerelle afin de vous aider à résoudre les problèmes de passerelle. Par défaut, AWS Support l'accès à votre passerelle est désactivé. Vous activez cet accès par le biais de la console locale Amazon EC2. Vous vous connectez à la console locale Amazon EC2 via SSH (Secure Shell). Pour vous connecter avec succès via SSH, le groupe de sécurité de l'instance doit avoir une règle qui ouvre le port TCP 22.

Note

Si vous ajoutez une règle à un groupe de sécurité existant, la nouvelle règle s'applique à toutes les instances qui utilisent ce groupe de sécurité. Pour plus d'informations sur les

groupes de sécurité et sur l'ajout d'une règle à un groupe de sécurité, consultez [Groupes de sécurité Amazon EC2](#) dans le Guide de l'utilisateur Amazon EC2.

Pour AWS Support vous devez d'abord vous connecter à votre passerelle, vous devez d'abord vous connecter à la console locale pour l'instance Amazon EC2, puis accéder à la console de la passerelle de stockage, puis fournir l'accès.

Pour activer AWS Support accès à une passerelle déployée sur une instance Amazon EC2

1. Connectez-vous à la console locale pour votre instance Amazon EC2. Pour plus d'informations, consultez [Connectez-vous à votre instance](#) dans le Guide de l'utilisateur Amazon EC2.

Vous pouvez utiliser la commande suivante pour vous connecter à la console locale de l'instance EC2.

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

Note

Le *CLÉ PRIVÉE* est le `.pem` contenant le certificat privé de la key pair EC2 que vous avez utilisée pour lancer l'instance Amazon EC2. Pour de plus amples informations, veuillez consulter [Récupération de la clé publique pour votre paire de clés sous Linux](#) dans le Guide de l'utilisateur Amazon EC2.

Le *INSTANCE-PUBLIC-DNS-NAME* est le nom DNS (Domain Name System) public de votre instance Amazon EC2 sur laquelle la passerelle est exécutée. Pour obtenir ce nom DNS public, sélectionnez l'instance Amazon EC2 dans la console EC2, puis cliquez sur le bouton `Description Onglet`.

2. À l'invite, entrez `6 - Command Prompt` pour ouvrir AWS Support Console Channel.
3. Saisissez `h` pour ouvrir la fenêtre AVAILABLE COMMANDS (COMMANDES DISPONIBLES).
4. Effectuez l'une des actions suivantes :
 - Si votre passerelle utilise un point de terminaison public, dans le `COMMANDES DISPONIBLES` fenêtre, saisissez `open-support-channel` pour se connecter au support client de Storage Gateway. Autorisez le port TCP 22 afin de pouvoir ouvrir un canal de support vers AWS. Lorsque vous vous connectez au support client, Storage Gateway vous attribue un numéro de support. Notez ce numéro.

- Si votre passerelle utilise un point de terminaison de VPC, dans la fenêtre AVAILABLE COMMANDS (COMMANDES DISPONIBLES), saisissez **open-support-channel**. Si votre passerelle n'est pas activée, indiquez le point de terminaison VPC ou l'adresse IP pour vous connecter au service clientèle pour Storage Gateway. Autorisez le port TCP 22 afin de pouvoir ouvrir un canal de support vers AWS. Lorsque vous vous connectez au support client, Storage Gateway vous attribue un numéro de support. Notez ce numéro.

Note

Le numéro de canal n'est pas un numéro de port de TCP/UDP (Transmission Control Protocol/User Datagram Protocol). Au lieu de cela, la passerelle permet une connexion SSH (Secure Shell) (TCP 22) aux serveurs Storage Gateway et fournit le canal de support pour la connexion.

5. Une fois que le canal de support est établi, fournissez votre numéro de service de support à AWS Support. AWS Support peut fournir une assistance au dépannage.
6. Une fois la session de support terminée, saisissez **q** pour y mettre fin. Ne fermez pas la session tant que le support Amazon Web Services ne vous a pas notifié que la session de support est terminée.
7. Saisissez **exit** pour quitter la console Storage Gateway.
8. Suivez les menus de la console pour vous déconnecter de l'instance de Storage Gateway.

Dépannage des problèmes d'appliance matérielle

Les rubriques suivantes présentent les problèmes rencontrés avec l'appliance matérielle Storage Gateway et les suggestions sur le dépannage.

Vous ne pouvez pas déterminer l'adresse IP du service

Lorsque vous tentez de vous connecter à votre service, veillez à utiliser l'adresse IP du service au lieu de l'adresse IP de l'hôte. Configurez l'adresse IP du service dans la console du service, et l'adresse IP de l'hôte dans la console matérielle. Vous voyez la console matérielle lorsque vous démarrez l'appliance matérielle. Pour accéder à la console du service sur la console matérielle, choisissez Open Service Console.

Comment effectuer une réinitialisation d'usine ?

Si vous devez effectuer une réinitialisation d'usine sur votre appareil, contactez l'équipe du dispositif matériel Storage Gateway pour obtenir de l'aide, comme décrit dans la section Support ci-après.

Où obtenez-vous le support Dell iDRAC ?

Le serveur Dell PowerEdge R640 est livré avec l'interface de gestion Dell iDRAC. Nous vous recommandons la procédure suivante :

- Si vous utilisez l'interface de gestion iDRAC, vous devez modifier le mot de passe par défaut. Pour de plus amples informations sur les informations d'identification iDRAC, veuillez consulter [Dell PowerEdge - Quels sont le nom d'utilisateur et le mot de passe par défaut pour iDRAC ?](#).
- Afin d'éviter des failles de sécurité, vérifiez que le microprogramme est à jour.
- Si l'interface réseau iDRAC est transférée sur un port normal (em), des problèmes de performances peuvent se produire ou le fonctionnement de l'appliance peut être perturbé.

Vous ne trouvez pas le numéro de série de l'appliance matérielle

Pour trouver le numéro de série de l'appliance matérielle, accédez à la page **Matériel** dans la console Storage Gateway, comme illustré ci-dessous.

Storage Gateway

Gateways

File shares

Volumes

Tapes

Hardware

Successfully launched File Gateway on praksuji-bh

Order appliance Quotes and orders Activate appliance Actions

Filter by hardware appliance name, ID or launched gateway type.

Hardware Appliance Name	Hardware Appliance ID	Model	Launched Gateway
<input checked="" type="checkbox"/> praksuji-bh	vi5loueix9yotyn5	Dell PowerEdge R640	File Gateway
<input type="checkbox"/> praksuji-hw-pdx	wlyd0dgh6j7kg4no	Dell PowerEdge R640	File Gateway

Details

Name	praksuji-bh	Vendor	Dell
ID	vi5loueix9yotyn5	Model	Dell PowerEdge R640
Time Zone	GMT	Serial Number	5Q8Y0M2
		RAID Volume Manager	ZFS

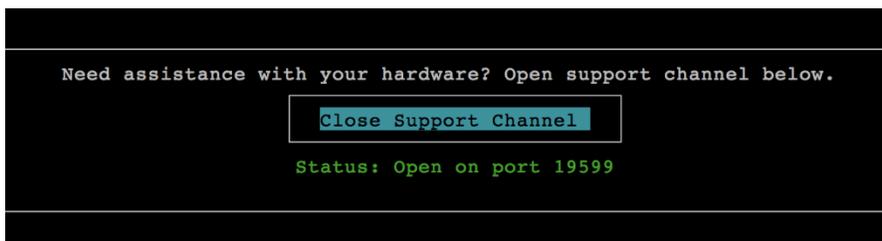
Où obtenir la prise en charge de l'appliance matérielle

Pour contacter le support de Storage Gateway Hardware Appliance, voir [AWS Support](#).

LeAWS SupportUne équipe peut vous demander d'activer le canal d'assistance technique pour résoudre les problèmes de la passerelle à distance. Il n'est pas nécessaire que ce port soit ouvert pour que votre passerelle fonctionne normalement, mais il doit l'être pour résoudre les problèmes. Vous pouvez activer le canal de support technique à partir de la console matérielle, comme indiqué dans la procédure ci-après.

Pour ouvrir un canal de support technique pourAWS

1. Ouvrez la console matérielle.
2. Choisissez Open Support Channel (Ouvrir un canal de support technique), comme indiqué ci-dessous.



Le numéro de port attribué doit apparaître dans les 30 secondes en l'absence de problèmes de connectivité réseau ou de pare-feu.

3. Notez le numéro de port et indiquez-le àAWS Support.

Dépannage des problèmes de passerelle de fichiers

Vous pouvez configurer votre passerelle de fichiers avec un groupe de journaux Amazon CloudWatch lorsque vous exécutez VMware vSphere High Availability (HA). Si vous le faites, vous recevez des notifications sur l'intégrité de votre passerelle de fichiers et sur les erreurs rencontrées par la passerelle de fichiers. Vous trouverez des informations sur ces notifications d'erreur et d'intégrité dans CloudWatch Logs.

Dans les sections suivantes, vous trouverez des informations qui peuvent vous aider à comprendre la cause de chaque notification d'erreur et d'intégrité et à résoudre les problèmes.

Rubriques

- [Erreur: InaccessibleStorageClass](#)
- [Erreur: Accès S3 refusé](#)
- [Erreur: InvalidObjectState](#)

- [Erreur: ObjectMissing](#)
- [: Notification Redémarrer](#)
- [: Notification HardReboot](#)
- [: Notification HealthCheckFailure](#)
- [: Notification AvailabilityMonitorTest](#)
- [Erreur: RoleTrustRelationshipInvalid](#)
- [Dépannage des métriques CloudWatch](#)

Erreur: InaccessibleStorageClass

Vous pouvez obtenir un `InaccessibleStorageClass` erreur lorsqu'un objet a été transféré hors de la classe de stockage Standard Amazon S3.

Ici, généralement, votre passerelle de fichiers rencontre l'erreur lorsqu'elle tente de charger l'objet spécifié dans le compartiment S3 ou de lire l'objet à partir du compartiment S3. Avec cette erreur, l'objet est généralement déplacé vers Amazon S3 Glacier ou S3 Glacier Deep Archive.

Pour résoudre une erreur de `InaccessibleStorageClass`

- Redéplacez l'objet de la classe de stockage S3 Glacier ou S3 Glacier Deep Archive vers S3.

Si vous déplacez l'objet dans le compartiment S3 pour corriger une erreur de chargement, le fichier finit par être chargé. Si vous déplacez l'objet dans le compartiment S3 pour corriger une erreur de lecture, le client SMB ou NFS de la passerelle de fichiers peut alors lire le fichier.

Erreur: Accès S3 refusé

Vous pouvez obtenir un `S3AccessDenied` erreur d'accès au compartiment Amazon S3 d'un partage de fichiers AWS Identity and Access Management (IAM) rôle. Dans ce cas, le compartiment S3 accède au rôle IAM spécifié par `roleArn` dans l'erreur n'autorise pas l'opération impliquée. L'opération n'est pas permise en raison des autorisations pour les objets du répertoire spécifié par le préfixe Amazon S3.

Pour résoudre une erreur `S3AccessDenied`

- Modifier la stratégie d'accès Amazon S3 attachée à `roleArn` dans le journal d'intégrité de la passerelle de fichiers pour autoriser l'opération Amazon S3. Assurez-vous que la stratégie d'accès

autorise l'opération à l'origine de l'erreur. En outre, permettez l'autorisation pour le répertoire spécifié dans le journal de `prefix`. Pour plus d'informations sur les autorisations Amazon S3, consultez [Spécification des autorisations d'une stratégie](#) dans Manuel de l'utilisateur Amazon Simple Storage Service.

Ces opérations peuvent entraîner cette erreur `S3AccessDenied` :

- `S3HeadObject`
- `S3GetObject`
- `S3ListObjects`
- `S3DeleteObject`
- `S3PutObject`

Erreur: `InvalidObjectState`

Vous pouvez obtenir un `InvalidObjectState` lorsqu'un enregistreur autre que la passerelle de fichiers spécifiée modifie le fichier spécifié dans le compartiment S3 spécifié. Par conséquent, l'état du fichier pour la passerelle de fichiers ne correspond pas à son état dans Amazon S3. Les chargements ultérieurs du fichier dans Amazon S3 ou les récupérations du fichier à partir d'Amazon S3 échouent.

Pour résoudre une erreur `InvalidObjectState`

Si l'opération qui modifie le fichier est `S3Upload` ou `S3GetObject`, procédez comme suit :

1. Enregistrez la dernière copie du fichier dans le système de fichiers local de votre client SMB ou NFS (vous avez besoin de cette copie de fichier à l'étape 4). Si la version du fichier dans Amazon S3 est la plus récente, téléchargez cette version. Vous pouvez effectuer cette opération avec AWS Management Console ou avec l'AWS CLI.
2. Supprimez le fichier dans Amazon S3 à l'aide de l'AWS Management Console ou AWS CLI.
3. Supprimez le fichier de la passerelle de fichiers à l'aide de votre client SMB ou NFS.
4. Copiez la dernière version du fichier que vous avez enregistrée à l'étape 1 sur Amazon S3 à l'aide de votre client SMB ou NFS. Pour ce faire, utilisez votre passerelle de fichiers.

Erreur: ObjectMissing

Vous pouvez obtenir un `ObjectMissing` lorsqu'un enregistreur autre que la passerelle de fichiers spécifiée supprime le fichier spécifié du compartiment S3. Tous les chargements suivants sur Amazon S3 ou extractions à partir d'Amazon S3 pour l'objet échouent.

Pour résoudre une erreur `ObjectMissing`

Si l'opération qui modifie le fichier est `S3Upload` ou `S3GetObject`, procédez comme suit :

1. Enregistrez la dernière copie du fichier dans le système de fichiers local de votre client SMB ou NFS (vous avez besoin de cette copie de fichier à l'étape 3).
2. Supprimez le fichier de la passerelle de fichiers à l'aide de votre client SMB ou NFS.
3. Copiez la dernière version du fichier que vous avez enregistrée à l'étape 1 à l'aide de votre client SMB ou NFS. Pour ce faire, utilisez votre passerelle de fichiers.

: Notification Redémarrer

Vous pouvez obtenir une notification de redémarrage lorsque la machine virtuelle de la passerelle est redémarrée. Vous pouvez redémarrer une machine virtuelle de passerelle à l'aide de la console de gestion des hyperviseurs de VM ou de la console Storage Gateway. Vous pouvez également la redémarrer à l'aide du logiciel de la passerelle pendant le cycle de maintenance de la passerelle.

Si l'heure du redémarrage se situe dans les 10 minutes de [l'heure de démarrage de la maintenance](#) configurée de la passerelle, ce redémarrage est probablement une occurrence normale et non un signe de problème. Si le redémarrage s'est produit largement en dehors de la fenêtre de maintenance, vérifiez si la passerelle a été redémarrée manuellement.

: Notification HardReboot

Vous pouvez obtenir une notification `HardReboot` lorsque la machine virtuelle de la passerelle est redémarrée de façon inattendue. Un tel redémarrage peut être dû à une perte de puissance, à une défaillance matérielle ou à un autre événement. Pour les passerelles VMware, une réinitialisation par la surveillance de l'application vSphere High Availability peut déclencher cet événement.

Lorsque votre passerelle s'exécute dans un tel environnement, vérifiez la présence de la notification `HealthCheckFailure` et consultez le journal des événements VMware pour la machine virtuelle.

: Notification HealthCheckFailure

Pour une passerelle sur VMware vSphere HA, vous pouvez recevoir une notification HealthCheckFailure lorsqu'une vérification de l'état échoue et qu'un redémarrage de la machine virtuelle est demandé. Cet événement se produit également lors d'un test de surveillance de la disponibilité, indiqué par une notification AvailabilityMonitorTest. Dans ce cas, la notification HealthCheckFailure est attendue.

Note

Cette notification concerne uniquement les passerelles VMware.

Si cet événement se produit à plusieurs reprises sans notification AvailabilityMonitorTest, recherchez les problèmes éventuels de votre infrastructure de machine virtuelle (stockage, mémoire, etc.). Si vous avez besoin d'aide supplémentaire, contactez AWS Support.

: Notification AvailabilityMonitorTest

Vous obtenez une AvailabilityMonitorTest notification lorsque vous [exécutez un test de Surveillance de la disponibilité et des applications](#) sur les passerelles exécutées sur une plateforme VMware vSphere HA.

Erreur: RoleTrustRelationshipInvalid

Vous obtenez cette erreur lorsque le rôle IAM pour un partage de fichiers présente une relation d'approbation IAM mal configurée (autrement dit, le rôle IAM ne fait pas confiance au mandataire Storage Gateway nommé `storagegateway.amazonaws.com`). Par conséquent, la passerelle de fichiers ne serait pas en mesure d'obtenir les informations d'identification pour exécuter des opérations sur le compartiment S3 qui sauvegarde le partage de fichiers.

Pour résoudre une erreur RoleTrustRelationshipInvalid

- Utilisez la console IAM ou l'API IAM pour inclure `storagegateway.amazonaws.com` en tant que principal approuvé par l'iamRole de votre partage de fichiers. Pour obtenir des informations sur le rôle IAM, consultez [Tutoriel : déléguer l'accès à travers AWS comptes utilisant des rôles IAM](#).

Dépannage des métriques CloudWatch

Vous trouverez ci-après des informations sur les actions visant à résoudre les problèmes liés à l'utilisation des métriques Amazon CloudWatch avec Storage Gateway.

Rubriques

- [Votre passerelle réagit lentement lorsque vous parcourez des répertoires](#)
- [Votre passerelle ne répond pas](#)
- [Votre passerelle met du temps à transférer des données vers Amazon S3](#)
- [Votre passerelle effectue plus d'opérations Amazon S3 que prévu](#)
- [Vous ne voyez pas de fichiers dans votre compartiment Amazon S3](#)
- [Votre tâche de sauvegarde de passerelle échoue ou des erreurs se produisent lors de l'écriture sur votre passerelle.](#)

Votre passerelle réagit lentement lorsque vous parcourez des répertoires

Si votre passerelle de fichiers réagit lentement lorsque vous exécutez `ls` ou parcourez les répertoires, vérifiez les mesures CloudWatch `IndexFetch` et `IndexEviction` :

- Si l'icône `IndexFetch` est supérieure à 0 lorsque vous exécutez `ls` dans les répertoires de navigation, votre passerelle de fichiers a démarré sans informations sur le contenu du répertoire concerné et a dû accéder à Amazon S3. Les opérations ultérieures pour répertorier le contenu de ce répertoire devraient s'exécuter plus rapidement.
- Si l'icône `IndexEviction` La métrique est supérieure à 0, cela signifie que votre passerelle de fichiers a atteint la limite de ce qu'elle peut gérer dans son cache à ce moment-là. Dans ce cas, votre passerelle de fichiers doit libérer de l'espace de stockage du répertoire le moins récemment consulté pour répertorier un nouveau répertoire. Si cela se produit fréquemment et qu'il y a un impact sur les performances, contactez AWS Support.

Discutez avec AWS Support le contenu du compartiment S3 associé et les recommandations pour améliorer les performances en fonction de votre cas d'utilisation.

Votre passerelle ne répond pas

Si votre passerelle de fichiers ne répond pas, procédez comme suit :

- Dans le cas d'une mise à jour logicielle ou d'un redémarrage récent, vérifiez la métrique `IOWaitPercent`. Cette métrique indique le pourcentage de temps pendant lequel le processeur est inactif lorsqu'une demande d'E/S disque est en attente. Dans certains cas, ce pourcentage peut être élevé (10 ou plus) et peut avoir augmenté après le redémarrage ou la mise à jour du serveur. Dans ces cas, votre passerelle de fichiers peut être limitée par un disque racine lent pendant la reconstitution du cache d'index en RAM. Vous pouvez résoudre ce problème en utilisant un disque physique plus rapide pour le disque racine.
- Si l'icône `MemUsedBytes` est égale ou presque identique à la mesure `MemTotalBytes`, votre passerelle de fichiers est à court de RAM disponible. Assurez-vous que votre passerelle de fichiers dispose au moins de la RAM minimale requise. Si c'est déjà le cas, envisagez d'ajouter plus de RAM à votre passerelle de fichiers en fonction de votre charge de travail et de votre cas d'utilisation.

Si le partage de fichiers est SMB, le problème peut également être dû au nombre de clients SMB connectés au partage de fichiers. Pour connaître le nombre de clients connectés à un moment donné, vérifiez la métrique `SMBV(1/2/3)Sessions`. Si de nombreux clients sont connectés, vous devrez peut-être ajouter plus de RAM à votre passerelle de fichiers.

Votre passerelle met du temps à transférer des données vers Amazon S3

Si votre passerelle de fichiers met du temps à transférer des données vers Amazon S3, procédez comme suit :

- Si l'icône `CachePercentDirty` La métrique est égale ou supérieure à 80, votre passerelle de fichiers écrit des données plus rapidement sur le disque qu'elle ne peut charger les données dans Amazon S3. Pensez à augmenter la bande passante pour le chargement à partir de votre passerelle de fichiers, à ajouter un ou plusieurs disques de cache ou à ralentir les écritures client.
- Si l'icône `CachePercentDirty` métrique présente une valeur peu élevée, vérifiez la `IoWaitPercent` Métriques. Si `IoWaitPercent` est supérieure à 10, votre passerelle de fichiers peut être limitée par la vitesse du disque de cache local. Nous recommandons des disques SSD (Solid State Drive) locaux pour votre cache, de préférence NVM Express (NVMe). Si de tels disques ne sont pas disponibles, essayez d'utiliser plusieurs disques de cache provenant de disques physiques distincts pour améliorer les performances.
- Si `S3PutObjectRequestTime`, `S3UploadPartRequestTime`, ou `S3GetObjectRequestTime` sont élevés, il peut y avoir un goulot d'étranglement réseau.

Essayez d'analyser votre réseau pour vérifier que la passerelle dispose de la bande passante attendue.

Votre passerelle effectue plus d'opérations Amazon S3 que prévu

Si votre passerelle de fichiers effectue plus d'opérations Amazon S3 que prévu, vérifiez le `FilesRenamed` Métriques. Les opérations de renommage sont coûteuses à exécuter dans Amazon S3. Optimisez votre flux de travail pour réduire le nombre d'opérations de renommage.

Vous ne voyez pas de fichiers dans votre compartiment Amazon S3

Si vous remarquez que les fichiers sur la passerelle ne sont pas reflétés dans le compartiment Amazon S3, vérifiez le `FilesFailingUpload` Métriques. Si la mesure indique que certains fichiers ne sont pas chargés, vérifiez vos notifications de santé. Lorsque les fichiers ne parviennent pas à charger, la passerelle génère une notification d'intégrité contenant plus de détails sur le problème.

Votre tâche de sauvegarde de passerelle échoue ou des erreurs se produisent lors de l'écriture sur votre passerelle.

Si votre tâche de sauvegarde de passerelle de fichiers échoue ou si des erreurs se produisent lors de l'écriture sur votre passerelle de fichiers, procédez comme suit :

- Si l'icône `CachePercentDirty` La métrique est égale ou supérieure à 90 %, votre passerelle de fichiers ne peut pas accepter de nouvelles écritures sur le disque car l'espace disponible sur le disque de cache est insuffisant. Pour connaître la vitesse des chargements entre votre passerelle de fichiers et vers Amazon FSx ou Amazon S3, consultez le `CloudBytesUploaded` Métriques. Comparez cette mesure avec le `WriteBytes`, qui indique la vitesse à laquelle le client écrit des fichiers sur votre passerelle de fichiers. Si votre passerelle de fichiers écrit plus rapidement qu'elle ne peut charger sur Amazon FSx ou Amazon S3, ajoutez plus de disques de cache pour couvrir au minimum la taille de la tâche de sauvegarde. Vous pouvez également augmenter la bande passante de chargement.
- Si une tâche de sauvegarde échoue, mais que la commande `CachePercentDirty` est inférieure à 80 %, votre passerelle de fichiers est peut-être confrontée à un délai d'expiration de session côté client. Pour SMB, vous pouvez augmenter ce délai d'expiration à l'aide de la commande `PowerShell Set-SmbClientConfiguration -SessionTimeout 300`. L'exécution de cette commande définit le délai d'expiration à 300 secondes.

Pour NFS, assurez-vous que le client est monté à l'aide d'un montage physique et non d'un montage logiciel.

Dépannage des problèmes de partage de fichiers

Vous trouverez ci-après des informations sur les actions à mettre en œuvre si vous rencontrez des problèmes inattendus avec votre partage de fichiers.

Rubriques

- [Votre partage de fichiers est bloqué dans le statut CREATING](#)
- [Vous ne pouvez pas créer de partage de fichiers](#)
- [Les partages de fichiers SMB n'autorisent pas plusieurs méthodes d'accès différentes](#)
- [Plusieurs partages de fichiers ne peuvent pas écrire dans le compartiment S3 mappé](#)
- [Impossible de télécharger des fichiers dans votre compartiment S3](#)
- [Impossible de modifier le chiffrement par défaut pour utiliser SSE-KMS pour chiffrer les objets stockés dans mon compartiment S3](#)
- [Les modifications apportées directement dans un compartiment S3 avec le versionnement d'objet activé peuvent affecter ce que vous voyez dans votre partage de fichiers](#)
- [Lorsque vous écrivez dans un compartiment S3 avec le versionnement d'objet activé, Amazon S3 File Gateway peut créer plusieurs versions d'un objet S3](#)
- [Les modifications apportées à un compartiment S3 ne sont pas reflétées dans Storage Gateway](#)
- [Les autorisations ACL ne fonctionnent pas comme prévu](#)
- [Les performances de votre passerelle ont diminué après avoir effectué une opération récursive](#)

Votre partage de fichiers est bloqué dans le statut CREATING

Lorsque votre partage de fichiers est en cours de création, l'état est CREATION. L'état passe à DISPONIBLE après la création du partage de fichiers. Si votre partage de fichiers est bloqué dans l'état CREATION, procédez comme suit :

1. Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.
2. Assurez-vous que le compartiment S3 sur lequel vous avez mappé votre partage de fichiers existe. Si le compartiment n'existe pas, créez-le. Une fois le compartiment créé, l'état du partage de

- fichiers passe à DISPONIBLE. Pour plus d'informations sur la création d'un compartiment S3, consultez [Créer un compartiment](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.
3. Assurez-vous que le nom de votre compartiment respecte les règles d'attribution de nom de compartiments dans Amazon S3. Pour plus d'informations, consultez la section [Règles relatives à l'attribution des noms de compartiments](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.
 4. Assurez-vous que le rôle IAM que vous avez utilisé pour accéder au compartiment S3 possède les autorisations appropriées et vérifiez que le compartiment S3 est répertorié en tant que ressource dans la stratégie IAM. Pour plus d'informations, consultez [Octroi d'accès à un compartiment Amazon S3](#).

Vous ne pouvez pas créer de partage de fichiers

1. Si vous ne parvenez pas à créer un partage de fichiers car celui-ci est bloqué dans l'état CREATION, vérifiez que le compartiment S3 auquel vous avez mappé votre partage de fichiers existe. Pour plus d'informations sur la procédure à appliquer, consultez [Votre partage de fichiers est bloqué dans le statut CREATING](#), ci-dessus.
2. Si le compartiment S3 existe, vérifiez que AWS Security Token Service est activé dans la région dans laquelle vous créez le partage de fichiers. Si aucun jeton de sécurité n'est activé, activez-en un. Pour plus d'informations sur l'activation d'un jeton à l'aide de AWS Security Token Service, voir [Activation et désactivation AWSSTS dans un AWSRegion \(Région\)](#) dans le IAM User Guide.

Les partages de fichiers SMB n'autorisent pas plusieurs méthodes d'accès différentes

Les restrictions suivantes s'appliquent aux partages de fichiers SMB :

1. Lorsqu'un client tente de monter à la fois un partage de fichiers Active Directory et SMB avec un accès invité, le message d'erreur suivant s'affiche : `Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Un utilisateur Windows ne peut pas rester connecté à deux partages de fichiers SMB avec un accès invité, et peut se trouver déconnecté lorsqu'une nouvelle connexion avec un accès invité est établie.

3. Un client Windows ne peut pas monter à la fois un partage de fichiers SMB invité et Active Directory exporté par la même passerelle.

Plusieurs partages de fichiers ne peuvent pas écrire dans le compartiment S3 mappé

Nous déconseillons de configurer votre compartiment S3 pour autoriser plusieurs partages de fichiers à écrire dans un compartiment S3. Cette opération peut donner des résultats imprévisibles.

Nous vous recommandons plutôt d'autoriser un seul partage de fichiers à écrire dans chaque compartiment S3. Créez une stratégie de compartiment autorisant uniquement le rôle associé à votre partage de fichiers à écrire dans le compartiment. Pour plus d'informations, consultez [Bonnes pratiques de partage de fichiers](#).

Impossible de télécharger des fichiers dans votre compartiment S3

Si vous ne parvenez pas à charger des fichiers dans votre compartiment S3, procédez comme suit :

1. Vérifiez que vous avez accordé l'accès nécessaire pour que la passerelle de fichiers Amazon S3 charge des fichiers dans votre compartiment S3. Pour plus d'informations, consultez [Octroi d'accès à un compartiment Amazon S3](#).
2. Assurez-vous que le rôle qui a créé le compartiment dispose des autorisations d'écriture dans le compartiment S3. Pour plus d'informations, consultez [Bonnes pratiques de partage de fichiers](#).
3. Si votre passerelle de fichiers utilise SSE-KMS pour le chiffrement, assurez-vous que le rôle IAM associé au partage de fichiers inclut kms:Encrypt, kms:Decrypt, KMS : Reencrypt, kms:GenerateDataKey, etkms:DescribeKey autorisations. Pour de plus amples informations, veuillez consulter [Utilisation des stratégies basées sur l'identité \(stratégies IAM\) pour Storage Gateway](#).

Impossible de modifier le chiffrement par défaut pour utiliser SSE-KMS pour chiffrer les objets stockés dans mon compartiment S3

Si vous modifiez le chiffrement par défaut et effectuez un chiffrement SSE-KMS (côté serveur) avec AWS KMS—les clés gérées par) la valeur par défaut pour votre compartiment S3, les objets stockés dans le compartiment par une passerelle de fichiers Amazon S3 ne sont pas chiffrés avec SSE-KMS. Par défaut, une passerelle de fichiers S3 utilise le chiffrement côté serveur géré avec

Amazon S3 (SSE-S3) lorsqu'elle écrit des données dans un compartiment S3. Si vous changez la valeur par défaut, votre chiffrement ne sera pas automatiquement changé.

Pour changer le chiffrement en vue d'utiliser SSE-KMS avec votre propre clé AWS KMS, vous devez activer le chiffrement SSE-KMS. Pour ce faire, vous devez fournir l'Amazon Resource Name (ARN) de la clé KMS lorsque vous créez votre partage de fichiers. Vous pouvez également mettre à jour les paramètres KMS de votre partage de fichiers à l'aide de l'opération d'API `UpdateNFSFileShare` ou `UpdateSMBFileShare`. Cette mise à jour s'applique aux objets stockés dans les compartiments S3 après la mise à jour. Pour plus d'informations, consultez [Chiffrement des données avec AWS KMS](#).

Les modifications apportées directement dans un compartiment S3 avec le versionnement d'objet activé peuvent affecter ce que vous voyez dans votre partage de fichiers

Si votre compartiment S3 contient des objets écrits par un autre client, il se peut que la vue que vous avez du compartiment S3 se soit plus à jour, suite à la gestion des versions d'objets du compartiment S3. Vous devez toujours actualiser votre cache avant d'examiner les fichiers qui vous intéressent.

La gestion des versions d'objets est une fonctionnalité facultative de compartiment S3 qui participe à la protection des données en stockant plusieurs copies d'un objet portant le même nom. Chaque copie possède une valeur d'ID distincte, par exemple `file1.jpg :ID="xxx"` et `file1.jpg :ID="yyy"`. Le nombre d'objets portant le même nom et leur durée de vie sont contrôlés par des stratégies de cycle de vie Amazon S3. Pour de plus amples informations sur ces concepts Amazon S3, consultez [Utilisation de la gestion des versions](#) et [Gestion du cycle de vie des objets](#) dans le Manuel du développeur Amazon S3.

Lorsque vous supprimez un objet versionné, celui-ci est indiqué par un marqueur de suppression, mais conservé. Seul le propriétaire d'un compartiment S3 peut supprimer définitivement un objet dont la gestion des versions est activée.

Les fichiers affichés dans votre passerelle de fichiers S3 correspondent aux versions les plus récentes des objets qui se trouvent dans un compartiment S3 au moment de leur récupération ou de l'actualisation du cache. Les passerelles de fichiers S3 ignorent toutes les versions plus anciennes ou objets marqués pour suppression. Lorsque vous lisez un fichier, vous lisez les données de la version la plus récente. Lorsque vous écrivez un fichier dans votre partage de fichiers, votre passerelle de fichiers S3 crée une nouvelle version d'un objet nommé contenant vos modifications, et cette version devient la plus récente.

Votre passerelle de fichiers S3 continue la lecture de la version antérieure, et les mises à jour que vous apportez sont basées sur la version antérieure si une nouvelle version est ajoutée au compartiment S3 en dehors de votre application. Pour lire la version la plus récente d'un objet, utilisez l'action d'API [RefreshCache](#) ou procédez à une actualisation depuis la console, comme décrit dans [Actualisation des objets dans votre compartiment Amazon S3](#).

 Important

Nous déconseillons d'écrire des objets ou fichiers dans votre compartiment S3 File Gateway S3 depuis l'extérieur du partage de fichiers.

Lorsque vous écrivez dans un compartiment S3 avec le versionnement d'objet activé, Amazon S3 File Gateway peut créer plusieurs versions d'un objet S3

Lorsque le versionnement d'objet est activé, plusieurs versions d'un objet peuvent être créées dans Amazon S3 à chaque mise à jour d'un fichier à partir de votre client NFS ou SMB. Voici des scénarios qui peuvent entraîner la création de plusieurs versions d'un objet dans votre compartiment S3 :

- Lorsqu'un fichier est modifié dans Amazon S3 File Gateway par un client NFS ou SMB après son téléchargement sur Amazon S3, la passerelle de fichiers S3 télécharge les données nouvelles ou modifiées au lieu de charger le fichier entier. La modification du fichier entraîne la création d'une nouvelle version de l'objet Amazon S3.
- Lorsqu'un fichier est écrit sur la passerelle de fichiers S3 par un client NFS ou SMB, la passerelle de fichiers S3 télécharge les données du fichier vers Amazon S3 suivies de ses métadonnées (propriétaires, horodatage, etc.). Le téléchargement des données de fichier crée un objet Amazon S3, et le téléchargement des métadonnées du fichier met à jour les métadonnées de l'objet Amazon S3. Ce processus crée une autre version de l'objet, entraînant deux versions d'un objet.
- Lorsque la passerelle de fichiers S3 télécharge des fichiers plus volumineux, il peut être nécessaire de charger des morceaux plus petits du fichier avant que le client n'ait fini d'écrire sur la passerelle de fichiers. Cela peut être dû notamment à libérer de l'espace cache ou à augmenter le taux d'écriture dans un fichier. Cela peut entraîner plusieurs versions d'un objet dans le compartiment S3.

Vous devez surveiller votre compartiment S3 pour déterminer le nombre de versions d'un objet existant avant de configurer des stratégies de cycle de vie pour déplacer des objets vers différentes classes de stockage. Vous devez configurer l'expiration du cycle de vie pour les versions précédentes afin de minimiser le nombre de versions dont vous disposez pour un objet dans votre compartiment S3. L'utilisation de la réplication de même région (SRR) ou de la réplication entre régions (CRR) entre compartiments S3 augmentera le stockage utilisé. Pour de plus amples informations sur la réplication, veuillez consulter [Réplication](#).

 Important

Ne configurez pas la réplication entre les compartiments S3 tant que vous n'avez pas compris la quantité de stockage utilisée lorsque le versionnement d'objet est activé.

L'utilisation de compartiments S3 versionnés peut augmenter considérablement la quantité de stockage dans Amazon S3, car chaque modification apportée à un fichier crée une nouvelle version de l'objet S3. Amazon S3 continue à stocker toutes ces versions par défaut, sauf si vous créez spécifiquement une stratégie pour remplacer ce comportement et limiter le nombre de versions conservées. Si vous remarquez un nombre anormalement élevé d'objets stockés dont la gestion des versions est activée, vérifiez que vos stratégies de stockage sont correctement définies. Une augmentation du nombre de réponses HTTP 503-slow down aux requêtes du navigateur peut également résulter de problèmes au niveau de la gestion des versions d'objets.

Si vous activez la gestion des versions d'objets après avoir installé une passerelle de fichiers S3, tous les objets uniques sont conservés (ID="NULL") et vous pouvez tous les voir dans le système de fichiers. Un ID unique est attribué aux nouvelles versions d'objets (les versions plus anciennes sont conservées). En fonction de l'horodatage de l'objet, seul l'objet versionné le plus récent est visible dans le système de fichiers NFS.

Une fois que vous avez activé la gestion des versions d'objets, votre compartiment S3 ne peut plus être désactivé pour la gestion des versions. Toutefois, vous pouvez désactiver la gestion des versions. Lorsque vous désactivez la gestion des versions, un ID est attribué à un nouvel objet. S'il existe un objet du même nom avec une valeur ID="NULL", la version antérieure est remplacée. Toutefois, toute version contenant un ID dont la valeur n'est pas NULL sera conservée. L'horodatage permet d'identifier un nouvel objet comme l'actuel, et c'est celui-là qui apparaît dans le système de fichiers NFS.

Les modifications apportées à un compartiment S3 ne sont pas reflétées dans Storage Gateway

Storage Gateway met automatiquement à jour le cache de partage de fichiers lorsque vous écrivez des fichiers dans le cache localement à l'aide du partage de fichiers. Toutefois, Storage Gateway ne met pas automatiquement à jour le cache lorsque vous téléchargez un fichier directement sur Amazon S3. Lorsque vous faites cela, vous devez exécuter un `RefreshCache` pour voir les modifications apportées au partage de fichiers. Si vous avez plusieurs partages de fichiers, vous devez exécuter le `RefreshCache` opération sur chaque partage de fichiers.

Vous pouvez actualiser le cache à l'aide de la console Storage Gateway et de la console AWS Command Line Interface (AWS CLI) :

- Pour actualiser le cache à l'aide de la console Storage Gateway, consultez [Actualisation des objets](#) dans votre compartiment Amazon S3.
- Pour actualiser le cache à l'aide de la commande AWS CLI :
 1. Exécutez la commande `aws storagegateway list-file-shares`
 2. Copiez l'Amazon Resource Name (ARN) du partage de fichiers avec le cache que vous souhaitez actualiser.
 3. Exécutez le `refresh-cache` avec votre ARN comme valeur de `--file-share-arn` :

```
aws storagegateway refresh-cache --file-share-arn
arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
```

Pour automatiser l'`RefreshCache` opération, voir [Comment puis-je automatiser l'opération RefreshCache sur Storage Gateway ?](#)

Les autorisations ACL ne fonctionnent pas comme prévu

Si les autorisations des listes de contrôle d'accès (ACL) ne fonctionnent pas comme escompté avec votre partage de fichiers SMB, vous pouvez effectuer un test.

Pour ce faire, vous devez d'abord tester les autorisations sur un serveur Microsoft Windows ou un partage de fichiers Windows local. Ensuite, comparez le comportement au partage de fichiers de votre passerelle.

Les performances de votre passerelle ont diminué après avoir effectué une opération récursive

Dans certains cas, vous pouvez effectuer une opération récursive, telle que renommer un répertoire ou activer l'héritage d'une liste de contrôle d'accès (ACL), et le forcer dans l'arborescence. Si vous procédez ainsi, votre passerelle de fichiers S3 applique de façon récursive l'opération à tous les objets du partage de fichiers.

Par exemple, supposons que vous appliquiez l'héritage à des objets existants dans un compartiment S3. Votre passerelle de fichiers S3 applique, de façon récursive, l'héritage à tous les objets du compartiment. Ces opérations peuvent entraîner une dégradation des performances de votre passerelle.

Notifications d'intégrité relatives à la haute disponibilité

Lorsque vous exécutez votre passerelle sur la plateforme VMware vSphere High Availability (HA), vous pouvez recevoir des notifications d'intégrité. Pour plus d'informations sur les notifications relatives à l'état, consultez [Dépannage des problèmes de haute disponibilité](#).

Dépannage des problèmes de haute disponibilité

Vous trouverez ci-dessous des informations sur les actions à entreprendre si vous rencontrez des problèmes de disponibilité.

Rubriques

- [Notification d'Health](#)
- [Métriques](#)

Notification d'Health

Lorsque vous exécutez votre passerelle sur VMware vSphere HA, toutes les passerelles produisent les notifications d'intégrité suivantes pour votre groupe de journaux Amazon CloudWatch configuré. Ces notifications vont dans un flux de journaux appelé `AvailabilityMonitor`.

Rubriques

- [: Notification Redémarrer](#)

- : [Notification HardReboot](#)
- : [Notification HealthCheckFailure](#)
- : [Notification AvailabilityMonitorTest](#)

: Notification Redémarrer

Vous pouvez obtenir une notification de redémarrage lorsque la machine virtuelle de la passerelle est redémarrée. Vous pouvez redémarrer une machine virtuelle de passerelle à l'aide de la console de gestion des hyperviseurs de VM ou de la console Storage Gateway. Vous pouvez également la redémarrer à l'aide du logiciel de la passerelle pendant le cycle de maintenance de la passerelle.

Action à exécuter

Si l'heure du redémarrage se situe dans les 10 minutes de l'[heure de démarrage de la maintenance](#) configurée de la passerelle, ce redémarrage est probablement une occurrence normale et non un signe de problème. Si le redémarrage s'est produit largement en dehors de la fenêtre de maintenance, vérifiez si la passerelle a été redémarrée manuellement.

: Notification HardReboot

Vous pouvez obtenir une notification `HardReboot` lorsque la machine virtuelle de la passerelle est redémarrée de façon inattendue. Un tel redémarrage peut être dû à une perte de puissance, à une défaillance matérielle ou à un autre événement. Pour les passerelles VMware, une réinitialisation par la surveillance de l'application vSphere High Availability peut déclencher cet événement.

Action à exécuter

Lorsque votre passerelle s'exécute dans un tel environnement, vérifiez la présence de la notification `HealthCheckFailure` et consultez le journal des événements VMware pour la machine virtuelle.

: Notification HealthCheckFailure

Pour une passerelle sur VMware vSphere HA, vous pouvez recevoir une notification `HealthCheckFailure` lorsqu'une vérification de l'état échoue et qu'un redémarrage de la machine virtuelle est demandé. Cet événement se produit également lors d'un test de surveillance de la disponibilité, indiqué par une notification `AvailabilityMonitorTest`. Dans ce cas, la notification `HealthCheckFailure` est attendue.

 Note

Cette notification concerne uniquement les passerelles VMware.

Action à exécuter

Si cet événement se produit à plusieurs reprises sans notification `AvailabilityMonitorTest`, recherchez les problèmes éventuels de votre infrastructure de machine virtuelle (stockage, mémoire, etc.). Si vous avez besoin d'aide supplémentaire, contactez [AWS Support](#).

: Notification `AvailabilityMonitorTest`

Pour une passerelle sur VMware vSphere HA, vous pouvez obtenir une `AvailabilityMonitorTest` notification lorsque vous [exécutez un test du `Surveillance de la disponibilité et des applications` système](#) dans VMware.

Métriques

La métrique `AvailabilityNotifications` est disponible sur toutes les passerelles. Cette métrique représente le nombre de notifications d'intégrité liées à la disponibilité et générées par la passerelle. Utilisez la statistique Sum pour observer si la passerelle rencontre des événements liés à la disponibilité. Consultez votre groupe de journaux CloudWatch configuré pour plus de détails sur les événements.

Bonnes pratiques pour la récupération de vos données

Bien que cela soit rare, votre passerelle peut rencontrer une défaillance irrécupérable. Une panne peut se produire sur l'ordinateur virtuel (VM), la passerelle elle-même, le stockage local ou ailleurs. En cas de défaillance, nous vous recommandons de suivre les instructions de la section appropriée pour récupérer vos données.

 Important

Storage Gateway ne prend pas en charge la récupération d'un ordinateur virtuel de passerelle à partir d'un instantané créé par votre hyperviseur ou de votre Amazon EC2 Amazon Machine Image (AMI). Si l'ordinateur virtuel de la passerelle fonctionne mal,

activez une nouvelle passerelle et récupérez vos données pour cette passerelle à l'aide des instructions ci-après.

Rubriques

- [Récupération après un arrêt inattendu de la machine virtuelle](#)
- [Récupération de vos données à partir d'un disque cache défectueux](#)
- [Récupération de vos données depuis un centre de données inaccessible](#)

Récupération après un arrêt inattendu de la machine virtuelle

Si votre ordinateur virtuel s'arrête de façon inattendue, par exemple pendant une panne de courant, votre passerelle devient inaccessible. Lorsque la connectivité réseau et l'alimentation sont restaurés, votre passerelle devient accessible et commence à fonctionner normalement. Voici quelques actions que vous pouvez mettre en œuvre à ce moment-là pour faciliter la récupération de vos données :

- Si une panne entraîne des problèmes de connectivité réseau, vous pouvez résoudre le problème. Pour plus d'informations sur le test de la connectivité réseau, consultez [Test de la connectivité réseau de votre passerelle](#).
- Si votre passerelle fonctionne mal et si des problèmes se produisent avec vos volumes ou bandes suite à un arrêt inattendu, vous pouvez récupérer vos données. Pour plus d'informations sur la récupération de vos données, consultez les sections suivantes qui s'appliquent à votre scénario.

Récupération de vos données à partir d'un disque cache défectueux

Si votre disque de cache rencontre une défaillance, nous vous recommandons de mettre en œuvre les actions suivantes pour récupérer vos données en fonction de votre situation :

- Si la panne s'est produite car un disque de cache a été supprimé de votre hôte, fermez la passerelle, ajoutez à nouveau le disque, puis redémarrez la passerelle.
- Si le disque de cache est corrompu ou inaccessible, fermez la passerelle, réinitialisez le disque de cache, reconfigurez le disque pour le stockage de cache, puis redémarrez la passerelle.

Pour plus d'informations, consultez [Récupération de vos données à partir d'un disque cache défectueux](#).

Récupération de vos données depuis un centre de données inaccessible

Si votre passerelle ou votre centre de données devient inaccessible pour une raison quelconque, vous pouvez récupérer vos données sur une autre passerelle dans un autre centre de données ou les récupérer sur une passerelle hébergée sur une instance Amazon EC2. Si vous n'avez pas accès à un autre centre de données, nous vous recommandons de créer la passerelle sur une instance Amazon EC2. Les étapes à suivre dépendent du type de la passerelle à partir de laquelle vous récupérez les données.

Pour récupérer des données depuis une passerelle de fichiers dans un centre de données inaccessible

Pour une passerelle de fichiers, vous mappez un nouveau partage de fichiers au compartiment Amazon S3 qui contient les données que vous souhaitez récupérer.

1. Créez et activez une nouvelle passerelle de fichiers sur un hôte Amazon EC2. Pour plus d'informations, consultez [Déploiement d'une passerelle de fichiers sur un hôte Amazon EC2](#).
2. Créez un nouveau partage de fichiers sur la passerelle EC2 que vous avez créée. Pour de plus amples informations, veuillez consulter [Pour créer un partage de fichiers](#).
3. Montez votre partage de fichiers sur votre client et mappez-le sur le compartiment S3 qui contient les données que vous souhaitez récupérer. Pour de plus amples informations, veuillez consulter [Montez et utilisez votre partage de fichiers](#).

Ressources supplémentaires Storage Gateway

Dans cette section, vous trouverez des informations sur AWS et des logiciels, outils et ressources tiers qui peuvent vous aider à configurer ou à gérer votre passerelle, ainsi que sur les quotas Storage Gateway.

Rubriques

- [Configuration de l'hôte](#)
- [Obtention d'une clé d'activation pour votre passerelle](#)
- [Utilisation d'AWS Direct Connect avec Storage Gateway](#)
- [Exigences de ports](#)
- [Connexion à votre passerelle](#)
- [Présentation des ressources et ID de ressource Storage Gateway](#)
- [Tagging Storage Gateway](#)
- [Utilisation de composants open source pour AWS Storage Gateway](#)
- [Quotas](#)
- [Utilisation des classes de stockage](#)

Configuration de l'hôte

Rubriques

- [Configuration de VMware for Storage Gateway](#)
- [Synchronisation de l'heure de l'ordinateur virtuel de la passerelle](#)
- [Déploiement d'une passerelle de fichiers sur un hôte Amazon EC2](#)

Configuration de VMware for Storage Gateway

Lorsque vous configurez VMware for Storage Gateway, veillez à synchroniser l'heure de votre machine virtuelle avec l'heure de votre hôte, configurez la VM pour qu'elle utilise des contrôleurs de disque de paravirtualisation lors du provisionnement du stockage et fournissez une protection contre les défaillances dans la couche d'infrastructure prenant en charge une VM passerelle.

Rubriques

- [Synchronisation de l'heure de l'ordinateur virtuel et de celle de l'hôte](#)
- [Utiliser Storage Gateway avec la haute disponibilité de VMware](#)

Synchronisation de l'heure de l'ordinateur virtuel et de celle de l'hôte

Pour activer correctement la passerelle, vous devez veiller à ce que l'heure de l'ordinateur virtuel soit synchronisée sur l'heure de l'hôte et à ce que l'heure de l'hôte soit définie correctement. Dans cette section, vous commencerez par synchroniser l'heure de l'ordinateur virtuel sur celle de l'hôte. Puis vous vérifierez l'heure de l'hôte et, si nécessaire, vous réglerez l'heure de l'hôte et configurerez l'hôte de façon à synchroniser son temps automatiquement sur un serveur NTP (Network Time Protocol).

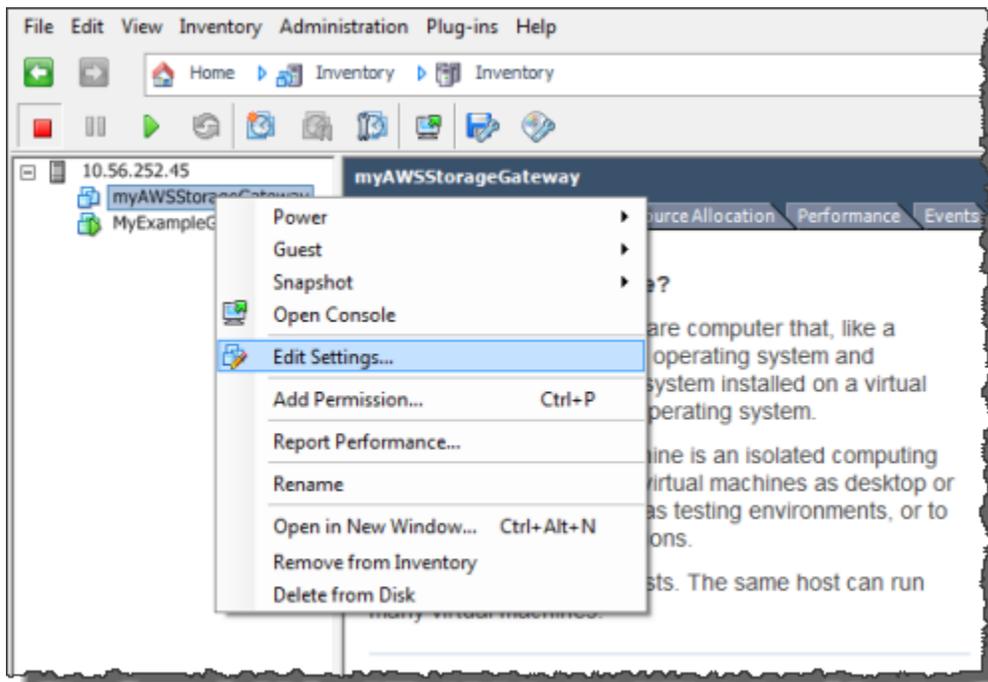
Important

La synchronisation de l'heure de l'ordinateur virtuel sur celle de l'hôte est nécessaire pour activer correctement la passerelle.

Pour synchroniser l'heure de l'ordinateur virtuel sur celle de l'hôte

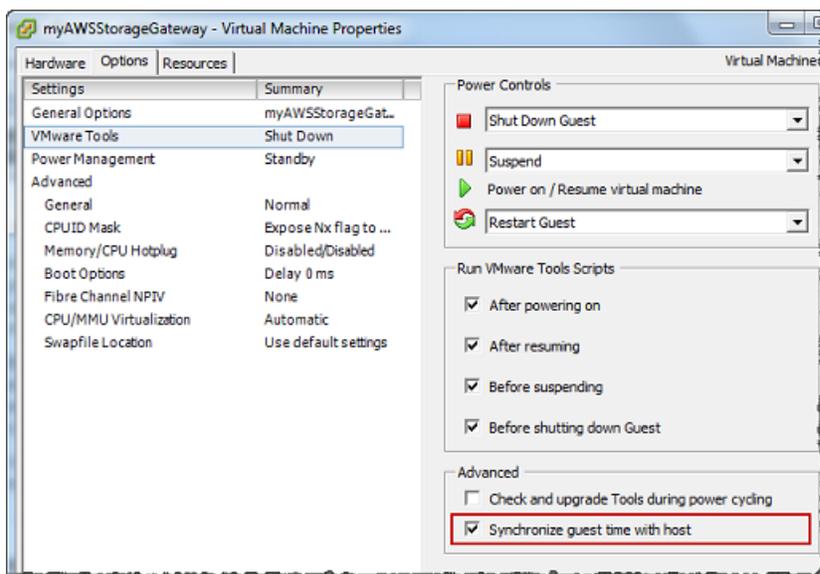
1. Configurez l'heure de votre ordinateur virtuel.
 - a. Dans le client vSphere, ouvrez le menu contextuel (clic droit) pour l'ordinateur virtuel de la passerelle, puis choisissez Modifier les paramètres.

La boîte de dialogue Propriétés de l'ordinateur virtuel s'ouvre.



- b. Choisissez l'onglet Options, puis sélectionnez Outils VMware dans la liste d'options.
- c. Cochez l'option Synchroniser l'heure de l'invité avec l'hôte, puis choisissez OK.

L'ordinateur virtuel synchronise son heure avec l'hôte.

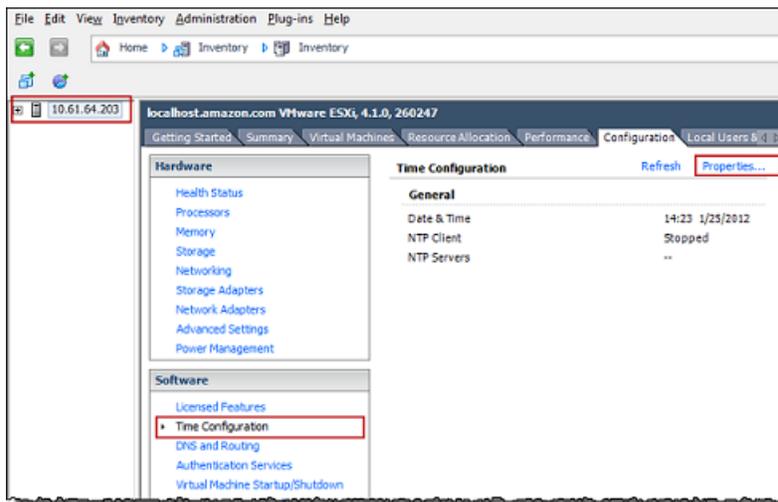


2. Configurez l'heure de l'hôte.

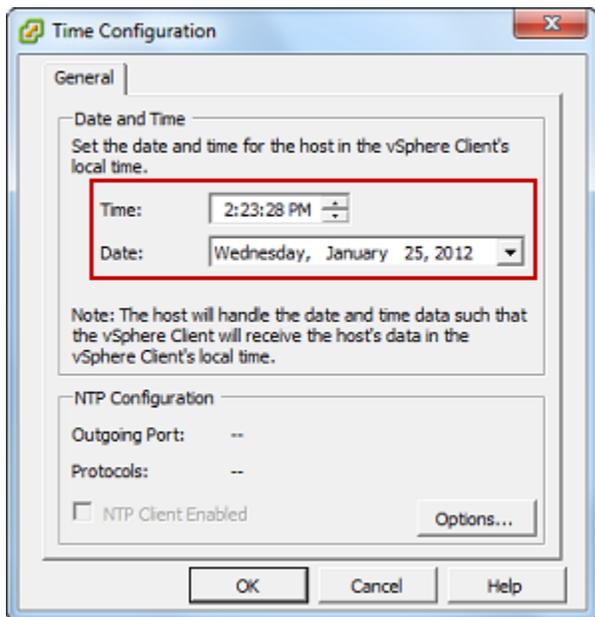
Il est important de s'assurer que l'horloge de l'hôte est réglée sur la bonne heure. Si vous n'avez pas configuré votre horloge hôte, effectuez les opérations suivantes pour la définir et la synchroniser avec un serveur NTP.

- a. Dans le client VMware vSphere, sélectionnez le nœud d'hôte vSphere dans le volet de gauche, puis choisissez l'onglet Configuration.
- b. Sélectionnez Configuration de l'heure dans le volet Logiciels, puis choisissez le lien Propriétés.

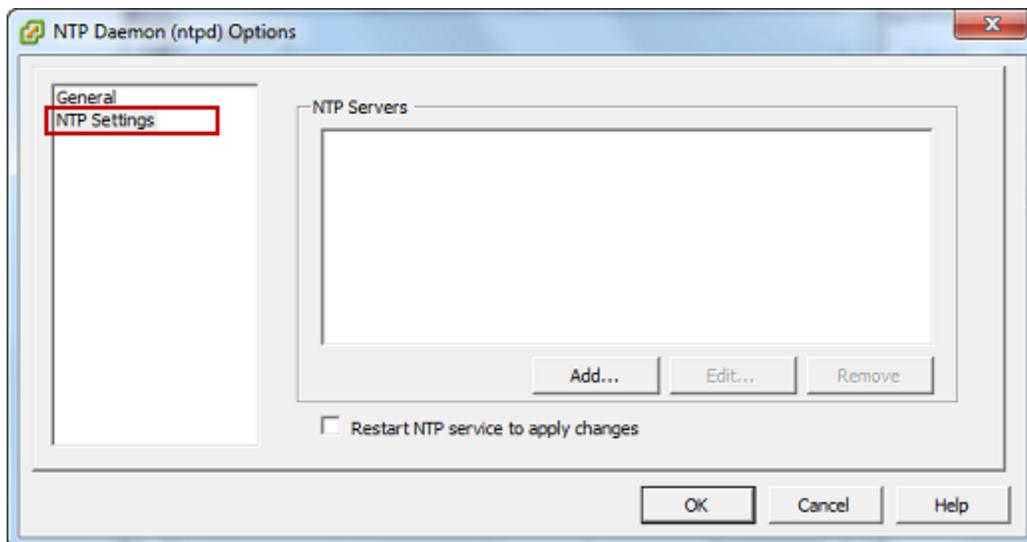
La boîte de dialogue Configuration de l'heure s'affiche.



- c. Dans le volet Date et heure, définissez la date et l'heure.



- d. Configurez l'hôte afin de synchroniser son heure automatiquement sur un serveur NTP.
 - i. Choisissez Options dans la boîte de dialogue Configuration de l'heure puis, dans la boîte de dialogue Options NTP Daemon (ntpd), choisissez Paramètres NTP dans le volet de gauche.



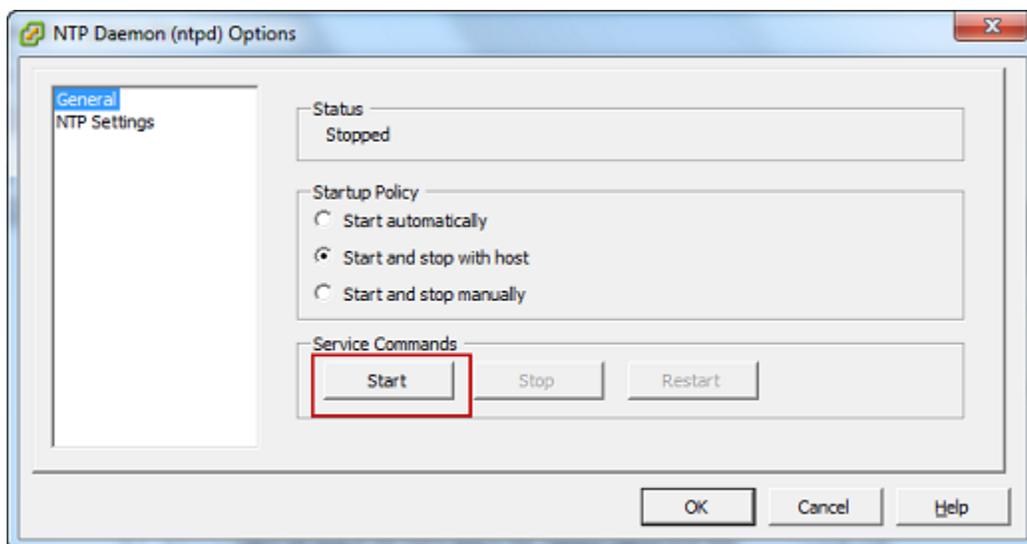
- ii. Choisissez Ajouter pour ajouter un serveur NTP.
 - iii. Dans la boîte de dialogue Ajouter un serveur NTP, tapez l'adresse IP ou le nom de domaine complet d'un serveur NTP, puis choisissez OK.

Vous pouvez utiliser `pool.ntp.org` comme illustré dans l'exemple suivant.



- iv. Dans la boîte de dialogue Options NTP Daemon (ntpd), choisissez Général dans le volet de gauche.
- v. Dans le volet Commandes de service, choisissez Démarrer pour lancer le service.

Notez que si vous modifiez cette référence de serveur NTP ou si vous en ajoutez une autre par la suite, vous devrez redémarrer le service pour utiliser le nouveau serveur.



- e. Choisissez OK pour fermer la boîte de dialogue Options Daemon NTP (ntpd).
- f. Choisissez OK pour fermer la boîte de dialogue Configuration de l'heure.

Utiliser Storage Gateway avec la haute disponibilité de VMware

La haute disponibilité de VMware est un composant de vSphere qui peut fournir une protection contre les défaillances dans la couche de l'infrastructure qui prend en charge un ordinateur virtuel de passerelle. La disponibilité élevée de VMware effectue cette opération à l'aide de plusieurs hôtes configurés comme cluster pour que, si un hôte qui exécute un ordinateur virtuel de passerelle échoue, cet ordinateur virtuel de passerelle puisse être redémarré automatiquement sur un autre hôte au sein du cluster. Pour plus d'informations sur VMware HA, consultez [VMware HA : Concepts et bonnes pratiques](#) sur le site Web de VMware.

Pour utiliser Storage Gateway avec VMware HA, nous vous recommandons de procéder comme suit :

- Déployez VMware ESX .ovapackage téléchargeable contenant la machine virtuelle Storage Gateway sur un seul hôte du cluster.
- Lors du déploiement du package .ova, sélectionnez une banque de données qui ne soit pas locale pour un hôte. Utilisez plutôt une banque de données accessible à tous les hôtes du cluster. Si vous sélectionnez une banque de données locale pour un hôte et que ce dernier connaît une défaillance, la source de données risque de ne pas être accessible à d'autres hôtes du cluster et il est possible que le basculement vers un autre hôte échoue.
- Avec les clusters, si vous déployez le package .ova sur le cluster, sélectionnez un hôte lorsque vous êtes invité à le faire. Vous pouvez aussi déployer directement sur l'hôte d'un cluster.

Synchronisation de l'heure de l'ordinateur virtuel de la passerelle

Pour une passerelle déployée sur VMware ESXi, la définition de l'heure de l'hôte de l'hyperviseur et la synchronisation de l'heure de l'ordinateur virtuel sur l'hôte suffisent pour éviter la dérive de l'heure. Pour plus d'informations, consultez [Synchronisation de l'heure de l'ordinateur virtuel et de celle de l'hôte](#). Pour une passerelle déployée sur Microsoft Hyper-V, vérifiez régulièrement l'heure de l'ordinateur virtuel à l'aide de la procédure décrite ci-après.

Pour afficher et synchroniser l'heure de la machine virtuelle de la passerelle de l'hyperviseur sur un serveur NTP

1. Connectez-vous à la console locale de la passerelle :
 - Pour plus d'informations sur la journalisation dans la console locale VMware ESXi, consultez [Accès à la console locale de la passerelle avec VMware ESXi](#).
 - Pour plus d'informations sur la journalisation dans la console locale Microsoft Hyper-V, consultez [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#).
 - Pour plus d'informations sur la connexion à la console locale pour KVM Linux, consultez [Accès à la console locale de la passerelle avec Linux KVM](#).
2. Dans la page Configuration Storage Gateway menu principal, entrez 4 pour Gestion du temps du système.

```
AWS Storage Gateway Configuration
#####
## Currently connected network adapters:
##
## eth0: 10.0.0.45
#####

1: SOCKS Proxy Configuration
2: Network Configuration
3: Test Network Connectivity
4: System Time Management
5: Gateway Console
6: View System Resource Check (0 Errors)

0: Stop AWS Storage Gateway

Press "x" to exit session

Enter command: _
```

3. Dans le menu System Time Management (Gestion de l'heure système), entrez **1** pour View and Synchronize System Time (Afficher et synchroniser l'heure système).

```
System Time Management

1: View and Synchronize System Time

Press "x" to exit

Enter command: _
```

4. Si le résultat indique que vous devez synchroniser l'heure de l'ordinateur virtuel sur l'heure du protocole NTP, entrez **y**. Sinon, entrez **n**.

Si vous entrez **y** pour synchroniser, la synchronisation peut prendre quelques instants.

La capture d'écran suivante présente un ordinateur virtuel qui ne requiert pas la synchronisation de l'heure.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 0.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

La capture d'écran suivante présente un ordinateur virtuel qui requiert la synchronisation de l'heure.

```
System Time Management
1: View and Synchronize System Time
Press "x" to exit
Enter command: 1
Current System Time: Sat Aug 22 00:33:41 UTC 2015
Determining current NTP time (this may take a few seconds ...)
Your Storage Gateway VM system time differs from NTP time
by 61.217617 seconds
A sync is recommended if the time differs by more than 60 seconds
Do you want to sync Storage Gateway VM system time with
NTP time? [y/n]: _
```

Déploiement d'une passerelle de fichiers sur un hôte Amazon EC2

Vous pouvez déployer et activer une passerelle de fichiers sur une instance Amazon Elastic Compute Cloud (Amazon EC2). L'AMI (Amazon Machine Image) de passerelle de fichiers est disponible en tant qu'AMI de la communauté.

Pour déployer une passerelle sur une instance Amazon EC2

1. Sur la page Sélectionner la plateforme hôte, choisissez Amazon EC2.
2. Choisissez Lancer l'instance pour lancer une AMI EC2 de passerelle de stockage. Vous êtes redirigé vers la console Amazon EC2 où vous pouvez choisir un type d'instance.
3. Dans la pageÉtape 2 : Choisir un type d'instance, choisissez la configuration matérielle de votre instance. Storage Gateway est pris en charge sur les types d'instances qui répondent à certaines exigences minimales. Nous vous recommandons de commencer avec le type d'instance m4.xlarge qui répond aux exigences minimales pour que votre passerelle fonctionne correctement. Pour plus d'informations, consultez [Exigences en matière de matériel pour les machines virtuelles sur site](#).

Vous pouvez redimensionner votre instance après le lancement si nécessaire. Pour de plus amples informations, veuillez consulter[Redimensionnement de l'instance](#) dans le Manuel de l'utilisateur Amazon EC2 pour les instances Linux.

Note

Certains types d'instance, en particulier EC2 i3, utilisent des disques SSD NVMe. Cela peut entraîner des problèmes lorsque vous démarrez ou arrêtez une passerelle de fichiers. Par exemple, vous pouvez perdre des données du cache. Surveillez leCachePercentDirtyMétrique Amazon CloudWatch, et démarrez ou arrêtez votre système uniquement lorsque que le paramètre a la valeur0. Pour en savoir plus sur la surveillance des métriques pour votre passerelle, consultez[Métriques et dimensions Storage Gateway](#) dans la documentation CloudWatch. Pour plus d'informations sur les exigences des types d'instances Amazon EC2, consultez[the section called "Configuration requise pour les types d'instances Amazon EC2"](#).

4. Choisissez Next (Suivant) Configurer les détails d'instance.
5. Dans la pageÉtape 3 : Configurer les détails d'instance, choisissez une valeur pourAttribuer automatiquement l'adresse IP publique. Si votre instance doit être accessible depuis l'Internet public, vérifiez que le champ Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique) est défini sur Enable (Activer). Si votre instance ne doit pas être accessible depuis Internet, définissez Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique) sur Disable (Désactiver).
6. PourRôle IAM, choisissez leAWS Identity and Access Management(IAM) que vous voulez utiliser pour votre passerelle.

7. Choisissez Next (Suivant) Add Storage.
8. Dans la pageÉtape 4 : Add Storage, choisissezAjout d'un nouveau volumepour ajouter du stockage à votre instance de passerelle de fichiers. Vous avez besoin d'au moins un volume Amazon EBS pour configurer pour le stockage de cache.

Tailles de disques recommandées : Cache (minimum) 150 GiB et cache (maximum) 64 TiB

9. Dans la pageÉtape 5 : Ajouter des balises, vous pouvez ajouter une balise facultative à votre instance. Ensuite, sélectionnez Next (Suivant). Configurer le groupe de sécurité.
10. Dans la pageÉtape 6 : Configurer le groupe de sécurité, ajoutez des règles de pare-feu pour qu'un trafic spécifique accède à votre instance. Vous pouvez créer un nouveau groupe de sécurité ou sélectionner un groupe de sécurité existant.

 Important

En plus des ports d'accès d'activation Storage Gateway et Secure Shell (SSH), les clients NFS ont besoin d'accéder à des ports supplémentaires. Pour plus d'informations, consultez [Exigences pour le réseau et le pare-feu](#).

11. Choisissez Vérifier et lancer pour vérifier votre configuration.
12. Dans la pageÉtape 7 : Examiner le lancement d'instance, choisissezLancement d'.
13. Dans la boîte de dialogue Sélectionner une paire de clés existante ou créer une nouvelle paire de clés, choisissez Choisir une paire de clés existante, puis sélectionnez la paire de clés créée lors de la configuration. Lorsque vous êtes prêt, cochez la case de confirmation, puis sélectionnez Lancer les instances.

Une page de confirmation vous indique que votre instance est en cours de lancement.

14. Sélectionnez View Instances pour fermer la page de confirmation et revenir à la console. Sur l'écran Instances, vous pouvez afficher le statut de votre instance. Il suffit de peu de temps pour lancer une instance. Lorsque vous lancez une instance, son état initial est pending. Une fois que l'instance a démarré, son état devient running, et elle reçoit un nom DNS public.
15. Sélectionnez votre instance, notez l'adresse IP publique dans leDescriptionet revenez à la baliseConnexion àAWSdans la console Storage Gateway pour poursuivre la configuration de votre passerelle.

Vous pouvez déterminer l'ID d'AMI à utiliser pour lancer une passerelle de fichiers à l'aide de la console Storage Gateway ou en interrogeant la passerelle de fichiers. AWS Systems Manager magasin de paramètres.

Pour déterminer l'ID d'AMI

1. Connectez-vous à la console AWS Management Console et ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Choisissez Create Gateway (Créer une passerelle), File Gateway (Passerelle de fichiers), puis Next (Suivant).
3. Sur la page Choisir une plateforme hôte, sélectionnez Amazon EC2.
4. Choisissez Lancer l'instance pour lancer une AMI Storage Gateway EC2. Vous êtes redirigé vers la page de l'AMI de la communauté EC2, où vous pouvez voir l'ID d'AMI pour votre AWS Région dans l'URL.

Sinon, vous pouvez interroger le stockage de paramètres Systems Manager. Vous pouvez utiliser le plugin AWS CLI ou l'API Storage Gateway pour interroger le paramètre public Systems Manager sous l'espace de noms `/aws/service/storagegateway/ami/FILE_S3/latest`. Par exemple, l'utilisation de la commande suivante de l'interface de ligne de commande renvoie l'ID d'AMI actuelle dans l'interface de ligne de commande actuelle. AWS Région .

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/FILE_S3/latest
```

La commande de l'interface de ligne de commande renvoie un résultat semblable à ce qui suit :

```
{
  "Parameter": {
    "Type": "String",
    "LastModifiedDate": 1561054105.083,
    "Version": 4,
    "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/FILE_S3/latest",
    "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
    "Value": "ami-123c45dd67d891000"
  }
}
```

Obtention d'une clé d'activation pour votre passerelle

Pour obtenir une clé d'activation pour votre passerelle, vous effectuez une demande web à l'ordinateur virtuel de la passerelle, qui renvoie une redirection contenant la clé d'activation. Cette clé d'activation est transmise en tant que paramètre à l'action d'API `ActivateGateway` pour spécifier la configuration de votre passerelle. Pour de plus amples informations, veuillez consulter [ActivateGateway](#) dans le Références de Storage Gateway.

La demande que vous adressez à la machine virtuelle de la passerelle contient le `AWS` Région dans laquelle l'activation a lieu. L'URL renvoyée par la redirection dans la réponse contient un paramètre de chaîne de requête appelé `activationkey`. Ce paramètre de chaîne de requête est votre clé d'activation. Le format de la chaîne de requête ressemble à ceci :
`http://gateway_ip_address/?activationRegion=activation_region.`

Rubriques

- [AWS CLI](#)
- [Linux \(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)

AWS CLI

Si vous ne l'avez pas déjà fait, vous devez installer et configurer AWS CLI. Pour ce faire, suivez les instructions du Guide de l'utilisateur AWS Command Line Interface :

- [Installation deAWS Command Line Interface](#)
- [Configuration deAWS Command Line Interface](#)

L'exemple suivant montre comment utiliser le `AWS CLI` pour extraire la réponse HTTP, analyser les en-têtes HTTP et obtenir la clé d'activation.

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \  
grep -i location | \  
grep -i key | \  
cut -d'=' -f2 |\  
cut -d'&' -f1
```

Linux (bash/zsh)

L'exemple suivant vous montre comment utiliser Linux (bash/zsh) pour extraire la réponse HTTP, analyser les en-têtes HTTP et obtenir la clé d'activation.

```
function get-activation-key() {
    local ip_address=$1
    local activation_region=$2
    if [[ -z "$ip_address" || -z "$activation_region" ]]; then
        echo "Usage: get-activation-key ip_address activation_region"
        return 1
    fi
    if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); then
        activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
        echo "$activation_key_param" | cut -f2 -d=
    else
        return 1
    fi
}
```

Microsoft Windows PowerShell

L'exemple suivant montre comment utiliser Microsoft Windows PowerShell pour extraire la réponse HTTP, analyser les en-têtes HTTP et obtenir la clé d'activation.

```
function Get-ActivationKey {
    [CmdletBinding()]
    Param(
        [parameter(Mandatory=$true)][string]$IpAddress,
        [parameter(Mandatory=$true)][string]$ActivationRegion
    )
    PROCESS {
        $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
        if ($request) {
            $activationKeyParam = $request.Headers.Location | Select-String -Pattern
"activationKey=( [A-Z0-9-]+)"
            $activationKeyParam.Matches.Value.Split("=")[1]
        }
    }
}
```

Utilisation d'AWS Direct Connect avec Storage Gateway

AWS Direct Connect lie votre réseau interne au cloud Amazon Web Services. En utilisant AWS Direct Connect avec Storage Gateway, vous pouvez créer une connexion pour une charge de travail à haut débit et fournir une connexion réseau dédiée entre votre passerelle sur site et AWS.

Storage Gateway utilise des points de terminaison publics. Avec un AWS Direct Connect en place, vous pouvez créer une interface virtuelle publique permettant l'acheminement du trafic aux points de terminaison Storage Gateway. L'interface virtuelle publique contourne les fournisseurs de services Internet dans votre chemin d'accès réseau. Le point de terminaison public du service Storage Gateway peut se trouver dans la même AWS Région ou il peut être dans une autre AWS Région.

L'illustration suivante présente un exemple de la façon dont AWS Direct Connect fonctionne avec Storage Gateway.

La procédure suivante suppose que vous avez créé une passerelle opérationnelle.

Pour utiliser AWS Direct Connect avec Storage Gateway

1. Créer et établir un AWS Direct Connect connexion entre votre centre de données sur site et votre point de terminaison Storage Gateway. Pour plus d'informations sur la création d'une connexion, consultez [Démarrer avec AWS Direct Connect](#) dans le AWS Direct Connect Guide de l'utilisateur.
2. Connectez votre appliance Storage Gateway sur site au AWS Direct Connect routeur.
3. Créez une interface virtuelle publique et configurez votre routeur sur site en conséquence. Pour de plus amples informations, veuillez consulter [Création d'une interface virtuelle](#) dans le AWS Direct Connect Guide de l'utilisateur.

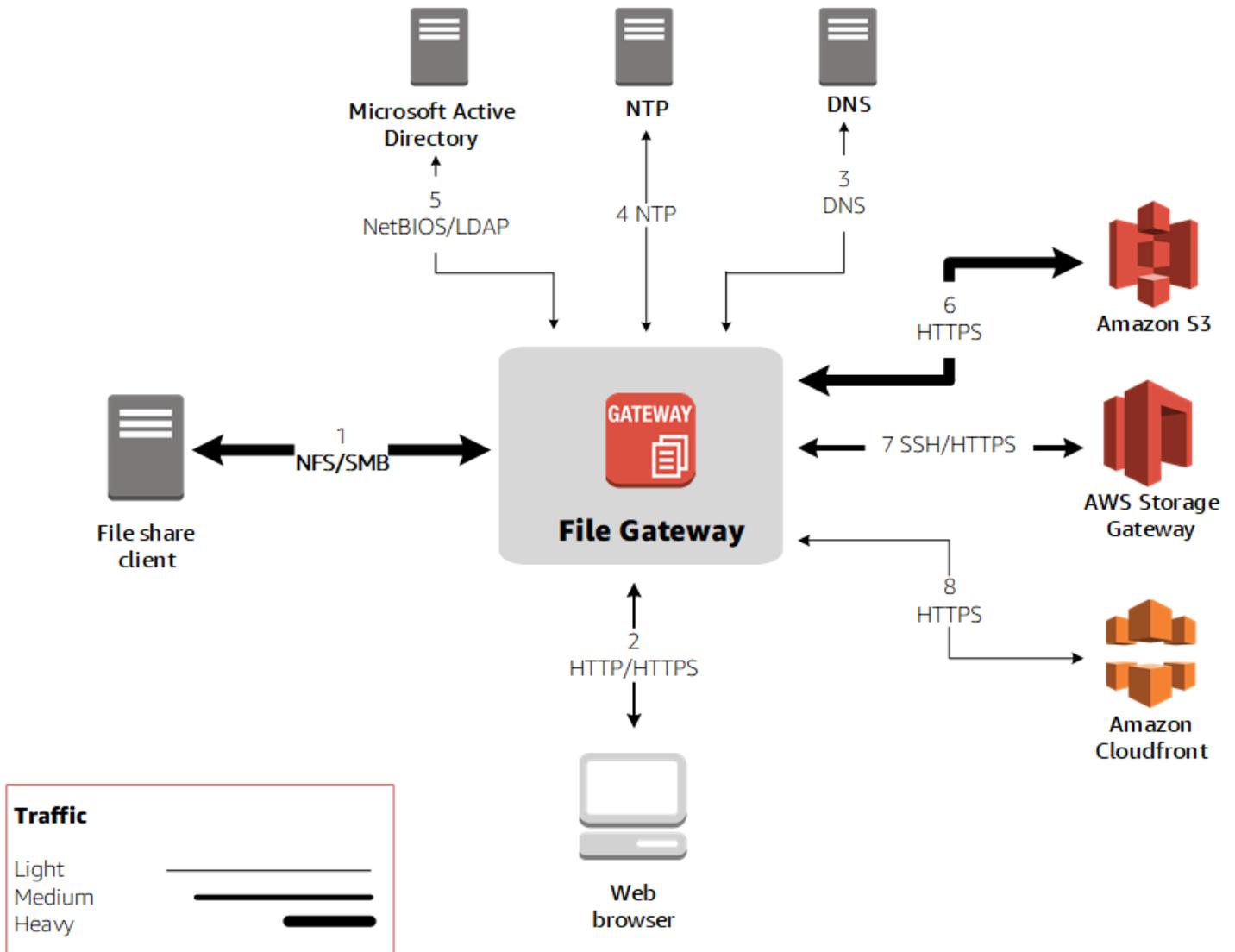
Pour plus de détails sur AWS Direct Connect, voir [Présentation d'AWS Direct Connect?](#) dans le AWS Direct Connect Guide de l'utilisateur.

Exigences de ports

Storage Gateway a besoin des ports suivants pour fonctionner efficacement. Certains ports sont communs à tous les types de passerelle et sont requis par toutes les types de passerelle. Les autres ports sont requis par des types de passerelle spécifiques. Dans cette section, vous trouverez une illustration des ports requis et une liste des ports nécessaires pour chaque type de passerelle.

Passerelles de fichiers

L'illustration suivante montre les ports à ouvrir pour les passerelles de fichiers.



Les ports suivants sont communs à tous les types de passerelles et sont requis par tous les types de passerelles.

De	Pour	Protocole	Port	Utilisation
Storage Gateway	Amazon Web Services	TCP (Transmission Control Protocol)	443 (HTTPS)	Pour les communications d'une machine

De	Pour	Protocole	Port	Utilisation
				virtuelle Storage Gateway vers unAWSpoint de terminais on du service. Pour plus d'informa tions sur les points de terminaison de service, consultez Accorder l'accès à AWS Storage Gateway via les pare- feu et les routeurs.

De	Pour	Protocole	Port	Utilisation
Votre navigateur web	Storage Gateway	TCP	80 (HTTP)	<p>Par les systèmes locaux pour obtenir la clé d'activation Storage Gateway. Le port 80 est utilisé uniquement lors de l'activation d'une appliance Storage Gateway.</p> <p>Une machine virtuelle Storage Gateway ne nécessite pas de port 80 pour être accessible publiquement. Le niveau requis de l'accès au port 80 dépend de la configuration de votre réseau. Si vous</p>

De	Pour	Protocole	Port	Utilisation	
				activez votre passerelle à partir de la console de gestion Storage Gateway, l'hôte à partir duquel vous vous connectez à la console doit avoir accès au port 80 de votre passerelle.	
Storage Gateway	Serveur DNS (Domain Name Service)	UDP/UDP (User Datagram Protocol)	53 (DNS)	Pour toute communication entre une machine virtuelle Storage Gateway et le serveur DNS.	

De	Pour	Protocole	Port	Utilisation	
Storage Gateway	Amazon Web Services	TCP	22 (canal de support)	Permet à Amazon Web Services Support d'accéder à votre passerelle pour vous aider à résoudre les problèmes de passerelle. Ce port ne doit pas être ouvert pour que votre passerelle fonctionne normalement, mais il doit l'être pour résoudre les problèmes.	

De	Pour	Protocole	Port	Utilisation
Storage Gateway	Serveur NTP (Network Time Protocol)	UDP	123 (NTP)	<p>Utilisé par les systèmes locaux pour synchroniser l'heure de l'ordinateur virtuel et celle de l'hôte. Une machine virtuelle Storage Gateway est configuré e pour utiliser les serveurs NTP suivants :</p> <ul style="list-style-type: none">• 0.amazon.pool.ntp.org• 1.amazon.pool.ntp.org• 2.amazon.pool.ntp.org• 3.amazon.pool.ntp.org

De	Pour	Protocole	Port	Utilisation
Appliance matérielle Storage Gateway	Proxy HTTP (Hypertext Transfer Protocol)	TCP	8080 (HTTP)	Requise brièvement pour activation.

Le tableau suivant répertorie les ports requis qui doivent être ouverts pour une passerelle de fichiers utilisant le protocole NFS (Network File System) ou SMB (Server Message Block). Ces règles des ports font partie de la définition de votre groupe de sécurité.

Rè	Élément de réseau	Type de partage de fichiers	Protocole	Port	Entra	Sortan	Obliga re ?	Remarques
1	Client de partage de fichiers	NFS	Données TCP/UDP	111	✓	✓	✓	Transfert de données de partage de fichiers (pour NFS uniquement)
			NFS TCP/UDP	2049	✓	✓	✓	Transfert de données de partage de fichiers (pour NFS uniquement)
			NFSv3 TCP/UDP	2004	✓	✓	✓	Transfert de données de partage de fichiers (pour NFS uniquement)
		SMB	SMBv2 TCP/UDP	139	✓	✓	✓	Service de session de transfert de données

Rè	Élément de réseau	Type de partage de fichiers	Protocole	Port	Entra	Sortan	Obliga re ?	Remarques
								de partage de fichiers (pour SMB uniquement) ; remplace les ports 137 à 139 pour Microsoft Windows NT et version ultérieure
			SMBv3 TCP/UDP	445	✓	✓	✓	Service de session de transfert de données de partage de fichiers (pour SMB uniquement) ; remplace les ports 137 à 139 pour Microsoft Windows NT et version ultérieure
2	Navigateur Web	NFS et SMB	HTTP TCP	80	✓	✓	✓	Amazon Web Services (activation uniquement)
			HTTPS TCP	443	✓	✓	✓	Amazon Web Services (toutes autres opérations)
3	DNS	NFS et SMB	DNS TCP/UDP	53	✓	✓	✓	Résolution du nom d'adresse IP

Rè	Élément de réseau	Type de partage de fichiers	Protocole	Port	Entra	Sortan	Obliga re ?	Remarques
4	NTP	NFS et SMB	NTP UDP	123	✓	✓	✓	Service de synchronisation du temps
5	Microsoft Active	SMB	NetBIOS UDP	137	✓	✓	✓	Service de nom (non utilisé pour NFS)
			NetBIOS UDP	138	✓	✓	✓	Service de datagramme
			LDAP TCP	389	✓	✓		DSA (Directory System Agent) ; connexion client
			LDAPS TCP	636	✓	✓		LDAPS : LDAP (Lightweight Directory Access Protocol) sur SSL (Secure Socket Layer)
6	Amazon S3	NFS et SMB	Données HTTPS	443	✓	✓	✓	Transfert de données de stockage
7	Storage Gateway	NFS et SMB	SSH TCP	22	✓	✓	✓	canal de support
			HTTPS TCP	443	✓	✓	✓	Contrôle de gestion
8	Amazon CloudFront	NFS et SMB	HTTPS TCP	443	✓	✓	✓	Pour activation

Connexion à votre passerelle

Une fois que vous avez choisi un hôte et déployé votre machine virtuelle passerelle, vous devez connecter et activer votre passerelle. Pour cela, vous avez besoin de l'adresse IP de votre machine virtuelle passerelle. Vous obtenez l'adresse IP auprès de la console locale de votre passerelle. Vous vous connectez à la console locale et vous obtenez l'adresse IP dans le haut de la page de la console.

Pour les passerelles déployées sur site, vous pouvez également obtenir l'adresse IP de votre hyperviseur. Pour les passerelles Amazon EC2, vous pouvez également obtenir l'adresse IP de votre instance Amazon EC2 auprès de la console de gestion Amazon EC2. Pour savoir comment obtenir l'adresse IP de votre passerelle, consultez l'un des sites suivants :

- Hôte VMware : [Accès à la console locale de la passerelle avec VMware ESXi](#)
- Hôte HyperV : [Accéder à la console locale de passerelle avec Microsoft Hyper-V](#)
- Hôte KVM (machine virtuelle basée sur le noyau Linux) : [Accès à la console locale de la passerelle avec Linux KVM](#)
- Hôte EC2 : [Obtention d'une adresse IP auprès d'un hôte Amazon EC2](#)

Lorsque vous localisez l'adresse IP, prenez-en note. Retournez ensuite à la console Storage Gateway et tapez l'adresse IP dans la console.

Obtention d'une adresse IP auprès d'un hôte Amazon EC2

Pour obtenir l'adresse IP de l'instance Amazon EC2 sur laquelle votre passerelle est déployée, connectez-vous à la console locale de l'instance EC2. Obtenez ensuite l'adresse IP en haut de la page de la console. Pour obtenir des instructions, consultez .

Vous pouvez également obtenir l'adresse IP auprès de la console de gestion Amazon EC2. Nous vous recommandons d'utiliser l'adresse IP publique pour l'activation. Pour obtenir l'adresse IP publique, utilisez la procédure 1. Si vous décidez d'utiliser plutôt l'adresse IP Elastic, utilisez la procédure 2.

Procédure 1 : Pour vous connecter à votre passerelle en utilisant l'adresse IP publique

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis sélectionnez l'instance EC2 sur laquelle votre passerelle est déployée.

3. Choisissez l'onglet Description en bas, puis notez l'adresse IP publique. Vous utilisez cette adresse IP pour vous connecter à la passerelle. Retournez à la console Storage Gateway et saisissez l'adresse IP.

Si vous voulez utiliser l'adresse IP Elastic pour l'activation, utilisez la procédure suivante.

Procédure 2 : Pour vous connecter à votre passerelle en utilisant l'adresse IP Elastic

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Instances, puis sélectionnez l'instance EC2 sur laquelle votre passerelle est déployée.
3. Choisissez l'onglet Description en bas, puis notez la valeur Adresses IP Elastic. Vous utilisez cette adresse IP Elastic pour vous connecter à la passerelle. Retournez à la console Storage Gateway et saisissez l'adresse IP Elastic.
4. Une fois votre passerelle activée, choisissez-la, puis cliquez sur l'onglet Appareils VTL dans le volet inférieur.
5. Obtenez les noms de tous vos appareils VTL.
6. Pour chaque cible, exécutez la commande suivante pour configurer la cible.

```
iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
```

7. Pour chaque cible, exécutez la commande suivante pour vous connecter.

```
iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
```

Votre passerelle est maintenant connectée avec l'adresse IP Elastic de l'instance EC2.

Présentation des ressources et ID de ressource Storage Gateway

Dans Storage Gateway, la ressource principale est passerelle mais les autres types de ressources sont les suivants : volume, bande virtuelle, Cible iSCSI, et appareil VTL. Ceux-ci sont appelés des sous-ressources, qui n'existent pas tant qu'elles n'ont pas été associées à une passerelle.

Ces ressources et sous-ressources ont des noms Amazon Resource Names (ARNs) uniques associés, comme cela est illustré dans le tableau suivant.

Type de ressource	Format ARN
ARN de passerelle	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
ARN de partage de fichiers	arn:aws:storagegateway: <i>region:account-id</i> :share/ <i>share-id</i>
Volume ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /volume/ <i>volume-id</i>
Bande ARN	arn:aws:storagegateway: <i>region:account-id</i> :tape/ <i>tapebarcode</i>
Cible ARN (cible iSCSI)	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSITarget</i>
ARN du dispositif VTL	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /device/ <i>vtldevice</i>

Storage Gateway prend également en charge l'utilisation des instances EC2, des volumes EBS et des instantanés. Ces ressources sont des ressources Amazon EC2 utilisées dans Storage Gateway.

Utilisation des ID de ressource

Lorsque vous créez une ressource, Storage Gateway lui attribue un ID de ressource unique. Cet ID de ressource fait partie de la ressource ARN. Un ID de ressource est constitué d'un identificateur de ressource suivi d'un tiret et d'une combinaison unique de huit lettres et chiffres. Par exemple, un ID de passerelle a le format `sgw-12A3456B`, `sgw` correspondant à l'identificateur de ressource pour les passerelles. Un ID de volume a le format `vol-3344CCDD`, `vol` correspondant à l'identificateur de ressource pour les volumes.

Pour les bandes virtuelles, vous pouvez ajouter un préfixe comportant jusqu'à quatre caractères à l'ID du code à barres pour vous aider à organiser les bandes.

Les ID de ressource Storage Gateway sont en majuscules. Toutefois, lorsque vous utilisez ces ID de ressource avec l'API Amazon EC2, Amazon EC2 attend des ID de ressource en minuscules. Vous devez modifier votre ID de ressource et utiliser des minuscules afin de pouvoir vous en servir avec l'API EC2. Par exemple, dans Storage Gateway, l'ID d'un volume peut être `vo1-1122AABB`. Lorsque vous utilisez cet ID avec l'API EC2, vous devez le remplacer par `vo1-1122aabb`. Sinon, l'API EC2 ne peut pas se comporter comme prévu.

Important

Les ID des volumes Storage Gateway et des instantanés Amazon EBS créés à partir de volumes de la passerelle passent à un format plus long. À partir de décembre 2016, tous les nouveaux volumes et instantanés seront créés avec une chaîne de 17 caractères. À compter d'avril 2016, vous serez en mesure d'utiliser ces ID plus longs afin de pouvoir tester les systèmes avec le nouveau format. Pour plus d'informations, consultez [ID de ressource EC2 et EBS plus longs](#).

Par exemple, un ARN de volume avec le format d'ID volume plus long ressemble à ceci :
`arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vo1-1122AABBCCDDEEFFG`.

Un ID d'instantané avec le format d'ID plus long ressemble à ceci :`snap-78e226633445566ee`.

Pour de plus amples informations, veuillez consulter [Annonce : Accès direct — Des ID de volume et d'instantané Storage Gateway plus longs à partir de 2016](#).

Tagging Storage Gateway

Dans Storage Gateway, vous pouvez utiliser des balises pour gérer vos ressources. Les balises vous permettent d'ajouter des métadonnées à vos ressources et de catégoriser vos ressources pour simplifier leur gestion. Chaque balise est composée d'une paire clé-valeur que vous définissez. Vous pouvez ajouter des balises aux passerelles, volumes et bandes virtuelles. Vous pouvez rechercher et filtrer ces ressources en fonction des balises que vous ajoutez.

Par exemple, vous pouvez utiliser les balises pour identifier les ressources Storage Gateway utilisées par chaque service de votre organisation. Vous pouvez baliser les passerelles et les volumes utilisés par votre service comptable de la façon suivante : `key=department` et `value=accounting`. Vous pouvez ensuite filtrer avec cette balise pour identifier toutes les passerelles et tous les volumes

utilisés par votre service comptable et utiliser les informations pour déterminer le coût. Pour plus d'informations, consultez [Utilisation des balises de répartition des coûts](#) et [Utilisation de Tag Editor](#).

Si vous archivez une bande virtuelle associée à des balises, cette bande conserve ses balises dans l'archive. De même, si vous extrayez une bande de l'archive pour la transférer sur une autre passerelle, les balises sont conservées dans la nouvelle passerelle.

Pour la passerelle de fichiers, vous pouvez utiliser des balises afin de contrôler l'accès aux ressources. Pour plus d'informations sur la procédure à utiliser, consultez [Utilisation de balises pour contrôler l'accès à votre passerelle et à vos ressources](#).

Les balises n'ont pas de signification sémantique mais sont plutôt interprétées comme des chaînes de caractères.

Les restrictions suivantes s'appliquent aux balises :

- Les clés et valeurs de balise sont sensibles à la casse.
- Le nombre maximum de balises pour chaque ressource est de 50.
- Les clés de balise ne peuvent pas commencer par `aws :`. Ce préfixe est réservé pour l'utilisation de AWS.
- Les caractères valides pour la propriété de clé sont les lettres UTF-8, les chiffres, les espaces et caractères spéciaux `+ - = . _ : /` et `@`.

Utilisation des balises

Vous pouvez utiliser des balises à l'aide de la console Storage Gateway, de l'API Storage Gateway ou de [l'interface de ligne de commande \(CLI\) Storage Gateway](#). Les procédures suivantes vous montrent comment ajouter, modifier et supprimer une balise sur la console.

Pour ajouter une balise

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Dans le volet de navigation, sélectionnez la ressource à laquelle vous souhaitez ajouter une balise.

Par exemple, pour associer une balise à une passerelle, choisissez Passerelles, puis sélectionnez la passerelle à laquelle vous souhaitez ajouter une balise dans la liste de passerelles.

3. Choisissez Balises, puis sélectionnez Ajouter/Modifier des balises.
4. Dans la boîte de dialogue Ajouter/Modifier des balises, choisissez Créer une balise.
5. Tapez une clé pour Clé et une valeur pour Valeur. Par exemple, vous pouvez taper **Department** pour la clé et **Accounting** pour la valeur.

 Note

Vous pouvez laisser la zone Valeur vide.

6. Choisissez Créer une balise pour ajouter des balises. Vous pouvez ajouter plusieurs balises à une ressource.
7. Lorsque vous avez terminé d'ajouter des balises, choisissez Enregistrer.

Pour modifier une balise

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Sélectionnez la ressource dont vous voulez modifier la balise.
3. Sélectionnez Balises pour ouvrir la boîte de dialogue Ajouter/Modifier des balises.
4. Choisissez l'icône de crayon en regard de la balise que vous voulez modifier, puis modifiez la balise.
5. Lorsque vous avez fini de modifier la balise, choisissez Enregistrer.

Pour supprimer une balise

1. Ouvrez la console Storage Gateway sur <https://console.aws.amazon.com/storagegateway/home>.
2. Sélectionnez la ressource dont vous voulez supprimer la balise.
3. Choisissez Balises, puis Ajouter/Modifier des balises pour ouvrir la boîte de dialogue Ajouter/Modifier des balises.
4. Choisissez l'icône X en regard de la balise que vous voulez supprimer, puis sélectionnez Enregistrer.

Voir aussi

[Utilisation de balises pour contrôler l'accès à votre passerelle et à vos ressources](#)

Utilisation de composants open source pour AWS Storage Gateway

Dans cette section, vous trouverez des informations sur les outils et licences tiers dont nous dépendons pour fournir les fonctionnalités Storage Gateway.

Rubriques

- [Composants open source pour Storage Gateway](#)
- [Composants open source pour Amazon S3 File Gateway](#)

Composants open source pour Storage Gateway

Plusieurs outils et licences tiers sont utilisés pour fournir des fonctionnalités pour la passerelle de volume, la passerelle de bande et Amazon S3 File Gateway.

Utilisez les liens suivants pour télécharger le code source pour certains composants de logiciels open source qui sont inclus dans AWS Storage Gateway logiciels :

- Pour les passerelles déployées sur VMware ESXi : [sources.tar](#)
- Pour les passerelles déployées sur Microsoft Hyper-V : [sources_hyperv.tar](#)
- Pour les passerelles déployées sur un hôte KVM (machine virtuelle basée sur le noyau Linux) : [sources_KVM.tar](#)

Ce produit comprend un logiciel développé par OpenSSL Project pour une utilisation dans OpenSSL Toolkit (<http://www.openssl.org/>). Pour connaître les licences pertinentes pour tous les outils tiers dépendants, veuillez consulter [Licences tierces](#).

Composants open source pour Amazon S3 File Gateway

Plusieurs outils et licences tiers sont utilisés pour fournir la fonctionnalité Amazon S3 File Gateway (S3 File Gateway).

Utilisez les liens suivants pour télécharger le code source de certains composants de logiciels open source qui sont inclus dans le logiciel S3 File Gateway :

- Pour Amazon S3 File Gateway : [sgw-file-s3-open-source.tgz](#)

Ce produit comprend un logiciel développé par OpenSSL Project pour une utilisation dans OpenSSL Toolkit (<http://www.openssl.org/>). Pour connaître les licences pertinentes pour tous les outils tiers dépendants, veuillez consulter [Licences tierces](#).

Quotas

Quotas pour partages de fichiers

Le tableau suivant répertorie les quotas pour les partages de fichiers.

Description	Passerelle de fichiers
Nombre maximum de partages de fichiers par compartiment Amazon S3. Un partage de fichiers et un compartiment S3 sont liés par un mappage un à un.	1
Nombre maximum de partages de fichiers par passerelle	10
Taille maximale d'un fichier individuel, soit la taille maximale d'un objet individuel dans Amazon S3.	5 To
<div data-bbox="115 1224 792 1587"><p>Note</p><p>Si vous écrivez un fichier d'une taille supérieure à 5 To, vous obtenez un message d'erreur de type « Fichier trop volumineux » et seulement les 5 premiers To du fichier sont chargés.</p></div>	
Longueur de chemin d'accès maximale	1024 bytes
<div data-bbox="115 1703 792 1885"><p>Note</p><p>Les clients ne sont pas autorisés à créer un chemin dépassant cette</p></div>	

Description	Passerelle de fichiers
longueur et cela génère une erreur. Cette limite s'applique aux deux protocoles pris en charge par les passerelles de fichiers : NFS et SMB.	

Tailles de disques locales recommandées pour votre passerelle

Le tableau suivant recommande des tailles pour le stockage du disque local associé à la passerelle déployée.

Type de passerelle	Cache (minimum)	Cache (maximum)	Autres disques locaux requis
Passerelle de fichiers S3	150 GiB	64 Tio	—

Note

Vous pouvez configurer un ou plusieurs disques locaux pour votre cache jusqu'à la capacité maximale.

Lorsque vous ajoutez un cache à une passerelle existante, il est important de créer des disques sur votre hôte (hyperviseur ou instance Amazon EC2). Ne modifiez pas la taille des disques existants si les disques ont été alloués en tant que cache.

Utilisation des classes de stockage

Storage Gateway prend en charge les classes de stockage Amazon S3 standard, Amazon S3 standard — Accès peu fréquent, Amazon S3 unizone — Accès peu fréquent, Amazon S3 Intelligent-Tiering et S3 Glacier. Pour plus d'informations sur les classes de stockage, consultez [Classes de stockage Amazon S3](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.

Rubriques

- [Utilisation de classes de stockage avec une passerelle de fichiers](#)
- [Utilisation de la classe de stockage GLACIER avec une passerelle de fichiers](#)

Utilisation de classes de stockage avec une passerelle de fichiers

Lorsque vous créez ou mettez à jour un partage de fichiers, vous pouvez sélectionner une classe de stockage pour vos objets. Vous pouvez choisir la classe de stockage Amazon S3 standard ou l'une des classes de stockage S3 standard — Accès peu fréquent, S3 unizone — Accès peu fréquent ou S3 Intelligent-Tiering. Les objets stockés dans l'une de ces classes de stockage peuvent être transférés vers GLACIER à l'aide d'une stratégie de cycle de vie.

Classe de stockage Amazon S3	Considérations
Standard	Choisissez Standard pour stocker vos fichiers fréquemment consultés dans plusieurs zones de disponibilité géographiquement séparées les unes des autres. Il s'agit de la classe de stockage par défaut. Consultez Tarification Amazon S3 pour plus d'informations.
S3 Intelligent-Tiering	<p>Choisissez Intelligent-Tiering (Hiérarchisation intelligente) pour optimiser les coûts de stockage en transférant automatiquement les données vers le niveau d'accès de stockage le plus économique.</p> <p>Les objets stockés dans la classe de stockage Intelligent-Tiering (Tiering Intelligent-Tiering) peuvent entraîner des frais supplémentaires liés au remplacement, à la suppression, à la demande ou à la transition d'objets entre classes de stockage dans les 30 jours suivant. La durée de stockage minimale est de 30 jours, et les objets supprimés avant 30 jours sont facturés au prorata des frais de stockage pour les jours restants. Prenez en compte la fréquence de changement de ces objets, la</p>

Classe de stockage Amazon S3	Considérations
	<p>durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les objets inférieurs à 128 Ko ne sont pas éligibles à la hiérarchisation automatique dans la classe de stockage Intelligent-Tiering (Niveau intelligent) Ces objets sont facturés aux tarifs de niveau d'accès fréquent, et des frais de suppression anticipée s'appliquent.</p> <p>S3 Intelligent-Tiering prend désormais en charge un niveau Archive Access et un niveau Deep Archive Access. S3 Intelligent-Tiering déplace automatiquement les objets qui n'ont pas été consultés pendant 90 jours vers le niveau Accès Archive, puis ceux qui n'ont pas été consultés pendant 180 jours, vers le niveau Accès Deep Archive. Chaque fois qu'un objet dans l'un des niveaux d'accès aux archives est restauré, l'objet passe au niveau Accès fréquent en quelques heures et est prêt à être récupéré. Cela crée des erreurs de délai d'expiration pour les utilisateurs ou les applications qui tentent d'accéder à des fichiers via un partage de fichiers si l'objet n'existe que dans l'un des deux niveaux d'archivage. N'utilisez pas les niveaux d'archivage avec S3 Intelligent-Tiering si vos applications accèdent à des fichiers via les partages de fichiers présentés par la passerelle de fichiers.</p> <p>Lorsque des opérations de fichiers qui mettent à jour des métadonnées (telles que le propriétaire, l'horodatage, les autorisations et les ACL) sont effectuées sur des fichiers gérés par la passerelle de fichiers, l'objet existant est</p>

Classe de stockage Amazon S3	Considérations
	<p>supprimé et une nouvelle version de l'objet est créée dans cette classe de stockage Amazon S3. Vous devez valider l'impact des opérations de fichiers sur la création d'objets avant d'utiliser cette classe de stockage en production, car des frais de suppression anticipée s'appliquent. Consultez Tarification Amazon S3 pour plus d'informations.</p>

Classe de stockage Amazon S3	Considérations
S3 standard – Accès peu fréquent	<p>Choisissez Standard-IA (Standard - Accès peu fréquent) pour stocker vos fichiers peu consultés dans plusieurs zones de disponibilité géographiquement séparées les unes des autres.</p> <p>Les objets stockés dans la classe de stockage Standard-IA (Standard - Accès peu fréquent) peuvent entraîner des frais supplémentaires liés au remplacement, à la suppression, à la récupération ou à la transition d'objets entre classes de stockage dans les 30 jours suivant. La durée de stockage est d'au moins 30 jours. Les objets supprimés avant 30 jours sont facturés au prorata des frais de stockage pour les jours restants. Prenez en compte la fréquence de changement de ces objets, la durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les objets de moins de 128 Ko sont facturés pour 128 Ko et des frais de suppression anticipée s'appliquent.</p> <p>Lorsque des opérations de fichiers qui mettent à jour des métadonnées (telles que le propriétaire, l'horodatage, les autorisations et les ACL) sont effectuées sur des fichiers gérés par la passerelle de fichiers, l'objet existant est supprimé et une nouvelle version de l'objet est créée dans cette classe de stockage Amazon S3. Vous devez valider l'impact des opérations de fichiers sur la création d'objets avant d'utiliser cette classe de stockage en production, car des frais de suppression anticipée s'appliquent.</p>

Classe de stockage Amazon S3	Considérations
	Consultez Tarification Amazon S3 pour plus d'informations.

Classe de stockage Amazon S3	Considérations
S3 One Zone-IA	<p>Choisissez One Zone_IA (One Zone_IA) pour stocker vos fichiers peu consultés dans une seule zone de disponibilité.</p> <p>Les objets stockés dans la classe de stockage One Zone-IA (Unizone — Accès peu fréquent) peuvent entraîner des frais supplémentaires liés au remplacement, à la suppression, à la demande, à la récupération ou à la transition d'objets entre classes de stockage dans les 30 jours. La durée de stockage minimale est de 30 jours, et les objets supprimés avant 30 jours sont facturés au prorata des frais de stockage pour les jours restants. Prenez en compte la fréquence de changement de ces objets, la durée pendant laquelle vous prévoyez de les conserver et la fréquence à laquelle vous devez y accéder. Les objets de moins de 128 Ko sont facturés pour 128 Ko et des frais de suppression anticipée s'appliquent.</p> <p>Lorsque des opérations de fichiers qui mettent à jour des métadonnées (telles que le propriétaire, l'horodatage, les autorisations et les ACL) sont effectuées sur des fichiers gérés par la passerelle de fichiers, l'objet existant est supprimé et une nouvelle version de l'objet est créée dans cette classe de stockage Amazon S3. Vous devez valider l'impact des opérations de fichiers sur la création d'objets avant d'utiliser cette classe de stockage en production, car des frais de suppression anticipée s'appliquent. Consultez Tarification Amazon S3 pour plus d'informations.</p>

Bien que vous puissiez écrire des objets directement à partir d'un partage de fichiers vers la classe de stockage S3 standard — Accès fréquent, S3 une zone — Accès peu fréquent ou S3 Intelligent-Tiering, nous vous recommandons d'utiliser une stratégie de cycle de vie pour transférer vos objets au lieu d'écrire directement à partir du partage de fichiers, en particulier si vous prévoyez de mettre à jour ou supprimer le fichier objet dans les 30 jours suivant son archivage. Pour plus d'informations sur la stratégie de cycle de vie, consultez [Gestion du cycle de vie des objets](#).

Utilisation de la classe de stockage GLACIER avec une passerelle de fichiers

Si vous transférez un fichier vers S3 Glacier via des stratégies de cycle de vie Amazon S3 et que ce fichier est visible par les clients de votre partage de fichiers via le cache, vous recevez des erreurs d'E/S lorsque vous mettez à jour le fichier. Nous vous recommandons de configurer CloudWatch Events pour recevoir des notifications lorsque ces erreurs d'E/S se produisent et d'utiliser la notification pour intervenir. Par exemple, vous pouvez intervenir pour restaurer dans Amazon S3 l'objet archivé. Une fois l'objet restauré dans S3, les clients du partage de fichiers peuvent y accéder et le mettre à jour via le partage de fichiers.

Pour plus d'informations sur la restauration d'objets archivés, consultez [Restauration d'objets archivés](#) dans le Manuel de l'utilisateur Amazon Simple Storage Service.

Référence API pour Storage Gateway

Outre la console, vous pouvez utiliser l'API AWS Storage Gateway pour configurer et gérer vos passerelles par programme. Cette section décrit les opérations AWS Storage Gateway, la signature des requêtes pour l'authentification et la gestion des erreurs. Pour plus d'informations sur les régions et points de terminaison disponibles pour Storage Gateway, consultez [AWS Storage Gateway Points de terminaison et quotas](#) dans le [AWS Référence générale](#).

Note

Vous pouvez également utiliser l'AWS Les kits SDK lors du développement d'applications avec Storage Gateway. Le AWS Les kits de développement logiciel SDK pour Java, .NET et PHP enveloppent l'API Storage Gateway sous-jacente, simplifiant vos tâches de programmation. Pour de plus amples informations sur le téléchargement des bibliothèques de kits SDK, veuillez consulter [Exemples de bibliothèques de codes](#).

Rubriques

- [AWS Storage Gateway En-têtes de requête obligatoires](#)
- [Signature des requêtes](#)
- [Réponses d'erreur](#)
- [Actions](#)

AWS Storage Gateway En-têtes de requête obligatoires

Cette section décrit les en-têtes obligatoires que vous devez envoyer avec toutes les requêtes POST à AWS Storage Gateway. Vous incluez les en-têtes HTTP pour identifier les informations clés relatives à la requête, y compris l'opération que vous souhaitez appeler, la date de la requête et les informations correspondant à votre autorisation en tant qu'expéditeur de la requête. Les en-têtes ne sont pas sensibles à la casse et leur ordre n'est pas important.

Les exemples suivants montrent les en-têtes qui sont utilisés dans l'opération [ActivateGateway](#).

```
POST / HTTP/1.1
```

```
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

Voici les en-têtes qui doivent être inclus avec vos requêtes POST à AWS Storage Gateway. Les en-têtes ci-dessous qui commencent par « x-amz » sont des en-têtes spécifiques AWS. Tous les autres en-têtes répertoriés sont des en-têtes courants utilisés dans les transactions HTTP.

En-tête	Description
Authorization	<p>L'en-tête d'autorisation contient plusieurs informations sur la requête qui permettent d'activer AWS Storage Gateway pour déterminer si la requête est une action valide pour le demandeur. Le format de cet en-tête est le suivant (sauts de ligne ajoutés pour faciliter la lecture) :</p> <pre>Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd</i>/<i>region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i></pre> <p>Dans la syntaxe précédente, vous spécifiez <i>YourAccessKey</i>, l'année, le mois et le jour (AAAAMMJJ), la région et la <i>CalculatedSignature</i>. Le format de l'en-tête d'autorisation est déterminé par les exigences du processus de signature V4. Les détails de la signature sont détaillés dans la rubrique Signature des requêtes.</p>
Content-Type	<p>Utiliser <code>application/x-amz-json-1.1</code> comme type de contenu pour toutes les requêtes à AWS Storage Gateway.</p> <pre>Content-Type: application/x-amz-json-1.1</pre>

En-tête	Description
Host	<p>Utilisez l'en-tête de l'hôte pour spécifier laAWS Storage Gatewaypoint de terminaison où vous envoyez votre demande. Par exemple,storagegateway.us-east-2.amazonaws.com est le point de terminaison pour la région USA Est (Ohio). Pour plus d'informations sur les points de terminaison disponibles pourAWS Storage Gateway, voirAWS Storage GatewayPoints de terminaison et quotasdans leAWSRéférence générale.</p> <pre data-bbox="475 617 1507 695">Host: storagegateway. <i>region</i>.amazonaws.com</pre>
x-amz-date	<p>Vous devez fournir l'horodatage dans l'en-tête HTTP Date ou dans l'en-tête AWS x-amz-date . (Certaines bibliothèques client HTTP ne vous permettent pas de définir l'en-tête Date.) Si unx-amz-date L'en-tête est présent, l'AWS Storage Gatewayignore n'importe lequelDateen-tête pendant l'authentification de la demande. Le format x-amz-date doit être de type ISO8601 Basic, au format AAAAMMJJ'T'HHMMSS'Z'. Si les en-têtes Date et x-amz-date sont utilisés, le format de l'en-tête de la date n'a pas besoin d'être de type ISO8601.</p> <pre data-bbox="475 1178 1507 1255">x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>
x-amz-target	<p>Cet en-tête spécifie la version de l'API et l'opération que vous demandez. Les valeurs d'en-tête cibles sont formées en concaténant la version de l'API avec le nom de l'API et ont le format suivant.</p> <pre data-bbox="475 1493 1507 1570">x-amz-target: StorageGateway_ <i>APIversion</i> .<i>operationName</i></pre> <p>LeoperationNameLa valeur (par exemple « ActivateGateway ») se trouve dans la liste des API,Référence API pour Storage Gateway.</p>

Signature des requêtes

Storage Gateway exige que vous authentifiez toutes les requêtes que vous envoyez en signant la demande. Pour signer une demande, vous calculez une signature numérique à l'aide d'une fonction de hachage cryptographique. Un hachage cryptographique est une fonction qui renvoie une valeur de hachage unique basée sur l'entrée. L'entrée de la fonction de hachage contient le texte de la demande et votre clé d'accès secrète. La fonction de hachage renvoie une valeur de hachage que vous incluez dans la demande comme votre signature. La signature fait partie de l'en-tête `Authorization` de votre demande.

Après avoir reçu votre demande, Storage Gateway recalcule la signature en utilisant la même fonction de hachage et la même entrée que celles que vous avez utilisées pour signer la demande. Si la signature obtenue correspond à la signature de la requête, Storage Gateway traite la demande. Sinon, la demande est rejetée.

Storage Gateway permet l'authentification à [AWSSignature Version 4](#). Le processus de calcul d'une signature peut être divisé en trois tâches :

- [Tâche 1 : Créer une demande canonique](#)

Réorganiser votre demande HTTP dans un format canonique. L'utilisation d'une forme canonique est nécessaire, car Storage Gateway utilise le même formulaire canonique lorsqu'il recalcule une signature à comparer à celle que vous avez envoyée.

- [Tâche 2 : Créer une chaîne de connexion](#)

Créez une chaîne que vous utiliserez comme une des valeurs d'entrée pour votre fonction de hachage cryptographique. La chaîne, appelée la chaîne de connexion, est une concaténation du nom de l'algorithme de hachage, de la date de la demande, d'une chaîne d'informations d'identification et de la demande convertie sous forme canonique de la tâche précédente. La chaîne d'informations d'identification elle-même est une concaténation de date, de région et d'informations de service.

- [Tâche 3 : Création d'une signature](#)

Créez une signature pour votre demande à l'aide d'une fonction de hachage cryptographique qui accepte deux chaînes d'entrée : votre chaîne de connexion et une clé dérivée. La clé dérivée est calculée en commençant par votre clé d'accès secrète et en utilisant la chaîne d'informations d'identification pour créer un ensemble de codes d'authentification de message basés sur le hachage (HMAC).

Exemple de calcul de signature

L'exemple suivant vous guide à travers les détails de la création d'une signature pour [ListGateways](#). L'exemple peut être utilisé comme référence pour vérifier votre méthode de calcul de signature. D'autres calculs de référence sont inclus dans le package [Signature Version 4 Test Suite](#) du Glossaire Amazon Web Services.

Dans cet exemple il est supposé que :

- L'horodatage de la demande est « Lun, 10 septembre 2012 00:00:00 GMT ».
- Le point de terminaison est la région USA Est (Ohio).

La syntaxe générale de la requête (y compris le corps JSON) est :

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{ }
```

La forme canonique de la requête calculée pour [Tâche 1 : Créer une demande canonique](#) est :

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

La dernière ligne de la demande canonique est le hachage du corps de la demande. Notez également la troisième ligne vide dans la demande canonique. En effet, il n'y a aucun paramètre de requête pour cette API (ou n'importe quelle API Storage Gateway).

La chaîne à signer pour [Tâche 2 : Créer une chaîne de connexion](#) est :

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

La première ligne de la chaîne à signer est l'algorithme, la deuxième ligne est l'horodatage, la troisième ligne comporte la portée des informations d'identification, et la dernière ligne est un hachage de la requête canonique issue de la tâche 1.

Pour [Tâche 3 : Création d'une signature](#), la clé dérivée peut être représentée sous la forme :

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20120910"), "us-
east-2"), "storagegateway"), "aws4_request")
```

Si la clé d'accès secrète, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, est utilisée, la signature calculée est :

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

L'étape finale consiste à construire l'en-tête `Authorization`. Pour la clé d'accès de la démonstration AKIAIOSFODNN7EXAMPLE, l'en-tête (avec les sauts de ligne ajoutés pour faciliter la lecture) est :

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Réponses d'erreur

Rubriques

- [Exceptions](#)
- [Codes d'erreur d'opération](#)
- [Réponses d'erreur](#)

Cette section fournit des informations de référence sur les erreurs AWS Storage Gateway. Ces erreurs sont représentées par une exception et un code d'erreur opération. Par exemple, l'exception `InvalidSignatureException` est retournée par toute réponse d'API en cas de problème avec la signature de la requête. Toutefois, le code d'erreur d'opération `ActivationKeyInvalid` est retourné uniquement pour l'API [ActivateGateway](#).

En fonction du type d'erreur, Storage Gateway peut retourner uniquement une exception, ou une exception et un code d'erreur opération. Vous trouverez des exemples de réponses d'erreur dans [Réponses d'erreur](#).

Exceptions

Le tableau suivant répertorie les exceptions de l'API AWS Storage Gateway. Lorsqu'une opération AWS Storage Gateway retourne une réponse d'erreur, le corps de la réponse contient une de ces exceptions. Les codes de message `InternalServerError` et `InvalidGatewayRequestException` retournent l'un des codes d'erreur d'opération [Codes d'erreur d'opération](#) qui vous donnent le code d'erreur d'opération spécifique.

Exception	Message	HTTP Status Code
<code>IncompleteSignatureException</code>	La signature spécifiée est incomplète.	400 : Requête erronée
<code>InternalFailure</code>	Le traitement de la requête a échoué en raison d'une erreur inconnue, d'une exception ou d'un échec.	500 Erreur de serveur interne
<code>InternalServerError</code>	Un des messages de code d'erreur d'opération Codes d'erreur d'opération .	500 Erreur de serveur interne
<code>InvalidAction</code>	L'action demandée ou le fonctionnement n'est pas valide.	400 : Requête erronée
<code>InvalidClientTokenId</code>	Le certificat X.509 ou AWS L'ID de clé d'accès fourni n'existe pas dans nos archives.	403 : Interdit

Exception	Message	HTTP Status Code
InvalidGatewayRequestException	Un des messages de code d'erreur d'opération dans Codes d'erreur d'opération .	400 : Requête erronée
InvalidSignatureException	La signature de demande que nous avons calculée ne correspond pas à la signature que vous avez fournie. Vérifiez votre AWS Clé d'accès et méthode de signature.	400 : Requête erronée
MissingAction	Il manque un paramètre d'action ou d'opération dans la requête.	400 : Requête erronée
MissingAuthenticationToken	La requête doit comporter un document valide (enregistré) AWSID de clé d'accès ou un certificat X.509.	403 : Interdit
RequestExpired	La requête a dépassé la date d'expiration ou la date de la requête (l'un ou l'autre avec un remplissage de 15 minutes), ou la date de la requête se produit dans 15 minutes à l'avenir.	400 : Requête erronée
SerializationException	Une erreur s'est produite lors de la sérialisation. Vérifiez que la charge utile JSON est bien formée.	400 : Requête erronée
ServiceUnavailable	La requête a échoué en raison d'une défaillance temporaire du serveur.	503 – Service non disponible
SubscriptionRequiredException	Le AWS L'ID de clé d'accès a besoin d'un abonnement pour le service.	400 : Requête erronée
ThrottlingException	Taux dépassé.	400 : Requête erronée

Exception	Message	HTTP Status Code
UnknownOperationException	Une opération inconnue a été spécifiée. Les opérations valides sont répertoriées dans Opérations dans Storage Gateway .	400 : Requête erronée
UnrecognizedClientException	Le jeton de sécurité inclus dans la demande n'est pas valide.	400 : Requête erronée
ValidationException	La valeur du paramètre d'entrée est inexacte ou hors de portée.	400 : Requête erronée

Codes d'erreur d'opération

Le tableau suivant illustre le mappage entre les codes d'erreur d'opération AWS Storage Gateway et les API qui peuvent retourner les codes. Tous les codes d'erreur d'opération sont renvoyés avec l'une des deux exceptions générales suivantes : `InternalServerError` et `InvalidGatewayRequestException`—décrit dans [Exceptions](#).

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
ActivationKeyExpired	La clé d'activation spécifiée a expiré.	ActivateGateway
ActivationKeyInvalid	La clé d'activation spécifiée n'est pas valide.	ActivateGateway
ActivationKeyNotFound	La clé d'activation spécifiée n'a pas été trouvée.	ActivateGateway

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
BandwidthThrottlescheduleNotFound	La limitation de bande passante spécifiée est introuvable.	DeleteBandwidthRateLimit
CannotExportSnapshot	L'instantané spécifié ne peut pas être exporté.	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	L'initiateur spécifié est introuvable.	DeleteChapCredentials
DiskAlreadyAllocated	Le disque spécifié est déjà attribué.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	Le disque spécifié n'existe pas.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	Le disque spécifié n'est pas aligné avec les Go.	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	La taille du disque spécifiée est supérieure à la taille maximum du volume.	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	La taille de disque spécifiée est inférieure à la taille du volume.	CreateStorediSCSIVolume

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
DuplicateCertificateInfo	Les informations de certificat spécifiées sont en doublon.	ActivateGateway
Conflit de configuration des points de terminaison de l'association de systèmes de fichiers	La configuration du point de terminaison de l'association de systèmes de fichiers existante est en conflit avec la configuration	Système de fichiers associé
Adresse IP d'association de systèmes de fichiers déjà en cours d'utilisation	L'adresse IP du point de terminaison spécifiée est déjà utilisée.	Système de fichiers associé
Adresse IP de l'association du système de fichiers de terminaison manquante	L'adresse IP du point de terminaison de File System Association est manquante.	Système de fichiers associé
Association de systèmes de fichiers introuvable	L'association de système de fichiers spécifiée est introuvable.	Mettre à jour l'association de systèmes de fichiers Dissocier le système de fichiers Décrire les associations de systèmes de fichiers
Système de fichiers introuvable	Le système de fichiers spécifié est introuvable.	Système de fichiers associé

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
GatewayInternalError	Une erreur interne de passerelle est survenue.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
GatewayNotConnected	La passerelle spécifiée n'est pas connectée.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
GatewayNotFound	La passerelle spécifiée est introuvable.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
GatewayProxyNetworkConnectionBusy	La connexion réseau du proxy de la passerelle spécifiée est occupée.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
InternalError	Une erreur interne s'est produite.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
InvalidParameters	La requête spécifiée contient des paramètres non valides.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	La limite de stockage local a été dépassée.	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	Le préfixe LUN spécifié est non valide.	CreateStorediSCSIVolume

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
MaximumVolumeCount Exceeded	Le nombre de volumes maximum a été dépassé.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
NetworkConfigurationChanged	La configuration du réseau de la passerelle a été modifiée.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
NotSupported	L'opération spécifiée n'est pas prise en charge.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	La passerelle spécifiée n'est pas à jour.	ActivateGateway
SnapshotInProgressException	L'instantané spécifié est en cours.	DeleteVolume
SnapshotIdInvalid	L'instantané spécifié n'est pas valide.	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	La zone intermédiaire est pleine.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
TargetAlreadyExists	La cible spécifiée existe déjà.	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	La cible spécifiée n'est pas valide.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	La cible spécifiée est introuvable.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
<code>UnsupportedOperationForGatewayType</code>	L'opération spécifiée n'est pas valide pour le type de passerelle.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
<code>VolumeAlreadyExists</code>	Le volume spécifié existe déjà.	CreateCachediSCSIVolume CreateStorediSCSIVolume
<code>VolumeIdInvalid</code>	Le volume spécifié n'est pas valide.	DeleteVolume
<code>VolumeInUse</code>	Le volume spécifié est déjà en cours d'utilisation.	DeleteVolume

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
VolumeNotFound	Le volume spécifié est introuvable.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	Le volume spécifié n'est pas prêt.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

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",
  "error":
    { "errorCode": "String",
```

```
    "errorDetails": "String"
  }
}
```

Le tableau suivant explique les champs de réponse d'erreur JSON affichés dans la syntaxe précédente.

__type

L'une des exceptions de [Exceptions](#).

Type : Chaîne

error

Contient les détails de l'erreur propres à l'API. Dans les erreurs générales (par exemple, celles qui ne sont pas spécifiques à une API en particulier), ces informations d'erreur n'apparaissent pas.

Type : Collection

errorCode

L'un des codes d'erreur d'opération

Type : Chaîne

errorDetails

Ce champ n'est pas utilisé dans la version actuelle de l'API.

Type : Chaîne

message

Un des messages de code d'erreur d'opération .

Type : Chaîne

Exemples de réponses d'erreur

Le corps JSON suivant est renvoyé si vous utilisez l'API DescribeStorediSCSIVolumes et que vous spécifiez une entrée de demande d'ARN de passerelle qui n'existe pas.

```
{
```

```
"__type": "InvalidGatewayRequestException",
"message": "The specified volume was not found.",
"error": {
  "errorCode": "VolumeNotFound"
}
}
```

Le corps JSON suivant est retourné si Storage Gateway calcule une signature qui ne correspond pas à celle envoyée avec une requête.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
provided."
}
```

Opérations dans Storage Gateway

Pour obtenir la liste des opérations Storage Gateway, consultez [Actions](#) dans le [AWS Storage Gateway API Reference](#).

Historique du document pourAWSStorage Gateway de

- Version d'API : 30-06-2013
- Dernière mise à jour de documentation : 12 octobre 2021

Le tableau ci-après décrit les modifications importantes dans chaque édition duAWSGuide d'utilisation Storage Gatewayaprès avril 2018. Pour recevoir les notifications des mises à jour de cette documentation, abonnez-vous à un flux RSS.

update-history-change

[Procédures de création d'une passerelle](#)

update-history-description

La procédure de création d'une nouvelle passerelle a été mise à jour pour prendre en compte les modifications relatives à la console Storage Gateway. Pour de plus amples informations, veuillez consulter [Créer et activer une passerelle de fichiers Amazon S3](#).

update-history-date

12 octobre 2021

[Support des fichiers à fermeture forcée sur les partages de fichiers SMB](#)

Vous pouvez désormais utiliser les paramètres de groupe local pour attribuer des autorisations d'administrateur de passerelle. Les administrateurs de passerelle peuvent utiliser le composant logiciel enfichable Microsoft Management Console des dossiers partagés pour forcer la fermeture des fichiers ouverts et verrouillés sur des partages de fichiers SMB. Pour de plus amples informations, veuillez consulter

12 octobre 2021

[Configurez des groupes locaux pour votre passerelle.](#)

[Prise en charge des journaux d'audit des partages de fichiers NFS](#)

Vous pouvez désormais configurer des partages de fichiers NFS pour générer des journaux d'audit qui fournissent des détails sur l'accès des utilisateurs aux fichiers et dossiers dans un partage de fichiers. Vous pouvez utiliser ces journaux pour surveiller les activités des utilisateurs et prendre des mesures si des modèles d'activité inappropriés sont identifiés. Pour de plus amples informations, veuillez consulter [Comprendre les journaux d'audit de passerelle de fichiers](#).

12 octobre 2021

[Prise en charge de l'alias du point](#)

Les partages de fichiers de passerelle de fichiers peuvent désormais se connecter au stockage Amazon S3 à l'aide d'alias de point d'accès de type compartiment. Pour de plus amples informations, veuillez consulter [Création d'un partage de fichiers](#).

12 octobre 2021

[Prise en charge des points d'accès et des points d'accès VPC](#)

Les partages de fichiers de passerelle de fichiers peuvent désormais se connecter à des compartiments S3 via des points d'accès ou des points de terminaison d'interface de votre VPC alimentés par AWS PrivateLink. Pour de plus amples informations, veuillez consulter [Création d'un partage de fichiers](#).

7 juillet 2021

[Support de verrouillage opportuniste](#)

Les partages de fichiers de passerelle de fichiers peuvent désormais utiliser un verrouillage opportuniste pour optimiser leur stratégie de mise en mémoire tampon des fichiers, ce qui améliore les performances dans la plupart des cas, en particulier en ce qui concerne les menus contextuels Windows. Pour de plus amples informations, veuillez consulter [Création d'un partage de fichiers SMB](#).

7 juillet 2021

[conformité au programme FedRAMP](#)

Storage Gateway est désormais conforme à FedRAMP. Pour de plus amples informations, veuillez consulter [Validation de la conformité pour Storage Gateway](#).

24 novembre 2020

[Limitation de la bande passante basée sur les horaires](#)

Storage Gateway prend désormais en charge la limitation de la bande passante basée sur la planification pour les passerelles de bande et de volume. Pour de plus amples informations, veuillez consulter [Planification de la limitation de bande passante à l'aide de la console Storage Gateway](#).

9 novembre 2020

[Notification de chargement de fichiers pour passerelle de fichiers](#)

La passerelle de fichiers fournit désormais une notification de chargement de fichiers, qui vous avertit lorsqu'un fichier a été complètement téléchargé sur Amazon S3 par la passerelle de fichiers. Pour de plus amples informations, veuillez consulter [Obtenir une notification de téléchargement de fichiers](#).

9 novembre 2020

[Énumération basée sur l'accès pour la passerelle de fichiers](#)

La passerelle de fichiers fournit désormais une énumération basée sur l'accès, qui filtre l'énumération des fichiers et des dossiers sur un partage de fichiers SMB en fonction des ACL du partage. Pour de plus amples informations, veuillez consulter [Création d'un partage de fichiers SMB](#).

9 novembre 2020

Migration de la passerelle	La passerelle de fichiers fournit désormais un processus documenté pour remplacer une passerelle de fichiers existante par une nouvelle passerelle de fichiers. Pour de plus amples informations, veuillez consulter Remplacement d'une passerelle de fichiers par une nouvelle passerelle de fichiers .	30 octobre 2020
Performances de lecture du cache froid de la passerelle de fichiers 4x	Storage Gateway a augmenté les performances de lecture du cache froid 4x. Pour de plus amples informations, veuillez consulter Conseils de performance pour les passerelles de fichiers .	31 août 2020
Commandez l'appliance matérielle via la console	Vous pouvez désormais commander l'appliance matérielle via leAWSConsole Storage Gateway. Pour de plus amples informations, veuillez consulter Utilisation de l'appliance matérielle Storage Gateway .	12 août 2020

[Support des points de terminaison FIPS \(Federal Information Processing Standard\) dans les nouveaux AWS Régions](#)

Vous pouvez désormais activer une passerelle avec des points de terminaison FIPS dans les régions USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Californie du Nord), USA Ouest (Oregon) et Canada (Centre). Pour de plus amples informations, veuillez consulter [AWS Points de terminaison et quotas Storage Gateway](#) dans le [AWS Référence générale](#).

31 juillet 2020

[Support de plusieurs partages de fichiers attachés à un seul compartiment Amazon S3](#)

7 juillet 2020

La passerelle de fichiers prend désormais en charge la création de plusieurs partages de fichiers pour un seul compartiment S3 et la synchronisation du cache local de la passerelle de fichiers avec un compartiment en fonction de la fréquence d'accès au répertoire. Vous pouvez limiter le nombre de compartiments nécessaires à la gestion des partages de fichiers que vous créez sur votre passerelle de fichiers. Vous pouvez définir plusieurs préfixes S3 pour un compartiment S3 et mapper un préfixe S3 unique à un partage de fichiers de passerelle unique. Vous pouvez également définir les noms de partage de fichiers de passerelle pour qu'ils soient indépendants du nom du compartiment pour correspondre à la convention de dénomination des partages de fichiers sur site. Pour de plus amples informations, veuillez consulter [Création d'un partage de fichiers NFS](#) ou [Création d'un partage de fichiers SMB](#).

[Augmentation de 4x du stockage en cache local de la passerelle](#)

Storage Gateway prend désormais en charge un cache local pouvant atteindre 64 To pour la passerelle de fichiers, ce qui améliore les performances des applications locales en fournissant un accès à faible latence à des jeux de données de travail plus volumineux. Pour de plus amples informations, veuillez consulter [Tailles de disques locales recommandées pour votre passerelle](#) dans le Guide d'utilisation Storage Gateway.

7 juillet 2020

[Afficher les alarmes Amazon CloudWatch dans la console Storage Gateway](#)

Vous pouvez désormais afficher les alarmes CloudWatch dans la console Storage Gateway. Pour de plus amples informations, veuillez consulter [Présentation des alarmes CloudWatch](#).

29 mai 2020

[Prise en charge des points de terminaison FIPS \(Federal Information Processing Standard\)](#)

Vous pouvez désormais activer une passerelle avec des points de terminaison FIPS dans les régions AWS GovCloud (US). Pour choisir un point de terminaison FIPS pour une passerelle de fichiers, veuillez consulter [Choix d'un point de terminaison de service](#). Pour choisir un point de terminaison FIPS pour une passerelle de volumes, veuillez consulter [Choix d'un point de terminaison de service](#). Pour choisir un point de terminaison FIPS pour une passerelle de bandes, veuillez consulter [Choix d'un point de terminaison de service](#).

22 mai 2020

[Nouvelles régions AWS](#)

Storage Gateway est désormais disponible dans les régions Afrique (Le Cap) et Europe (Milan). Pour de plus amples informations, veuillez consulter [AWS Points de terminaison et quotas Storage Gateway](#) dans le [Référé](#)nce générale.

7 mai 2020

[Prise en charge de la classe de stockage S3 Intelligent-Tiering](#)

Storage Gateway prend désormais en charge la classe de stockage S3 Intelligent-Tiering. La classe de stockage S3 Intelligent-Tiering optimise les coûts de stockage en déplaçant automatiquement les données vers le niveau d'accès de stockage le plus économique, sans incidence sur les performances ni sur les frais d'exploitation. Pour de plus amples informations, veuillez consulter [Classe de stockage pour optimiser automatiquement les objets à accès fréquent et peu fréquent](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

30 avril 2020

[NouvelleAWSRegion \(Région\)](#)

Storage Gateway est désormais disponible dans laAWSRégion GovCloud (USA Est). Pour de plus amples informations, veuillez consulter [AWSPoints de terminaison et quotas Storage Gateway](#) dans leAWSRéférence générale.

12 mars 2020

[Prise en charge de l'hyperviseur KVM \(machine virtuelle basée sur le noyau Linux\)](#)

Storage Gateway permet désormais de déployer une passerelle sur site sur la plateforme de virtualisation KVM. Les passerelles déployées sur KVM disposent des mêmes fonctionnalités que les passerelles locales existantes. Pour de plus amples informations, veuillez consulter [Hyperviseurs pris en charge et exigences pour l'hôte](#) dans le Guide d'utilisation Storage Gateway.

4 février 2020

[Prise en charge de VMware vSphere HA \(High Availability\)](#)

Storage Gateway prend désormais en charge la haute disponibilité sur VMware afin de protéger les charges de travail de stockage contre les défaillances de matériel, d'hyperviseur ou de réseau. Pour de plus amples informations, veuillez consulter [L'utilisation de VMware vSphere High Availability avec Storage Gateway](#) dans le Guide d'utilisation Storage Gateway. Cette version inclut également des améliorations de performances. Pour de plus amples informations, veuillez consulter [Performances](#) dans le Guide d'utilisation Storage Gateway.

20 novembre 2019

[NouvelleRégion AWSpour
Passerelle de bande](#)

La passerelle de bande est désormais disponible dans la région Amérique du Sud (Sao Paulo). Pour de plus amples informations, veuillez consulter [AWSPoints de terminaison et quotas Storage Gateway](#) dans leAWSRéférence générale.

24 septembre 2019

[Support de Amazon
CloudWatch Logs](#)

Vous pouvez désormais configurer des passerelles de fichiers avec des groupes de journaux Amazon CloudWatch pour être informé des erreurs et de l'état de votre passerelle et de ses ressources. Pour de plus amples informations, veuillez consulter [Réception de notifications sur l'Health passerelle et les erreurs avec les groupes de journaux Amazon CloudWatch](#) dans leGuide utilisateur de Storage Gateway.

4 septembre 2019

[NouvelleRégion AWS](#)

Storage Gateway est désormais disponible dans la région Asie-Pacifique (Hong Kong). Pour de plus amples informations, veuillez consulter [AWSPoints de terminaison et quotas Storage Gateway](#) dans leAWSRéférence générale.

14 août 2019

[Nouvelle Région AWS](#)

Storage Gateway est désormais disponible dans la région Moyen-Orient (Bahreïn) . Pour de plus amples informations, veuillez consulter [AWSPoints de terminaison et quotas Storage Gateway](#) dans leAWSRéférence générale.

29 juillet 2019

[Prise en charge de l'activation d'une passerelle dans un Virtual Private Cloud \(VPC\)](#)

Vous pouvez désormais activer une passerelle dans un VPC. Vous pouvez créer une connexion privée entre votre appliance logicielle sur site et une infrastructure de stockage basée sur le cloud. Pour plus d'informations, consultez [Activation d'une passerelle dans un Virtual Private Cloud.](#)

20 juin 2019

[Prise en charge du partage de fichiers SMB pour les listes de contrôle d'accès \(ACL\) Microsoft Windows](#)

Pour les passerelles de fichiers, vous pouvez désormais utiliser des listes de contrôle d'accès (ACL) Microsoft Windows pour contrôler l'accès aux partages de fichiers SMB (Server Message Block). Pour plus d'informations, consultez [Utilisation des listes ACL Microsoft Windows pour contrôler l'accès à un partage de fichiers SMB.](#)

8 mai 2019

[La passerelle de fichiers prend en charge l'autorisation basée sur les balises](#)

La passerelle de fichiers prend désormais en charge l'autorisation basée sur les balises. Vous pouvez contrôler l'accès aux ressources de la passerelle de fichiers en fonction des balises de ces ressources. Vous pouvez également contrôler l'accès en fonction des balises qui peuvent être transmises dans une condition de demande IAM. Pour plus d'informations, consultez [Contrôle de l'accès aux ressources de la passerelle de fichiers](#).

4 mars 2019

[Disponibilité de l'appliance matérielle Storage Gateway en Europe](#)

L'appliance matérielle Storage Gateway est désormais disponible en Europe. Pour de plus amples informations, veuillez consulter [AWS Régions Storage Gateway](#) dans le [AWS Référence générale](#). De plus, vous pouvez désormais augmenter le stockage utilisable sur l'appliance matérielle Storage Gateway de 5 To à 12 To et remplacer la carte réseau cuivre installée par une carte réseau à fibre optique 10 Gigabits. Pour plus d'informations, consultez [Configuration de votre appliance matérielle](#).

25 février 2019

[Support de Storage Gateway](#) L'appliance matérielle Storage Gateway inclut le logiciel Storage Gateway préinstallé sur un serveur tiers. Vous pouvez gérer l'appliance dans l'AWS Management Console. L'appliance peut héberger les passerelles de fichiers, de bande et de volume. Pour de plus amples informations, veuillez consulter [Utilisation de l'appliance matérielle Storage Gateway](#). 18 septembre 2018

[Prise en charge du protocole SMB \(Server Message Block\)](#) La prise en charge des passerelles de fichiers a été ajoutée pour le protocole SMB (Server Message Block) aux partages de fichiers. Pour plus d'informations, consultez [Création d'un partage de fichiers](#). le 20 juin 2018

Mises à jour antérieures

Le tableau ci-après décrit les modifications importantes dans chaque édition du AWS Guide d'utilisation Storage Gateway avant mai 2018.

Modification	Description	Date de modification
Support de la classe de stockage S3 unizone — Accès peu courant	Pour les passerelles de fichiers, vous pouvez désormais choisir la classe de stockage S3 One Zone-IA comme classe de stockage par défaut pour vos partages de fichiers. L'utilisation de cette classe de stockage vous permet de stocker vos données d'objet	4 avril 2018

Modification	Description	Date de modification
	dans une seule zone de disponibilité dans Amazon S3. Pour plus d'informations, consultez Création d'un partage de fichiers .	
Nouveau Région AWS	La passerelle de bande est désormais disponible dans la région Asie-Pacifique (Singapour). Pour plus d'informations, consultez Régions AWS prises en charge .	3 avril 2018
Support de la notification d'actualisation du cache, du paiement par le demandeur et des listes ACL prêtes à l'emploi pour les compartiments Amazon S3	<p>Les passerelles de fichiers vous permettent désormais d'être informé lorsque la passerelle termine l'actualisation du cache pour votre compartiment Amazon S3. Pour de plus amples informations, veuillez consulter RefreshCache.html dans le Référence de Storage Gateway.</p> <p>Pour les passerelles de fichiers, vous pouvez désormais spécifier que le demandeur ou le lecteur paie les frais d'accès au lieu du propriétaire du compartiment.</p> <p>Les passerelles de fichiers vous permettent désormais d'activer Accorder le contrôle total au propriétaire du compartiment S3 qui est mappé sur le partage de fichiers NFS.</p> <p>Pour plus d'informations, consultez Création d'un partage de fichiers.</p>	1 mars 2018
Nouveau Région AWS	Storage Gateway est désormais disponible dans la région Paris (Paris). Pour plus d'informations, consultez Régions AWS prises en charge .	18 décembre 2017

Modification	Description	Date de modification
Prise en charge de la notification de chargement de fichier et de la détermination du type MIME	<p>Les passerelles de fichiers vous permettent désormais d'obtenir une notification lorsque tous les fichiers écrits dans votre partage de fichiers NFS ont été chargés dans Amazon S3. Pour de plus amples informations, veuillez consulter NotifyWhenUploaded dans le Référence de Storage Gateway.</p> <p>Les passerelles de fichiers vous permettent désormais de deviner le type MIME des objets chargés en fonction des extensions de fichier. Pour plus d'informations, consultez Création d'un partage de fichiers.</p>	21 novembre 2017
Prise en charge de VMware ESXi Hypervisor version 6.5	AWSStorage Gateway prend désormais en charge VMware ESXi Hypervisor version 6.5. Ceci s'ajoute aux versions 4.1, 5.0, 5.1, 5.5 et 6.0. Pour plus d'informations, consultez Hyperviseurs pris en charge et exigences pour l'hôte .	13 septembre 2017
Prise en charge de la passerelle de fichiers pour l'hyperviseur Microsoft Hyper-V	Vous pouvez désormais déployer une passerelle de fichiers sur un hyperviseur Microsoft Hyper-V. Pour plus d'informations, veuillez consulter Hyperviseurs pris en charge et exigences pour l'hôte .	22 juin 2017
Nouveau Région AWS	Storage Gateway est désormais disponible dans la région Asie-Pacifique (Mumbai). Pour plus d'informations, consultez Régions AWS prises en charge .	02 mai 2017

Modification	Description	Date de modification
Mises à jour des paramètres de partage de fichiers Prise en charge de l'actualisation du cache pour les partages de fichiers	<p>Les passerelles de fichiers ajoutent désormais des options de montage aux paramètres de partage de fichiers. Vous pouvez désormais définir des options d'écrasement et de lecture seule pour votre partage de fichiers. Pour plus d'informations, consultez Création d'un partage de fichiers.</p> <p>Les passerelles de fichiers peuvent désormais rechercher dans le compartiment Amazon S3 les objets qui ont été ajoutés ou supprimés depuis que la passerelle a répertorié pour la dernière fois le contenu du compartiment et mis en cache les résultats. Pour plus d'informations, consultez RefreshCache dans API Reference.</p>	28 mars 2017
Prise en charge des passerelles de fichiers sur Amazon EC2	<p>AWSStorage Gateway permet désormais de déployer une passerelle de fichiers dans Amazon EC2. Vous pouvez lancer une passerelle de fichiers dans Amazon EC2 à l'aide Storage Gateway l'Amazon Machine Image (AMI) désormais disponible en tant qu'AMI de la communauté. Pour plus d'informations sur la création d'une passerelle de fichiers et son déploiement sur une instance EC2, consultez Créer et activer une passerelle de fichiers Amazon S3. Pour plus d'informations sur le lancement d'une passerelle de fichiers AMI, consultez Déploiement d'une passerelle de fichiers sur un hôte Amazon EC2.</p> <p>En outre, la passerelle de fichiers prend désormais en charge la configuration d'un proxy HTTP. Pour plus d'informations, consultez Routage de votre passerelle déployée sur EC2 via un proxy HTTP.</p>	08 février 2017

Modification	Description	Date de modification
Nouveau Région AWS	Storage Gateway est désormais disponible dans la région Europe (Londres). Pour plus d'informations, consultez Régions AWS prises en charge .	13 décembre 2016
Nouveau Région AWS	Storage Gateway est désormais disponible dans la région Canada (Centre). Pour plus d'informations, consultez Régions AWS prises en charge .	08 décembre 2016
Prise en charge de la passerelle de fichiers	En plus des passerelles de volume et de la passerelle de bande, Storage Gateway fournit désormais la passerelle de fichiers. File Gateway combine un service et une appliance logicielle virtuelle, vous permettant de stocker et récupérer des objets dans Amazon S3 à l'aide de protocoles de fichiers standard tels que NFS Network File System (NFS). La passerelle permet d'accéder aux objets dans Amazon S3 sous forme de fichiers sur un point de montage NFS.	29 novembre 2016

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.