Guide de l'utilisateur d'Amazon FSx File Gateway

AWS Storage Gateway

Version de l'API 2021-03-31

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

AWS Storage Gateway: Guide de l'utilisateur d'Amazon FSx File Gateway

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

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

Table of Contents

..... x
Qu'est-ce qu'Amazon FSx File Gateway 1
FSx Fonctionnement de File Gateway 1
Commencer avec AWS Storage Gateway 4
S'inscrire à Amazon Web Services 4
Création d'un utilisateur IAM doté de privilèges d'administrateur 5
Accès AWS Storage Gateway 7
Régions AWS compatibles avec Storage Gateway 7
Exigences relatives à la configuration de File Gateway 9
Conditions préalables 9
Exigences en matière de matériel et de stockage 10
Configuration matérielle requise pour les installations sur site VMs 10
Exigences relatives aux types d’instances Amazon EC2 10
Besoins de stockage 11
Exigences pour le réseau et le pare-feu 12
Exigences relatives aux ports 13
Exigences en matière de mise en réseau et de pare-feu pour l’appliance matérielle 28
Accorder l’accès à la passerelle via la passerelle et les routeurs 31
Configuration d’un groupe de sécurité 33
Hyperviseurs pris en charge et exigences pour l’hôte 34
Clients SMB pris en charge pour File Gateway 35
Opérations de système de fichiers prises en charge 36
Gestion des disques locaux 36
Déterminer la quantité de stockage du disque local 37
Ajouter un espace de stockage en cache 38
Utilisation du stockage éphémère avec les passerelles EC2 39
Utilisation de l’appliance matérielle 41
Configuration de votre appliance matérielle 42
Installation physique de votre appliance matérielle 44
Accès à la console de l'appliance matérielle 46
Configuration des paramètres réseau de l'appliance matérielle 47
Activation de votre appliance matérielle 49
Création d'une passerelle sur votre appliance matérielle 50
Configuration d'une adresse IP de passerelle sur l'appliance matérielle 51

Suppression du logiciel de passerelle de votre appliance matérielle 54
Suppression de votre appliance matérielle 55
Création de votre passerelle 57
Présentation - Activation de la passerelle 57
Configuration d'une passerelle 57
Connect à AWS 58
Vérifier et activer 58
Présentation - Configuration de la passerelle 58
Présentation - Ressources de stockage 58
Création d'un système de fichiers Amazon FSx pour Windows File Server 59
Création et activation d'un Amazon FSx File Gateway 60
Configurer un Amazon FSx File Gateway 60
Connectez votre Amazon FSx File Gateway à AWS 62
Vérifiez les paramètres et activez votre Amazon FSx File Gateway 63
Configuration de votre Amazon FSx File Gateway 64
Activation d'une passerelle dans un VPC 67
Création d'un point de terminaison VPC pour Storage Gateway 67
Configuration des paramètres d'accès au domaine Microsoft Active Directory 69
Joindre un système de FSx fichiers Amazon 71
Montez et utilisez votre partage de FSx fichiers Amazon 75
Montez votre partage de fichiers SMB sur votre client 75
Testez votre passerelle FSx de fichiers 77
Gestion de vos ressources Amazon FSx File Gateway 78
État de la passerelle 78
Comprendre l'état du système de fichiers 79
Modifier les informations de base de la passerelle 80
Définir le niveau de sécurité de la passerelle 81
Modification des paramètres Active Directory pour n FSx File Gateway 83
Modification des paramètres d'un système de FSx fichiers Amazon 84
Détacher un système de FSx fichiers Amazon 86
Surveillance de Storage Gateway 87
Comprendre les CloudWatch alarmes 88
Créez des CloudWatch alarmes recommandées 89
Création d'une CloudWatch alarme personnalisée 90
Surveillance de votre passerelle de 93
Obtenir les journaux de santé de File Gateway 93

Utilisation des CloudWatch métriques Amazon 94
Présentation des métriques de la passerelle 96
Comprendre les métriques du système de fichiers 103
Comprendre les journaux d'audit de File Gateway 106
Maintenance de votre passerelle 111
Gestion des mises à jour de passerelle 111
Fréquence de mise à jour et comportement attendu 112
Activer ou désactiver les mises à jour de maintenance 113
Modifier le calendrier de la fenêtre de maintenance de la passerelle 114
Appliquer une mise à jour manuellement 115
Exécution de tâches de maintenance à l'aide de la console locale 116
Accès à la console locale de la passerelle 117
Exécution de tâches sur la console locale de la machine virtuelle 120
Exécution de tâches sur la console locale EC2 137
Arrêt de votre machine virtuelle de passerelle 145
Remplacement de votre passerelle de existante par une nouvelle instance 145
Suppression de votre passerelle et suppression de ressources 148
Suppression de la passerelle à l’aide de la console Storage Gateway 148
Performances et optimisation 150
Conseils de performance de base pour File Gateway 150
FSx Performances de la passerelle de fichiers sur les clients Windows 151
Optimisation des performances de la passerelle 152
Ajouter des ressources à la passerelle 152
Ajouter des ressources à votre environnement d’application 154
Optimisation du débit de la passerelle de fichiers S3 155
Déployez votre passerelle au même endroit que vos clients 155
Réduisez les goulots d'étranglement causés par la lenteur des disques 156
Ajuster l'allocation des ressources des machines virtuelles pour le processeur, la RAM et les disques de cache 156
Régler le niveau de sécurité des PME 158
Utiliser plusieurs threads et clients pour paralléliser les opérations d'écriture 159
Désactiver l'actualisation automatique du cache 162
Augmenter le nombre de threads de téléchargement sur Amazon S3 162
Augmenter les paramètres de délai d'expiration des PME 163
Activez le verrouillage opportuniste pour les applications compatibles 163

Ajustez la capacité de la passerelle en fonction de la taille de l'ensemble de fichiers de travail ... 164
Déployez plusieurs passerelles pour des charges de travail plus importantes ... 165
Optimisation de la passerelle de fichiers S3 pour les sauvegardes de bases de données SQL Server ... 166
Déployez votre passerelle au même endroit que vos serveurs SQL ... 166
Réduisez les goulots d'étranglement causés par la lenteur des disques ... 167
Ajuster l'allocation des ressources de la machine virtuelle S3 File Gateway pour le processeur, la RAM et les disques de cache ... 167
Améliorez le débit des clients des PME en ajustant le niveau de sécurité de votre passerelle de fichiers S3 ... 169
Améliorez le débit des clients PME en divisant les sauvegardes SQL en plusieurs fichiers .. 170
Empêchez les échecs de copie de fichiers volumineux en augmentant les paramètres de délai d'expiration SMB ... 171
Augmenter le nombre de threads de téléchargement sur Amazon S3 ... 172
Désactiver l'actualisation automatique du cache ... 172
Déployez plusieurs passerelles pour prendre en charge la charge de travail ... 173
Ressources supplémentaires pour les charges de travail de sauvegarde des bases de données ... 174
Sécurité ... 175
Protection des données ... 175
Chiffrement des données ... 176
Gestion des identités et des accès ... 177
Public ciblé ... 178
Authentification par des identités ... 178
Gestion de l’accès à l’aide de politiques ... 180
Comment AWS Storage Gateway fonctionne avec IAM ... 181
Exemples de politiques basées sur l’identité ... 187
Résolution des problèmes ... 190
Utilisation de balises pour contrôler l'accès aux ressources ... 193
Validation de conformité ... 195
Résilience ... 196
Sécurité de l’infrastructure ... 197
AWS Bonnes pratiques en matière de sécurité ... 198
Journalisation et surveillance ... 198
Informations sur Storage Gateway dans CloudTrail ... 199

Comprendre les entrées des fichiers journaux de Storage Gateway 200
Résolution des problèmes 203
Résolution des problèmes : problèmes liés à la connectivité hors connexion 204
Vérifiez le pare-feu ou le proxy associé 204
Vérifiez s'il existe une inspection SSL ou approfondie des paquets en cours du trafic de votre passerelle 204
Vérifiez la métrique de IOWait pourcentage après un redémarrage ou une mise à jour logicielle 205
Vérifiez l'absence d'une panne de courant ou d'une défaillance matérielle sur l'hôte de l'hyperviseur 205
Vérifiez les problèmes liés à un disque de cache associé 205
Résolution des problèmes : problèmes liés à Active Directory 206
Vérifiez que la passerelle peut atteindre le contrôleur de domaine en exécutant un test nping 206
Vérifiez les options DHCP définies pour le VPC de votre instance de passerelle Amazon EC2 207
Vérifiez que la passerelle peut résoudre le domaine en exécutant une requête DIG 207
Vérifiez les paramètres et les rôles du contrôleur de domaine 209
Vérifiez que la passerelle est connectée au contrôleur de domaine le plus proche 209
Vérifiez qu'Active Directory crée de nouveaux objets informatiques dans l'unité organisationnelle (UO) par défaut 209
Consultez les journaux des événements de votre contrôleur de domaine 210
Résolution des problèmes : problèmes d'activation de la passerelle 210
Résoudre les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison public 211
Résolvez les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison Amazon VPC 214
Résolvez les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison public et qu'il existe un point de terminaison VPC Storage Gateway dans le même VPC 218
Résolution des problèmes liés à la passerelle sur site 219
Activer l' Support accès pour résoudre les problèmes liés à votre passerelle 224
Résolution des problèmes : problèmes d'installation de Microsoft Hyper-V 225
Résolution des problèmes : problèmes liés à la passerelle Amazon EC2 230
L’activation de passerelle ne se produit pas au bout de quelques instants 230
Vous ne trouvez pas l’instance de passerelle EC2 dans la liste des instances 231
Connexion à votre passerelle Amazon EC2 à l’aide de la Serial Console 231

Activer l' Support accès pour aider à résoudre les problèmes liés à la passerelle 232
Résolution des problèmes : problèmes liés à l'appliance matérielle 234
Comment déterminer l’adresse IP du service 234
Effectuer une réinitialisation d’usine 234
Réaliser un redémarrage à distance 235
Obtenir l’assistance pour Dell iDRAC 235
Trouver le numéro de série de l’appliance matérielle 235
Obtenir le support des appliances matérielles 235
Résolution des problèmes : problèmes liés à la passerelle de fichiers 236
Erreur : FileMissing 237
Erreur : FsxFileSystemAuthenticationFailure 237
Erreur : FsxFileSystemConnectionFailure 237
Erreur : FsxFileSystemFull 238
Erreur : GatewayClockOutOfSync 238
Erreur : InvalidFileState 238
Erreur : ObjectMissing 239
Erreur : DroppedNotifications 239
Notification : HardReboot 240
Notification : Reboot 240
Résolution des problèmes liés au domaine Active Directory 241
Résolution des problèmes avec CloudWatch les métriques 243
Notifications d’intégrité relatives à la haute disponibilité 246
Résolution des problèmes : problèmes de haute disponibilité 246
Notifications d’intégrité 246
Métriques 248
Bonnes pratiques 249
Récupération de vos données 249
Récupération après l’arrêt inattendu d’une machine virtuelle 249
Récupération des données d’un disque de cache défaillant 250
Récupération de données à partir d’un centre de données inaccessible 250
Restaurer les données sur Amazon FSx 251
Nettoyez les ressources inutiles 251
Ressources supplémentaires 253
Configuration de l'hôte 253
Déployer un hôte Amazon EC2 par défaut pour File Gateway 254
Déployez un hôte Amazon EC2 personnalisé pour File Gateway 257

Modifier les options de métadonnées de l'instance Amazon EC2 261
Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux .. 261
Synchroniser l'heure de la machine virtuelle avec VMware celle de l'hôte 262
Configuration des adaptateurs réseau pour votre passerelle 264
Utilisation de Storage Gateway avec VMware HA 267
Obtenir la clé d'activation 272
Linux (curl) 273
Linux (bash/zsh) 273
Microsoft Windows PowerShell 274
Utilisation de votre console locale 275
En utilisant Direct Connect 275
Autorisations Active Directory 276
Obtenir l'adresse IP de la passerelle 277
Obtention d’une adresse IP auprès d’un hôte Amazon EC2 277
Comprendre les ressources et les ressources IDs 278
Travailler avec Resource IDs 279
Balisage de vos ressources 280
Utilisation des tags 281
Composants open source 282
Composants open source pour Storage Gateway 282
Composants open source pour Amazon FSx File Gateway 283
Quotas 283
Quotas pour les systèmes FSx de fichiers Amazon 283
Tailles des disques locaux recommandées pour votre passerelle 284
Référence d’API 286
En-têtes de requête obligatoires 286
Signature des requêtes 289
Exemple de calcul de signature 290
Réponses d’erreur 291
Exceptions 292
Codes d’erreur d’opération 294
Réponses d’erreur 314
Actions 316
Historique de la documentation 317
Mises à jour antérieures 331

Amazon FSx File Gateway n'est plus disponible pour les nouveaux clients. Les clients existants de FSx File Gateway peuvent continuer à utiliser le service normalement. Pour des fonctionnalités similaires à FSx File Gateway, consultez ce billet de blog.

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.

Qu'est-ce qu'Amazon FSx File Gateway

Amazon FSx File Gateway (FSx File Gateway) est un nouveau type de passerelle de fichiers qui fournit une faible latence et un accès efficace aux partages de fichiers sur le cloud FSx pour Windows File Server depuis votre installation sur site. Si vous maintenez un stockage de fichiers sur site pour des raisons de latence ou de bande passante, vous pouvez utiliser FSx File Gateway pour un accès fluide à des partages de fichiers Windows entièrement gérés, hautement fiables et pratiquement illimités fournis dans le AWS cloud par FSx for Windows File Server.

Avantages de l'utilisation d'Amazon FSx File Gateway

FSx File Gateway offre les avantages suivants :

- Permet d'éliminer les serveurs de fichiers sur site et de consolider toutes leurs données AWS afin de tirer parti de l'échelle et de la rentabilité du stockage dans le cloud.
- Fournit des options que vous pouvez utiliser pour toutes vos charges de travail de fichiers, y compris celles qui nécessitent un accès local aux données dans le cloud.
- Les applications qui doivent rester sur site peuvent désormais bénéficier de la même faible latence et des mêmes performances élevées que celles d'origine AWS, sans surcharger vos réseaux ni affecter les latences de vos applications les plus exigeantes.

Comment fonctionne Amazon FSx File Gateway

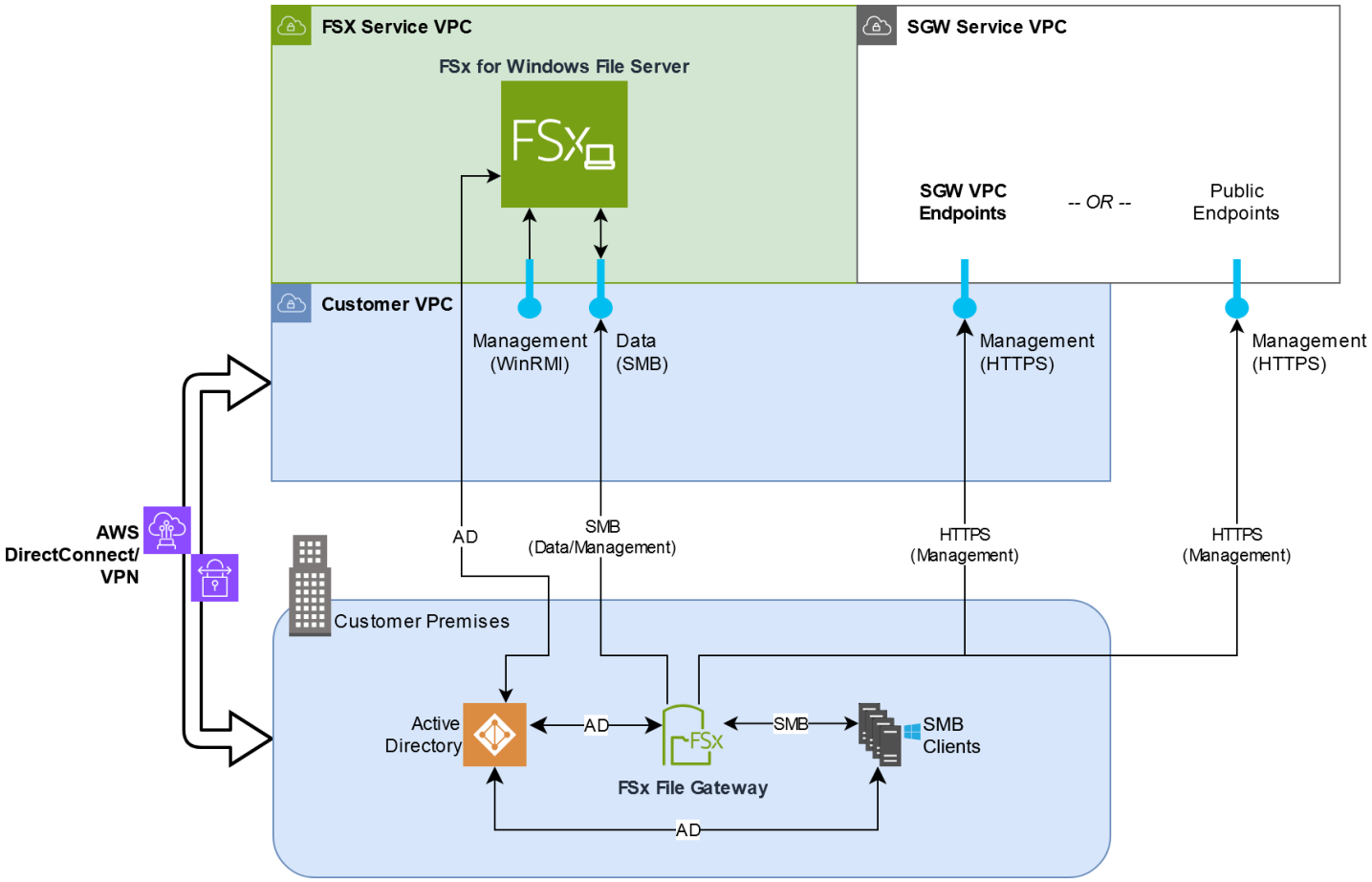
Pour utiliser Amazon FSx File Gateway (FSx File Gateway), vous devez disposer d'au moins un système de fichiers Amazon FSx pour Windows File Server. Vous devez également disposer d'un accès local au serveur FSx de fichiers Windows, via un VPN ou via une Direct Connect connexion. Pour plus d'informations sur l'utilisation des systèmes de FSx fichiers Amazon, consultez Qu'est-ce qu'Amazon FSx pour Windows File Server ?

Vous déployez la passerelle dans votre environnement sur site sous la forme d'une machine virtuelle (VM) exécutée sur VMware ESXi Microsoft Hyper-V ou d'une machine virtuelle basée sur le noyau Linux (KVM), ou sous forme d'appliance matérielle que vous commandez auprès de votre revendeur préféré. Vous pouvez également déployer la machine virtuelle Storage Gateway dans VMware Cloud AWS on ou en tant qu'AMI sur Amazon EC2. Après avoir déployé votre appliance, vous activez la passerelle de FSx fichiers depuis la console Storage Gateway ou via l'API Storage Gateway.

Une fois qu'Amazon FSx File Gateway est activé et que vous pouvez accéder au FSx serveur de fichiers Windows, utilisez la console Storage Gateway pour le joindre à votre domaine Microsoft Active Directory. Une fois que la passerelle a rejoint un domaine avec succès, vous pouvez utiliser la console Storage Gateway FSx pour connecter la passerelle à un serveur de fichiers Windows existant. FSx pour Windows File Server rend tous les partages du serveur disponibles sous forme de partages sur votre Amazon FSx File Gateway. Vous pouvez ensuite utiliser un client pour parcourir et vous connecter aux partages de fichiers sur FSx File Gateway qui correspondent à la passerelle de FSx fichiers sélectionnée.

Lorsque les partages de fichiers sont connectés, vous pouvez lire et écrire vos fichiers localement, tout en bénéficiant de toutes les fonctionnalités disponibles sur FSx Windows File Server. FSx File Gateway mappe les partages de fichiers locaux et leur contenu aux partages de fichiers stockés FSx à distance sur Windows File Server. Il existe une correspondance 1:1 entre les fichiers distants et visibles localement et leurs partages.

Le schéma suivant fournit une vue d'ensemble du déploiement du stockage de fichiers pour Storage Gateway.



Notez ce qui suit dans le schéma :

- Direct Connect ou un VPN est nécessaire pour permettre à la passerelle de FSx fichiers d'accéder au partage de FSx fichiers Amazon via SMB et FSx pour permettre au serveur de fichiers Windows de rejoindre votre domaine Active Directory local.
- Amazon Virtual Private Cloud (Amazon VPC) est nécessaire pour se connecter au service VPC FSx pour Windows File Server et au VPC du service Storage Gateway à l'aide de points de terminaison privés. La passerelle de FSx fichiers peut également se connecter aux points de terminaison publics.

Vous pouvez utiliser Amazon FSx File Gateway dans toutes les AWS régions où FSx Windows File Server est disponible.

Commencer avec AWS Storage Gateway

Cette section fournit des instructions pour démarrer avec AWS. Vous avez besoin d'un AWS compte avant de pouvoir commencer à l'utiliser AWS Storage Gateway. Vous pouvez utiliser un AWS compte existant ou créer un nouveau compte. Vous avez également besoin dans votre AWS compte d'un utilisateur IAM appartenant à un groupe disposant des autorisations administratives nécessaires pour effectuer les tâches de Storage Gateway. Les utilisateurs disposant des privilèges appropriés peuvent accéder à la console Storage Gateway et à l'API Storage Gateway pour effectuer des tâches de déploiement, de configuration et de maintenance de la passerelle. Si vous utilisez Storage Gateway pour la première fois, nous vous recommandons de consulter les sections AWS Régions prises en charge et Exigences de configuration de File Gateway avant de commencer à travailler avec Storage Gateway.

Cette section contient les rubriques suivantes, qui fournissent des informations supplémentaires sur la prise en main AWS Storage Gateway :

Rubriques

- S'inscrire à Amazon Web Services- Découvrez comment vous inscrire AWS et créer un AWS compte.
- Création d'un utilisateur IAM doté de privilèges d'administrateur- Découvrez comment créer un utilisateur IAM doté de privilèges administratifs pour votre AWS compte.
- Accès AWS Storage Gateway- Découvrez comment y accéder AWS Storage Gateway via la console Storage Gateway ou par programmation à l'aide du. AWS SDKs
- Régions AWS compatibles avec Storage Gateway- Découvrez les AWS régions que vous pouvez utiliser pour stocker vos données lorsque vous activez votre passerelle dans Storage Gateway.

S'inscrire à Amazon Web Services

Un Compte AWS est une exigence fondamentale pour accéder aux AWS services. Votre Compte AWS est le conteneur de base pour toutes les AWS ressources que vous créez en tant qu' AWS utilisateur. Vous Compte AWS êtes également la limite de sécurité de base pour vos AWS ressources. Toutes les ressources que vous créez dans votre compte sont accessibles aux utilisateurs qui possèdent des informations d'identification pour le compte. Avant de pouvoir commencer à utiliser AWS Storage Gateway, vous devez vous inscrire à un Compte AWS.

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

Pour vous inscrire à un Compte AWS

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

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

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

Nous vous recommandons également de demander à vos utilisateurs d'utiliser des informations d'identification temporaires lors de l'accès AWS. Pour fournir des informations d'identification temporaires, vous pouvez utiliser la fédération et un fournisseur d'identité, tel que AWS IAM Identity Center. Si votre entreprise utilise déjà un fournisseur d'identité, vous pouvez l'utiliser avec la fédération afin de simplifier la manière dont vous fournissez l'accès aux ressources de votre AWS compte.

Création d'un utilisateur IAM doté de privilèges d'administrateur

Après avoir créé votre AWS compte, suivez les étapes ci-dessous pour créer un utilisateur Gestion des identités et des accès AWS (IAM) pour vous-même, puis ajoutez cet utilisateur à un groupe doté d'autorisations administratives. Pour plus d'informations sur l'utilisation du Gestion des identités et des accès AWS service pour contrôler l'accès aux ressources Storage Gateway, consultezGestion des identités et des accès pour AWS Storage Gateway.

Afin de créer un utilisateur administrateur, choisissez l'une des options suivantes :

Choisissez un moyen de gérer votre administrateur	À	En	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des informations d'identification à court terme pour accéder à AWS. C'est conforme aux bonnes pratiques en matière de sécurité. Pour plus d'informations sur les bonnes pratiques, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.	Suivant les instructions fournies dans Mise en route dans le Guide de l'utilisateur AWS IAM Identity Center .	Configurez l'accès par programmation en configurant le AWS CLI à utiliser AWS IAM Identity Center dans le guide de l'AWS Command Line Interface utilisateur.
Dans IAM (Non recommandé)	Utiliser les informations d'identification à long terme pour accéder à AWS.	Suivant les instructions fournies dans Création d'un utilisateur IAM pour l'accès d'urgence dans le Guide de l'utilisateur IAM.	Configurer l'accès par programmation en suivant les instructions fournies dans Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

> **Warning**
>
> Les utilisateurs IAM disposent d'informations d'identification à long terme qui présentent un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces

utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires.

Accès AWS Storage Gateway

Vous pouvez utiliser la AWS Storage Gateway console pour effectuer diverses tâches de configuration et de maintenance des passerelles, notamment l'activation ou le retrait des dispositifs matériels Storage Gateway de votre déploiement, la création, la gestion et la suppression des différents types de passerelles, la , l'attachement, la gestion et la de systèmes de de fichiers détachés et le suivi de l'état des différents éléments du service Storage Gateway. Dans un souci de simplicité et de facilité d'utilisation, ce guide se concentre sur l'exécution de tâches à l'aide de l'interface Web de la console Storage Gateway. Vous pouvez accéder à la console Storage Gateway via votre navigateur Web à l'adresse suivante :https://console.aws.amazon.com/storagegateway/home/.

Si vous préférez une approche programmatique, vous pouvez utiliser l'interface de programmation d' AWS Storage Gateway applications (API) ou l'interface de ligne de commande (CLI) pour configurer et gérer les ressources de votre déploiement Storage Gateway. Pour plus d'informations sur les actions, les types de données et la syntaxe requise pour l'API Storage Gateway, consultez le manuel Storage Gateway API Reference. Pour plus d'informations sur la CLI Storage Gateway, consultez le manuel AWS CLI Command Reference.

Vous pouvez également utiliser le AWS SDKs pour développer des applications qui interagissent avec Storage Gateway. AWS SDKs Pour Java, .NET et PHP, ils encapsulent l'API Storage Gateway sous-jacente afin de simplifier vos tâches de programmation. Pour plus d'informations sur le téléchargement des bibliothèques du SDK, consultez le AWS Developer Center.

Pour plus d'informations sur la tarification, consultez Tarification AWS Storage Gateway.

Régions AWS compatibles avec Storage Gateway

An Région AWS est un emplacement physique dans le monde AWS comportant plusieurs zones de disponibilité. Les zones de disponibilité se composent d'un ou de plusieurs centres de AWS données distincts, chacun doté d'une alimentation, d'un réseau et d'une connectivité redondants, hébergés dans des installations distinctes. Cela signifie que chacune Région AWS est physiquement isolée et indépendante des autres régions. Les régions fournissent une tolérance aux pannes, une stabilité et une résilience, et peuvent également réduire la latence. Les ressources que vous créez dans une

région n'existent dans aucune autre région, sauf si vous utilisez explicitement une fonctionnalité de réplication proposée par un AWS service. Par exemple, Amazon S3 et Amazon EC2 prennent en charge la réplication entre régions. Certains services, tels que Gestion des identités et des accès AWS, ne disposent pas de ressources régionales. Vous pouvez lancer AWS des ressources dans des emplacements qui répondent aux besoins de votre entreprise. Par exemple, vous souhaiterez peut-être lancer des instances Amazon EC2 pour héberger vos AWS Storage Gateway appareils Région AWS en Europe ou pour vous rapprocher de vos utilisateurs européens, ou pour répondre aux exigences légales. Vous Compte AWS déterminez les régions prises en charge par un service spécifique que vous pouvez utiliser.

Amazon FSx File Gateway stocke les données des fichiers dans la AWS région où se trouve votre système de FSx fichiers Amazon. Avant de commencer à déployer votre passerelle, choisissez une région dans le coin supérieur droit de la console Storage Gateway.

- Amazon FSx File Gateway — Pour connaître les AWS régions prises en charge et la liste des points de terminaison de AWS service que vous pouvez utiliser avec Amazon FSx File Gateway, consultez la section Points de terminaison et quotas Amazon FSx File Gateway dans le. Références générales AWS
- Storage Gateway : pour connaître les AWS régions prises en charge et la liste des points de terminaison de AWS service que vous pouvez utiliser avec Storage Gateway, consultez la section AWS Storage Gateway Points de terminaison et quotas dans le. Références générales AWS
- Appliance matérielle Storage Gateway : pour connaître les régions prises en charge que vous pouvez utiliser avec l'appliance matérielle, consultez la section Régions de l'appliance AWS Storage Gateway matérielle dans le Références générales AWS.

Exigences relatives à la configuration de File Gateway

Sauf indication 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. Passez en revue les exigences qui s'appliquent à la configuration de votre passerelle avant de déployer votre passerelle.

Rubriques

- Conditions préalables
- 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 SMB pris en charge pour File Gateway
- Opérations de système de fichiers prises en charge pour File Gateway
- Gestion des disques locaux pour votre passerelle

Conditions préalables

Avant de configurer votre Amazon FSx File Gateway (passerelle de FSx fichiers) , vous devez remplir les conditions préalables suivantes :

- Créez et configurez un système de fichiers FSx pour Windows File Server. Pour obtenir des instructions, consultez l'étape 1 : créer votre système de fichiers dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.
- Configurez Microsoft Active Directory (AD) et créez un compte de service Active Directory avec les autorisations requises. Pour plus d'informations, voir Exigences relatives aux autorisations relatives aux aux comptes de service Active Directory.
- Assurez-vous que la bande passante réseau est suffisante entre la passerelle et AWS. Un minimum de 100 Mbits/s est requis pour télécharger, activer et mettre à jour correctement la passerelle.
- Configurez la connexion que vous souhaitez utiliser pour le trafic réseau entre AWS et l'environnement sur site dans lequel vous déployez votre passerelle. Vous pouvez vous connecter via Internet public, un réseau privé, un VPN ou Direct Connect. Si vous souhaitez que votre

passerelle communique AWS via une connexion privée avec un Amazon Virtual Private Cloud, configurez le VPC Amazon avant de configurer votre passerelle.

- Assurez-vous que votre passerelle peut résoudre le nom de votre contrôleur de domaine Active Directory. Vous pouvez utiliser le protocole DHCP dans votre domaine Active Directory pour gérer la résolution ou spécifier un serveur DNS manuellement dans le 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 configurations matérielles et de stockage minimales requises pour votre passerelle, ainsi que sur la quantité minimale d'espace disque à allouer pour le stockage requis.

Configuration matérielle requise pour les installations sur site VMs

Lorsque vous déployez votre passerelle sur site, assurez-vous que le matériel sous-jacent sur lequel vous déployez la machine virtuelle (VM) de passerelle peut consacrer les ressources minimales suivantes :

- Quatre processeurs virtuels assignés à la machine virtuelle
- 16 Gio de RAM réservée pour les passerelles de fichiers
- 80 GiB d'espace disque pour l'installation de l'image de la machine virtuelle et des données système

Exigences relatives aux types d’instances Amazon EC2

Lorsque vous déployez votre passerelle sur Amazon Elastic Compute Cloud (Amazon EC2), la taille de l'instance doit **`xlarge`**au moins être suffisante pour que votre passerelle fonctionne. Toutefois, pour la famille d'instances optimisée pour le calcul, la taille doit être d'au moins. **`2xlarge`**

> **Note**
>
> L'AMI Storage Gateway est uniquement compatible avec les instances x86 qui utilisent des processeurs Intel ou AMD. Les instances basées sur ARM qui utilisent des processeurs Graviton ne sont pas prises en charge.

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 usage général : type d'instance m5, m6 ou m7. Choisissez une taille d'instance xlarge ou supérieure pour répondre aux exigences en matière de processeur et de RAM Storage Gateway.
- Famille d'instances optimisée pour le calcul : types d'instances c5, c6 ou c7. Choisissez une taille d'instance 2 fois plus grande ou plus pour répondre aux exigences en matière de processeur et de RAM Storage Gateway.
- Famille d'instances optimisée pour la mémoire : types d'instances r5, r6 ou r7. Choisissez une taille d'instance xlarge ou supérieure pour répondre aux exigences en matière de processeur et de RAM Storage Gateway.
- Famille d'instances optimisée pour le stockage : types d'instances i3, i4 ou i7. Choisissez une taille d'instance xlarge ou supérieure pour répondre aux exigences en matière de processeur et de RAM Storage Gateway.

> **Note**
>
> Lorsque vous lancez votre passerelle dans Amazon EC2 et que le type d'instance que vous choisissez prend en charge le stockage éphémère, les disques sont répertoriés automatiquement. Pour plus d'informations sur le stockage d'instance Amazon EC2, consultez la section Stockage d'instance dans le guide de l'utilisateur Amazon EC2.

Besoins de stockage

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

Type de passerelle	Cache (minimum)	Cache (maximum)			
Passerelle de fichier	150 Gio	64 Tio			

> **Note**
>
> Vous pouvez configurer un ou plusieurs disques locaux pour votre cache, dans la limite de leur capacité maximale.
> Lorsque vous ajoutez du cache à une passerelle existante, il est important de créer de nouveaux disques sur votre hôte (hyperviseur ou instance Amazon EC2). Ne modifiez pas la taille des disques existants s'ils ont déjà été alloués en tant que cache.

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 exigences en bande passante du réseau varient en fonction de la quantité de données chargées et téléchargées par la passerelle. Un minimum de 100 Mbits/s 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 votre passerelle sur Amazon EC2 ou utiliser d'autres types de déploiement (y compris sur site) avec des politiques de sécurité réseau qui limitent les plages d' AWS adresses IP. Dans ces cas, votre passerelle peut rencontrer des problèmes de connectivité au service lorsque les valeurs de la plage d' AWS adresses IP changent. Les valeurs de plage d'adresses AWS IP que vous devez utiliser se trouvent dans le sous-ensemble de services Amazon correspondant à la AWS région dans laquelle vous activez votre passerelle. Pour consulter les valeurs des plages d'adresses IP actuelles, consultez Plages d'adresses IP AWS dans le document Références générales AWS.

Rubriques

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

- Autoriser AWS Storage Gateway l'accès par le biais de pare-feux et de routeurs
- Configuration des groupes de sécurité pour votre instance de passerelle Amazon EC2

Exigences relatives aux ports

FSx File Gateway nécessite que des ports spécifiques soient autorisés par le biais de la sécurité de votre réseau pour un déploiement et un fonctionnement réussis. Certains ports sont requis pour toutes les passerelles, tandis que d'autres ne le sont que pour des configurations spécifiques, par exemple lors de la connexion à des points de terminaison VPC.

Pour FSx File Gateway, vous devez utiliser Microsoft Active Directory pour autoriser les utilisateurs du domaine à accéder à un partage de fichiers SMB (Server Message Block). Vous pouvez associer votre passerelle de fichiers à n'importe quel domaine Microsoft Windows valide (résolvable par DNS).

Vous pouvez également utiliser le Directory Service pour créer un AWS Managed Microsoft ADdans le cloud Amazon Web Services. Pour la plupart AWS Managed Microsoft AD des déploiements, vous devez configurer le service DHCP (Dynamic Host Configuration Protocol) pour votre VPC. Pour plus d'informations sur la création d'un jeu d'options DHCP, voir Création d'un ensemble d'options DHCP dans le Guide d'AWS Directory Service administration.

Le tableau suivant répertorie les ports nécessaires et décrit les exigences conditionnelles dans la colonne Remarques.

Exigences de port pour la passerelle de FSx fichiers

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
Navigateur Web	Votre navigateur web	Machine virtuelle Storage Gateway	HTTP TCP	80	✓	✓	✓	Utilisé par les systèmes locaux pour obtenir la clé d'activat

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								ion de Storage Gateway. Le port 80 est utilisé uniquement lors de l'activation d'une appliance Storage Gateway. Une machine virtuelle Storage Gateway ne nécessite pas de port 80 pour être accessible publiquement. Le niveau requis de

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								l'accès au port 80 dépend de la configuration de votre réseau. Si vous activez votre passerelle depuis la console de gestion Storage Gateway, l'hôte depuis lequel vous vous connectez à la console doit avoir accès au port

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								80 de votre passerelle.
Navigateur Web	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	443	✓	✓	✓	AWS Console de gestion (toutes les autres opérations)
DNS	Machine virtuelle Storage Gateway	Serveur DNS (Domain Name Service)	DNS TCP et UDP	53	✓	✓	✓	Utilisé pour la communication entre une machine virtuelle Storage Gateway et le serveur DNS pour la résolution des noms IP.

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
NTP	Machine virtuelle Storage Gateway	Serveur NTP (Network Time Protocol)	TCP et UDP NTP	123	✓	✓	✓	Utilisé par les systèmes sur site pour synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte. Une machine virtuelle Storage Gateway est configurée pour utiliser les serveurs NTP suivants : • 0.amazon.pool.ntp.org

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								• 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org **Note** Non requis pour les passerelles hébergées sur Amazon EC2.

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
Storage Gateway	Machine virtuelle Storage Gateway	Support Point final	SSH TCP	22	✓	✓	✓	Permet d'accéder Support à votre passerelle pour vous aider à résoudre les problèmes liés à la passerelle. Ce port ne doit pas être ouvert pour que votre passerelle fonctionne normalement, mais il doit l'être pour résoudre les

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								problèmes. Pour obtenir la liste des points de terminaison de support, consultez la section points de Support terminaison.
Storage Gateway	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	443	✓	✓	✓	Contrôle de gestion
Amazon CloudFront	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	443	✓	✓	✓	Pour activation

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	443	✓	✓	✓*	Contrôle de gestion *Obligatoire uniquement lors de l'utilisation de points de terminaison VPC
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	1026		✓	✓*	Point final du plan de contrôle *Obligatoire uniquement lors de l'utilisation de points de terminaison VPC

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	1027		✓	✓*	Plan de contrôle Anon (pour activation) *Obligatoire uniquement lors de l'utilisation de points de terminaison VPC
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	1028		✓	✓*	Point de terminaison proxy *Obligatoire uniquement lors de l'utilisation de points de terminaison VPC

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	1031		✓	✓*	Plan de données *Obligatoire uniquement lors de l'utilisation de points de terminaison VPC

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	2222		✓	✓*	Canal de support SSH pour VPCe *Requis uniquement pour ouvrir un canal de support lors de l'utilisation de points de terminaison VPC

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	443	✓	✓	✓*	Contrôle de gestion *Obligatoire uniquement lors de l'utilisation de points de terminaison VPC

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
Client de partage de fichiers	Client de PME	Machine virtuelle Storage Gateway	TCP ou UDP SMBv3	445	✓	✓	✓	Service de session de transfert de données de partage de fichiers. Remplace les ports 137 à 139 pour Microsoft Windows NT et versions ultérieures.
Microsoft	Machine virtuelle Storage Gateway	Serveur Active Directory	NetBIOS UDP	137	✓	✓	✓	Nom du service

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
Microsoft	Machine virtuelle Storage Gateway	Serveur Active Directory	NetBIOS UDP	138	✓	✓	✓	Service de datagramme
Microsoft	Machine virtuelle Storage Gateway	Serveur Active Directory	LDAP TCP ET UDP	389	✓	✓	✓	Connexion client DSA (Directory System Agent)
Microsoft	Machine virtuelle Storage Gateway	Serveur Active Directory	Kerberos TCP et UDP	88	✓	✓	✓	Kerberos
Microsoft	Machine virtuelle Storage Gateway	Serveur Active Directory	Mappeur de Environment/Endpoints de calcul distribués TCP (DCE/EMAP)	135	✓	✓	✓	RPC

Élément de réseau	De	À	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
FSx Connexion Amazon	Machine virtuelle Storage Gateway	FSx pour le serveur de fichiers Windows	TCP ou UDP SMBv3	445	✓	✓	✓	Service de session de partage de fichiers et de transfert de données

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

Chaque appliance matérielle Storage Gateway nécessite les services réseau suivants :

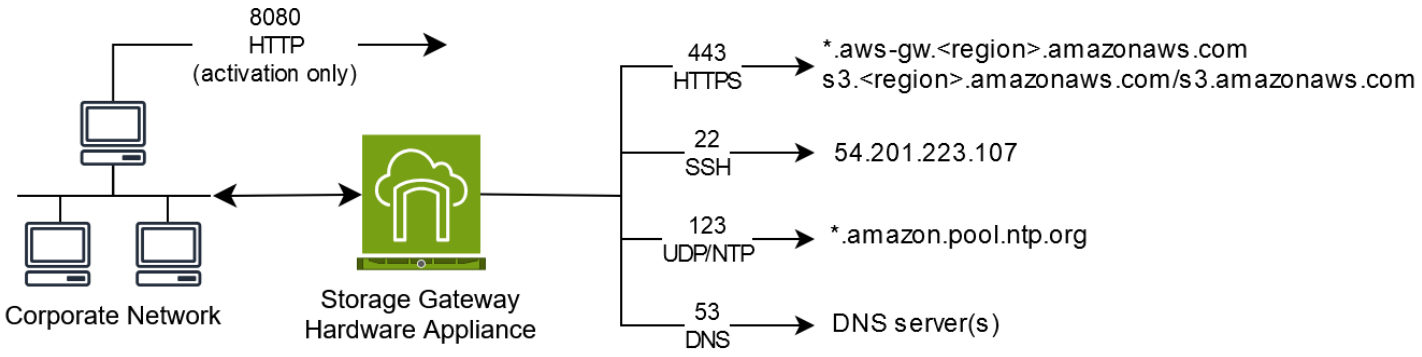
- Accès à Internet : une connexion réseau permanente à Internet via une interface réseau sur le serveur.
- Services DNS : des services DNS qui assurent la communication entre l’appliance matérielle et le serveur DNS.
- Synchronisation horaire : un service de temps Amazon NTP doit être accessible.
- Adresse IP : adresse DHCP ou IPv4 adresse statique attribuée. Vous ne pouvez pas attribuer d' IPv6 adresse.

Cinq ports réseau physiques se trouvent à l'arrière du serveur Dell PowerEdge R640. 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.

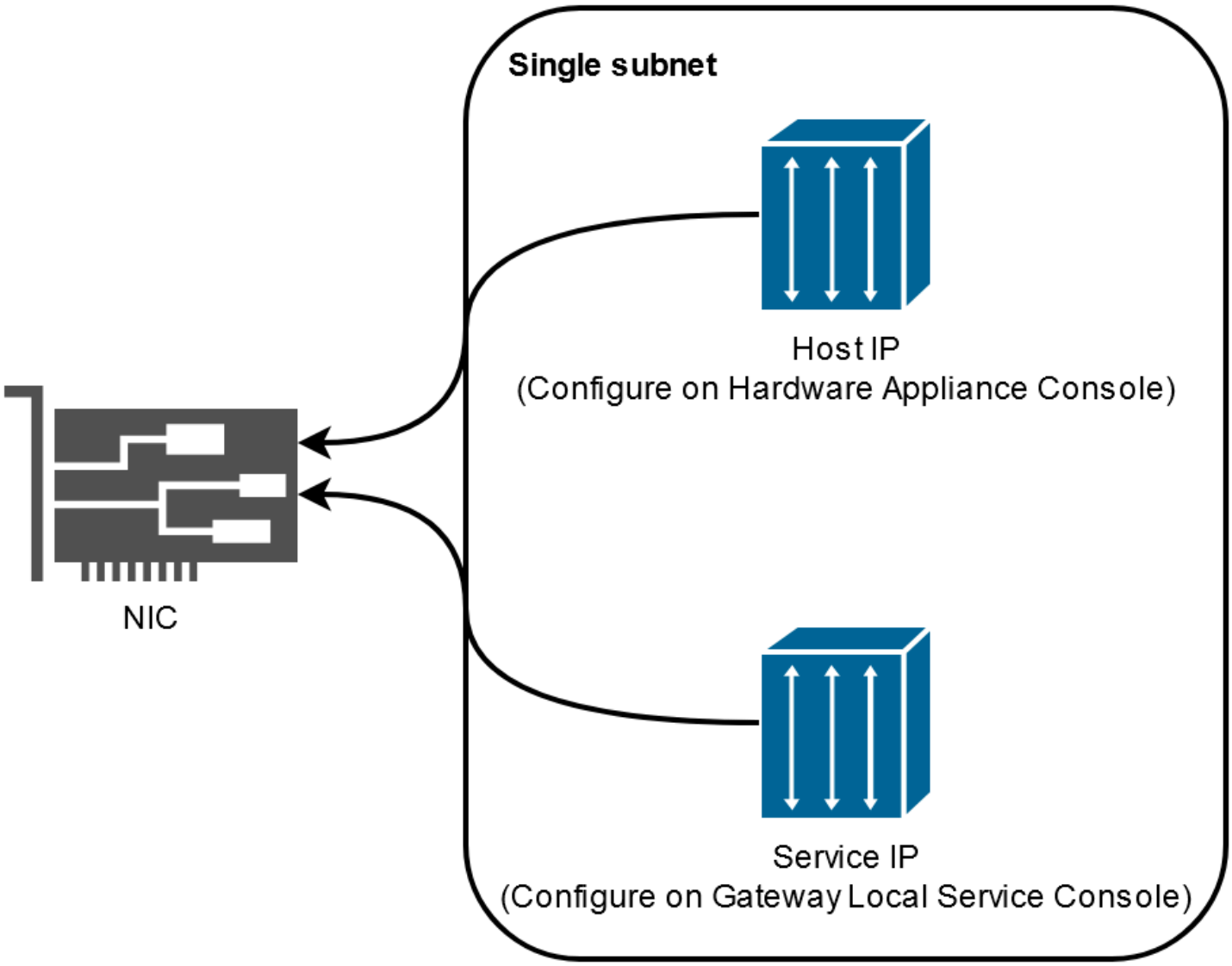
Protocole	Port	Direction	Source	Destination	Usage
SSH	22	Sortant	Appliance matérielle	`54.201.223.107`	canal de support
DNS	53	Sortant	Appliance matérielle	Serveurs DNS	Résolution de noms
UDP/NTP	123	Sortant	Appliance matérielle	`*.amazon.pool.ntp.org`	Synchronisation du temps
HTTPS	443	Sortant	Appliance 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 de plus amples informations, veuillez consulter Configuration des paramètres réseau de l'appliance matérielle.

> **Note**
>
> Pour une illustration montrant l'arrière du serveur avec ses ports, reportez-vous àInstallation physique de votre appliance matérielle.

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 plus d'informations sur l'activation et la configuration d'une appliance matérielle, consultezUtilisation de l'appliance matérielle AWS Storage Gateway.

Autoriser AWS Storage Gateway l'accès par le biais de pare-feux et de routeurs

Votre passerelle doit accéder aux points de terminaison du service Storage Gateway suivants pour communiquer avec AWS. Lors de la configuration de la passerelle, sélectionnez le type de point de terminaison de votre passerelle en fonction de votre environnement réseau. 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 AWS pour ces points de terminaison de service.

> **Note**
>
> Si vous configurez des points de terminaison VPC privés que votre Storage Gateway utilisera pour la connexion et le transfert de données vers et depuis AWS, votre passerelle n'a pas besoin d'accéder à l'Internet public. Pour plus d'informations, consultez Activation d'une passerelle dans un cloud virtuel privé.

> **Important**
>
> Remplacez *region* dans les exemples de point de terminaison suivants par la Région AWS chaîne appropriée pour votre passerelle, telle que`us-west-2`.
> *amzn-s3-demo-bucket*Remplacez-le par le nom réel du compartiment Amazon S3 de votre déploiement. Vous pouvez également utiliser un astérisque (*) à la place de *amzn-s3-demo-bucket* pour créer une entrée générique dans vos règles de pare-feu, ce qui permettra de répertorier le point de terminaison du service pour tous les noms de compartiment.
> Si vos passerelles sont déployées aux États-Unis d'Amérique ou au Canada et nécessitent des connexions aux terminaux conformes à la norme FIPS (Federal Information Processing Standard), remplacez-les par. Régions AWS *s3* `s3-fips`

Types de point de terminaison

Points de terminaison standard

Ces points de terminaison prennent en charge IPv4 le trafic entre votre appliance de passerelle et AWS.

Le point de terminaison de service suivant est requis par toutes les passerelles pour les opérations head-bucket.

```
bucket-name.s3.region.amazonaws.com:443
```

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

```
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
```

Outre les points de terminaison du service Storage Gateway et Amazon S3, Storage Gateway nécessite VMs également un accès réseau aux serveurs NTP suivants :

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

Pour plus d'informations sur les points de terminaison pris en charge Régions AWS et les points de terminaison de service, consultez Storage Gateway dans le Références générales AWS.

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

Dans AWS 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 devez autoriser les instances à se connecter à la passerelle depuis l'extérieur de son groupe de sécurité, nous vous recommandons d'autoriser les connexions uniquement sur le port 80 (pour l'activation).

- Si vous souhaitez activer votre passerelle depuis 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.
- N'autorisez l'accès au port 22 que si vous l'utilisez à Support des fins de dépannage. Pour de plus amples informations, veuillez consulter Vous souhaitez aider Support à résoudre les problèmes liés à votre passerelle Amazon EC2.

Hyperviseurs pris en charge et exigences pour l'hôte

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

> **Note**
>
> Le mode de démarrage UEFI avec démarrage sécurisé désactivé (loader_secure=no) est requis pour File Gateway 2.x, Volume Gateway 3.x et Tape Gateway 3.x. Un fichier XML est fourni avec chaque téléchargement de qcow en tant que configuration de configuration rapide.

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

- VMware ESXi Hyperviseur (version 7.0 ou 8.0) : pour cette configuration, vous avez également besoin d'un client VMware vSphere pour vous connecter à l'hôte.
- Hyperviseur Microsoft Hyper-V (2019, 2022 ou 2025) : pour cette configuration, vous avez besoin d'un gestionnaire Microsoft Hyper-V sur un ordinateur client Microsoft Windows pour vous connecter à l'hôte.
- Machine virtuelle de noyau Linux (KVM) – Une technologie de virtualisation libre et open-source. KVM est inclus dans toutes les versions de Linux 2.6.20 et versions ultérieures. Storage Gateway est testé et pris en charge pour les CentOS/RHEL distributions 7.7, RHEL 8.6, 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. Reportez-vous au fichier aws-storage-gateway .xml fourni pour les configurations de démarrage suggérées. Le mode de démarrage UEFI avec démarrage sécurisé désactivé (loader_secure=no) est requis pour File Gateway 2.x, Volume Gateway 3.x et Tape Gateway 3.x.

- Nutanix AHV (Acropolis Hypervisor) à partir de la version 10.0.1.1 : plate-forme de virtualisation basée sur KVM intégrée à la solution d'infrastructure hyperconvergée (HCI) Nutanix.
- Amazon Instance EC2 – Storage Gateway fournit une Amazon Machine Image (AMI) qui contient l'image de la machine virtuelle de la passerelle. Pour obtenir des informations sur le déploiement d'une passerelle sur Amazon EC2, consultez Déployer un hôte Amazon EC2 par défaut pour File Gateway FSx.
- Storage Gateway Hardware Appliance : Storage Gateway fournit une appliance matérielle physique comme option de déploiement sur site pour les sites dotés d'une infrastructure de machines virtuelles 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 la machine virtuelle de la passerelle fonctionne mal, activez une nouvelle passerelle et récupérez vos données pour cette passerelle. Pour plus d'informations, consultez Récupération après l'arrêt inattendu d'une machine virtuelle. Storage Gateway ne prend pas en charge la mémoire dynamique ni la mémoire virtuelle ballon.

Clients SMB pris en charge pour File Gateway

File Gateway prend en charge les clients SMB (Service Message Block) suivants :

- Microsoft Windows Server 2008 R2 et versions ultérieures
- Bureau Windows versions : 10, 8 et 7.
- Windows Terminal Server s'exécutant sur Windows Server 2008 et versions ultérieures

> **Note**
>
> Le chiffrement par blocs de messages du serveur nécessite des clients compatibles avec les dialectes SMB v3.x.

Opérations de système de fichiers prises en charge pour File Gateway

Votre client SMB peut écrire, lire, supprimer et tronquer des fichiers. Lorsque les clients envoient des écritures à Storage Gateway, celui-ci écrit dans le cache local de manière synchrone. Il écrit ensuite sur Amazon de FSx manière 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 extraites via Amazon FSx sous forme de cache de lecture.

Les lectures et écritures sont optimisées de sorte que seules les parties modifiées ou demandées sont transférées via la passerelle. Supprime et supprime des fichiers d'Amazon FSx.

Gestion des disques locaux pour votre passerelle

La machine virtuelle de la passerelle utilise les disques locaux que vous allouez sur site pour le tampon et le stockage. Une passerelle de fichiers que vous créez sur une instance Amazon EC2 utilisera les volumes Amazon EBS comme disques locaux. Vous décidez du nombre et de la taille des disques que vous souhaitez allouer à la passerelle. La passerelle utilise le stockage de cache que vous allouez pour fournir un accès à faible latence aux données que vous avez récemment consultées. Le stockage en cache fait office de stockage durable sur site pour les données en attente de téléchargement vers Amazon FSx. Les passerelles de fichiers nécessitent au moins un disque de 150 GiB pour être utilisées comme cache. Après la configuration initiale et le déploiement de votre passerelle, vous pouvez ajouter des disques supplémentaires pour le stockage en cache à mesure que la charge de travail augmente. Cette section contient les rubriques suivantes, qui décrivent les concepts et les procédures liés à la gestion des disques locaux.

Rubriques

- Déterminer la quantité de stockage du disque local- Découvrez comment déterminer le nombre et la taille des disques de cache locaux à allouer à votre passerelle de fichiers.

- Configuration d'un stockage de cache supplémentaire- Découvrez comment augmenter la capacité de stockage du cache de votre passerelle de fichiers en fonction de l'évolution des besoins de votre application.
- Utilisation du stockage éphémère avec les passerelles EC2- Découvrez comment éviter les pertes de données lors de l'utilisation du stockage sur disque éphémère avec File Gateway.

Déterminer la quantité de stockage du disque local

Lorsque vous déployez une Gateway, considérez la quantité de disque cache à allouer. File Gateway utilise l'algorithme le moins récemment utilisé pour expulser automatiquement les données du cache. Le cache d'une est partagé entre tous les partages de fichiers de cette passerelle. Si vous avez plusieurs partages actifs, il est important de noter qu'une utilisation intensive d'un partage peut avoir un impact sur la quantité de ressources de cache auxquelles un autre partage a accès, ce qui peut avoir un impact sur les performances.

Lorsque vous déterminez la quantité de disque cache dont vous avez besoin pour une charge de travail donnée, il est important de noter que vous pouvez toujours ajouter un disque de cache à votre passerelle (dans la limite des quotas actuels de la passerelle de fichiers), mais que vous ne pouvez pas réduire le cache pour une passerelle donnée. Vous pouvez effectuer une analyse de base sur le jeu de données pour déterminer la bonne quantité de disque cache, mais il n'existe aucun moyen de déterminer exactement la quantité de données « chaudes » devant être stockées localement, par rapport à « froides » et pouvant être hiérarchisées dans le cloud. Les charges de travail évoluent au fil du temps, et la Gateway offre flexibilité et élasticité en fonction de la quantité de ressources pouvant être consommées. La quantité de cache pouvant toujours être augmentée, l'approche la plus rentable est souvent de commencer par une petite quantité et de l'augmenter selon les besoins.

Vous pouvez utiliser une estimation initiale de 150 GiB pour provisionner des disques pour le stockage en cache lors de la configuration de la passerelle. Vous pouvez ensuite utiliser les métriques CloudWatch opérationnelles d'Amazon pour surveiller l'utilisation du stockage en cache et allouer davantage de stockage selon les besoins à l'aide de la console. Pour plus d’informations sur les métriques et la configuration des alarmes, consultez Performances et optimisation.

> **Note**
>
> Les ressources de stockage physiques sous-jacentes sont représentées sous la forme d'un magasin de données dans VMware. Lorsque vous déployez la machine virtuelle de la passerelle, vous choisissez une banque de données sur laquelle stocker les fichiers de la

machine virtuelle. Lorsque vous provisionnez un disque local (par exemple, pour l'utiliser comme stockage de cache), vous avez la possibilité de stocker le disque virtuel dans le même magasin de données que la machine virtuelle ou dans un autre magasin de données. Si vous disposez de plusieurs banques de données, nous vous recommandons vivement de choisir une banque de données pour le stockage en cache. Un magasin de données soutenu par un seul disque physique sous-jacent peut entraîner des performances médiocres dans certains cas lorsqu'il est utilisé pour sauvegarder à la fois le stockage en cache. Cela est également vrai si la sauvegarde est une configuration RAID moins performante, telle que. RAID1

Configuration d'un stockage de cache supplémentaire

À mesure que les besoins de votre application évoluent, vous pouvez augmenter la capacité de stockage du cache de la passerelle. Vous pouvez augmenter la capacité de stockage de votre passerelle sans interrompre ses fonctionnalités ni provoquer d'interruption. Lorsque vous ajoutez plus de capacité, vous le faites avec la machine virtuelle de la passerelle activée.

> **⚠ Important**
>
> Lorsque vous ajoutez du cache à une passerelle existante, vous devez créer de nouveaux disques sur l'hyperviseur hôte de la passerelle ou sur l'instance Amazon EC2. Ne supprimez pas ou ne modifiez pas la taille des disques existants qui ont déjà été alloués en tant que cache.

Pour configurer un stockage de cache supplémentaire pour votre passerelle

1. Allouez un ou plusieurs nouveaux disques sur votre hyperviseur hôte de passerelle ou sur votre instance Amazon EC2. Pour obtenir des informations sur la façon d'allouer un disque dans un hyperviseur, consultez la documentation de votre hyperviseur. Pour obtenir des informations sur l'allocation de volumes pour une instance Amazon EC2, consultez les Volumes Amazon EBS dans le Guide de l'utilisateur pour les instances Linux Amazon Elastic Compute Cloud. Dans les étapes suivantes, vous allez configurer ce disque comme stockage en cache.
2. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
3. Dans le volet de navigation, choisissez Passerelles.

4. Recherchez votre passerelle et sélectionnez-la dans la liste.
5. Dans le menu Actions, choisissez Configurer le stockage en cache.
6. Dans la section Configurer le stockage en cache, identifiez les disques que vous avez provisionnés. Si vos disques n'apparaissent pas, cliquez sur l'icône d'actualisation pour actualiser la liste. Pour chaque disque, choisissez Cache dans le menu déroulant Alloué à.

> **Note**
>
> Le cache est la seule option disponible pour allouer des disques sur une passerelle de fichiers.

7. Choisissez Enregistrer les modifications pour enregistrer les paramètres de configuration.

Utilisation du stockage éphémère avec les passerelles EC2

Nous ne recommandons pas l'utilisation de disques éphémères pour le stockage en cache sur les passerelles de FSx fichiers.

Les disques éphémères fournissent un stockage temporaire au niveau des blocs pour votre instance Amazon EC2. 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 éphémères sont automatiquement répertoriés. Vous pouvez sélectionner l'un des disques pour stocker les données du cache de votre passerelle. Pour plus d'informations, consultez le magasin d'instances Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Les données que les applications écrivent sur la passerelle sont stockées de manière synchrone dans le cache des disques éphémères, puis téléchargées de manière asynchrone vers un stockage durable dans FSx pour Windows File Server. Si l'instance Amazon EC2 est arrêtée après l'écriture des données dans le stockage éphémère, mais avant qu'un chargement asynchrone ne se produise, toutes les données qui n'ont pas encore été téléchargées sur pour Windows File Server peuvent être perdues.

> **Important**
>
> Si vous utilisez un stockage éphémère et que vous arrêtez et démarrez votre passerelle Amazon EC2, la passerelle sera hors ligne de manière permanente. Cela se produit parce que le disque de stockage physique est remplacé. Il n'existe aucune solution à ce problème.

La seule solution consiste à supprimer la passerelle et à en activer une nouvelle sur une nouvelle instance EC2.

Utilisation de l'appliance matérielle AWS Storage Gateway

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

L'appliance matérielle AWS Storage Gateway est une appliance matérielle physique sur laquelle le logiciel Storage Gateway est préinstallé sur une configuration de serveur validée. Vous pouvez gérer les appliances matérielles de votre déploiement depuis la page de présentation des appliances matérielles de la AWS Storage Gateway console.

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 l'appliance matérielle à votre Compte AWS. Après activation, votre appliance matérielle apparaît dans la console sur la page de présentation de l'appliance matérielle. Vous pouvez configurer l'appliance matérielle en tant que passerelle de fichiers S3, passerelle de FSx fichiers, passerelle de bande ou passerelle de volume. La procédure que vous utilisez pour déployer ces types de passerelles sur une appliance matérielle est la même que sur une plate-forme virtuelle.

Pour obtenir la liste des appareils pris en charge pour Régions AWS lesquels l'appliance matérielle AWS Storage Gateway est disponible pour activation et utilisation, consultez la section Régions de l'appliance matérielle AWS Storage Gateway dans le Références générales AWS.

Dans les sections qui suivent, vous trouverez des instructions sur la façon de configurer, de monter en rack, d'alimenter, de configurer, d'activer, de lancer, d'utiliser et de supprimer un dispositif matériel AWS Storage Gateway.

Rubriques

- Configuration de votre appliance matérielle AWS Storage Gateway
- Installation physique de votre appliance matérielle

- Accès à la console de l'appliance matérielle
- Configuration des paramètres réseau de l'appliance matérielle
- Activation AWS de votre appliance matérielle Storage Gateway
- Création d'une passerelle sur votre appliance matérielle
- Configuration d'une adresse IP de passerelle sur l'appliance matérielle
- Suppression du logiciel de passerelle de votre appliance matérielle
- Suppression AWS de votre appliance matérielle Storage Gateway

Configuration de votre appliance matérielle AWS Storage Gateway

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Après avoir reçu votre appliance matérielle Storage Gateway, vous utilisez la console locale de l'appliance matérielle pour configurer le réseau afin de fournir une connexion permanente à votre appliance AWS et de l'activer. L'activation associe votre appliance au AWS compte utilisé lors du processus d'activation. Une fois l'appliance activée, vous pouvez lancer une passerelle de fichiers, une passerelle de FSx fichiers, une passerelle de bande ou une passerelle de volume S3 depuis la console Storage Gateway.

Installation et configuration de votre appliance matérielle

1. Montez sur rack l’appliance et raccordez-la au secteur électrique et au réseau. Pour de plus amples informations, veuillez consulter Installation physique de votre appliance matérielle.
2. Définissez les adresses du protocole Internet version 4 (IPv4) pour l'appliance matérielle (l'hôte). Pour de plus amples informations, veuillez consulter Configuration des paramètres réseau de l'appliance matérielle.

3. Activez l'appliance matérielle sur la page de présentation de l'appliance matérielle de la console dans AWS la région de votre choix. Pour de plus amples informations, veuillez consulter Activation AWS de votre appliance matérielle Storage Gateway.
4. Créez une passerelle sur votre appliance matérielle. Pour de plus amples informations, veuillez consulter Création de votre passerelle.

   La configuration des passerelles sur l'appliance matérielle s'effectue de la même manière que celle des passerelles sur VMware ESXi, Microsoft Hyper-V, la machine virtuelle de noyau Linux (KVM) 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. Cela permet d'obtenir un cache plus important pour un accès à faible latence aux données entrantes AWS. Si vous avez commandé le modèle 5 To, vous pouvez augmenter le stockage utilisable à 12 To en achetant cinq disques SSD de SSDs 1,92 To.

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 faire passer le stockage utilisable sur l'appliance à 12 To, procédez comme suit :

1. Réinitialisez l'appliance matérielle à ses paramètres d'usine. Contactez AWS le Support pour obtenir des instructions sur la procédure à suivre.
2. Ajoutez cinq 1,92 To SSDs à l'appliance.

Options de carte d'interface réseau

Selon le modèle d'appareil que vous avez commandé, il peut être livré avec une carte réseau 10G-Base-T RJ45 en cuivre ou 10G DA/SFP+.

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

Installation physique de votre appliance matérielle

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Votre appareil a un facteur de format 1U et s'adapte à un rack de 19 pouces conforme aux normes de la Commission électrotechnique internationale (CEI).

Conditions préalables

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

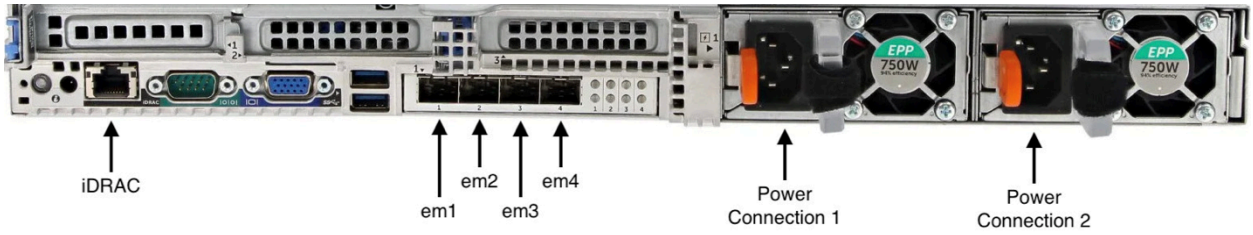
- Câble électriques : un obligatoire, deux recommandés.
- Câblage réseau pris en charge (en fonction de la carte d'interface réseau (NIC) incluse dans l'appliance matérielle). Câble DAC en cuivre Twinax, module optique SFP+ (compatible Intel) ou émetteur-récepteur cuivre SFP vers Base-T.
- Clavier et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

> **Note**
>
> Avant d'exécuter la procédure ci-dessous, vérifiez que vous respectez toutes les exigences requises pour l'appareil Storage Gateway Hardware Appliance, qui sont décrites dans Exigences en matière de mise en réseau et de pare-feu pour l'appliance matérielle Storage Gateway.

Pour installer physiquement votre appliance matérielle

1. Déballez votre appliance matérielle et suivez les instructions contenues dans la boîte pour monter le serveur en rack.

L'image suivante montre l'arrière de l'appliance matérielle avec des ports pour connecter l'alimentation, l'Ethernet, le moniteur, le clavier USB et l'iDRAC.
dispositif matériel, un à l'arrière, avec étiquettes de connexion réseau et d'alimentation.



dispositif matériel, un à l'arrière, avec étiquettes de connexion réseau et d'alimentation.

2. Branchez au secteur chacun des deux blocs d’alimentation. Il est possible de le brancher sur un seul câble d'alimentation, mais nous recommandons de le brancher aux deux blocs d'alimentation pour des raisons de redondance.
3. 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.

4. Branchez le clavier et le moniteur.
5. Mettez le serveur sous tension en appuyant sur le bouton Power (Marche/arrêt) sur le panneau avant, comme l’indique l’image suivante.
face avant de l’appliance matérielle avec étiquette du bouton d’alimentation.

face avant de l’appliance matérielle avec étiquette du bouton d’alimentation.

Étape suivante

Accès à la console de l'appliance matérielle

Accès à la console de l'appliance matérielle

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Lorsque vous allumez votre appliance matérielle, la console de l'appliance matérielle apparaît sur le moniteur. La console de l'appliance matérielle présente une interface utilisateur spécifique AWS que vous pouvez utiliser pour définir un mot de passe administrateur, configurer les paramètres réseau initiaux et ouvrir un canal d'assistance pour AWS.

Pour utiliser la console de l'appliance matérielle, entrez du texte à l'aide du clavier et utilisez les `Left Arrow` touches Up `DownRight`,, et pour vous déplacer sur l'écran dans la direction indiquée. 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.

La première fois que la console de l'appliance matérielle apparaît, la page de bienvenue s'affiche et vous êtes invité à définir un mot de passe pour le compte utilisateur administrateur avant de pouvoir accéder à la console.

Pour définir un mot de passe administrateur

- À l'invite Veuillez définir votre mot de passe de connexion, procédez comme suit :

  a. Pour Set Password (Définir un mot de passe), entrez un mot de passe, puis appuyez sur `Down arrow`.

  b. Pour Confirm (Confirmer), entrez à nouveau votre mot de passe, puis choisissez Save Password (Enregistrer le mot de passe).

Après avoir défini votre mot de passe, la page d'accueil de la console matérielle apparaît. La page d'accueil affiche les informations réseau pour les interfaces réseau em1, em2, em3 et em4, et propose les options de menu suivantes :

- Configuration du réseau
- Ouvrez la console de service
- Modifier le mot de passe
- Déconnexion
- Ouvrez la console de support

Étape suivante

Configuration des paramètres réseau de l'appliance matérielle

Configuration des paramètres réseau de l'appliance matérielle

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Une fois que l'appliance matérielle a démarré et que vous avez défini votre mot de passe d'utilisateur administrateur dans la console matérielle comme décrit dansAccès à la console de l'appliance matérielle, suivez la procédure suivante pour configurer les paramètres réseau afin que votre appliance matérielle puisse se connecter à AWS.

Pour définir une adresse réseau

1. Sur la page d'accueil, choisissez Configurer le réseau, puis appuyez sur`Enter`. La page Configurer le réseau apparaît. La page Configurer le réseau affiche les informations IP et DNS pour chacune des 4 interfaces réseau de l'appliance matérielle et inclut des options de menu permettant de configurer les adresses DHCP ou statiques pour chacune d'elles.

2. Pour l'interface em1, effectuez l'une des opérations suivantes :

   - Choisissez DHCP et appuyez `Enter` pour utiliser l' IPv4 adresse attribuée par votre serveur DHCP (Dynamic Host Configuration Protocol) à votre port réseau physique.

     Notez cette adresse pour une utilisation ultérieure lors de l'étape d'activation.

   - Choisissez Static et appuyez `Enter` pour configurer une IPv4 adresse statique.

     Entrez une adresse IP, un masque de sous-réseau, une passerelle et une adresse de serveur DNS valides pour l'interface réseau em1.

     Lorsque vous avez terminé, choisissez Enregistrer, puis appuyez `Enter` pour enregistrer la configuration.

> **Note**
>
> Vous pouvez utiliser cette procédure pour configurer d'autres interfaces réseau en plus de em1. Si vous configurez d'autres interfaces, elles doivent fournir la même connexion permanente aux AWS points de terminaison répertoriés dans les exigences.
> La liaison réseau et le protocole LACP (Link Aggrégation Control Protocol) ne sont pas pris en charge par l'appliance matérielle ni par Storage Gateway.
> Il est déconseillé de configurer plusieurs interfaces réseau sur le même sous-réseau, car cela peut parfois entraîner des problèmes de routage.

Pour vous déconnecter de la console du matériel

1. Choisissez Retour et appuyez sur `Enter` ce bouton pour revenir à la page d'accueil.
2. Choisissez Déconnexion et appuyez sur cette touche `Enter` pour revenir à la page d'accueil.

Étape suivante

Activation AWS de votre appliance matérielle Storage Gateway

Activation AWS de votre appliance matérielle Storage Gateway

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Après avoir configuré votre adresse IP, vous devez saisir cette adresse IP sur la page Matériel de la AWS Storage Gateway console pour activer votre appliance matérielle. Le processus d'activation enregistre l'appliance sur votre AWS compte.

Vous pouvez choisir d'activer votre appliance matérielle dans n'importe laquelle des solutions prises en charge Régions AWS. Pour obtenir la liste des régions prises en charge Régions AWS, consultez la section Régions de l'appliance matérielle Storage Gateway dans le Références générales AWS.

Pour activer votre appliance matérielle AWS Storage Gateway

1. Ouvrez la Console de gestion AWS Storage Gateway et connectez-vous avec les informations d’identification du compte à utiliser pour activer votre matériel.

   > **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. Le menu de navigation sur la gauche de la page, choisissez Matériel.
3. Choisissez Activer l’appliance.
4. Pour Adresse IP, entrez l’adresse IP que vous avez configurée pour votre appliance matérielle, puis choisissez Connexion.

Pour plus d'informations sur la configuration de l'adresse IP, consultez Configuration des paramètres réseau.

5. Pour Nom, entrez un nom pour votre appliance matérielle. Les noms peuvent comporter jusqu'à 255 caractères. La barre oblique n'est pas autorisée.
6. Pour Fuseau horaire de l'appliance matérielle, entrez le fuseau horaire local à partir duquel la majeure partie de la charge de travail de la passerelle sera générée, puis choisissez Suivant.

   Le fuseau horaire commande le moment où les mises à jour du matériel sont effectuées, soit à 2 h 00, heure locale. Idéalement, si le fuseau horaire est correctement défini, les mises à jour auront lieu par défaut en dehors des heures ouvrées locales.
7. Passez en revue les paramètres d'activation dans la section détaillée de l'appliance matérielle. Pour revenir en arrière et apporter des modifications, sélectionnez Précédent. Sinon, choisissez Activer pour terminer l'activation.

Une bannière s'affiche sur la page Présentation de l'appliance matérielle, indiquant que l'appliance matérielle a été correctement activée.

À ce stade, l'appliance est associée à votre compte. L'étape suivante consiste à configurer et à lancer une passerelle de fichiers, une passerelle de FSx fichiers, une passerelle de bande ou une passerelle de volume S3 sur le nouveau dispositif.

Étape suivante

Création d'une passerelle sur votre appliance matérielle

Création d'une passerelle sur votre appliance matérielle

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Vous pouvez créer une passerelle de fichiers, une passerelle de FSx fichiers, une passerelle de bande ou une passerelle de volume S3 sur n'importe quelle appliance matérielle AWS Storage Gateway de votre déploiement.

Pour créer une passerelle sur votre appliance matérielle

1. Connectez-vous à la console Storage Gateway AWS Management Console et ouvrez-la https://console.aws.amazon.com/storagegateway/chez vous.
2. Suivez les procédures décrites dans Creating Your Gateway pour configurer, connecter et configurer le type de Storage Gateway que vous souhaitez déployer.

Lorsque vous avez terminé de créer votre passerelle dans la console Storage Gateway, le logiciel Storage Gateway s'installe automatiquement sur l'appliance matérielle. Si vous utilisez le protocole DHCP (Dynamic Host Configuration Protocol), l'affichage d'une passerelle comme étant en ligne dans la console peut prendre de 5 à 10 minutes. Pour attribuer une adresse IP statique à votre passerelle installée, consultez Configuration d'une adresse IP pour la passerelle .

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 de passerelle sur l'appliance matérielle

Configuration d'une adresse IP de passerelle sur l'appliance matérielle

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

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 sur cette dernière, 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 depuis la console locale de passerelle pour cette passerelle. Vos applications (telles que votre client NFS ou SMB) se connectent à cette adresse IP. Vous pouvez accéder à la console locale de la passerelle depuis la console de l'appliance matérielle à l'aide de l'option Open Service Console.

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

1. Sur la console matérielle, choisissez Open Service Console, puis appuyez sur ce bouton `Enter` pour ouvrir la page de connexion de la console locale de la passerelle.
2. La page de connexion de la console AWS Storage Gateway locale vous invite à vous connecter pour modifier la configuration de votre réseau et d'autres paramètres.

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

   > **Note**
   >
   > Nous vous recommandons de modifier le mot de passe par défaut en saisissant le chiffre correspondant à la Console de passerelle dans le menu principal Activation de l'appliance AWS - Configuration, puis en exécutant la commande `passwd`. Pour plus d'informations sur l'exécution de la commande, consultez Exécution des commandes Storage Gateway sur la console locale. Vous pouvez également définir le mot de passe depuis la console Storage Gateway. Pour de plus amples informations, veuillez consulter Définition du mot de passe de la console locale depuis la console Storage Gateway.

3. La page Activation de l'AWS appliance - Configuration inclut les options de menu suivantes :

   - Configuration du proxy HTTP/SOCKS
   - Configuration réseau
   - Testez la connectivité réseau
   - Afficher la vérification des ressources du système
   - Gestion du temps du système
   - Informations sur la licence
   - Invite de commande

> **Note**
>
> Certaines options apparaissent uniquement pour des types de passerelles ou des plateformes hôtes spécifiques.

Entrez le chiffre correspondant pour accéder à la page de configuration réseau.

4. Procédez de l'une des manières suivantes pour configurer l'adresse IP de la passerelle :

   - Pour utiliser l'adresse IP attribuée par votre serveur DHCP (Dynamic Host Configuration Protocol), entrez le chiffre correspondant pour Configurer le DHCP, puis entrez des informations de configuration DHCP valides sur la page suivante.
   - Pour attribuer une adresse IP statique, entrez le chiffre correspondant pour Configurer une adresse IP statique, puis entrez une adresse IP et des informations DNS valides sur la page suivante.

   > **Note**
   >
   > L'adresse IP que vous spécifiez ici doit se trouver sur le même sous-réseau que l'adresse IP utilisée lors de l'activation de l'appliance matérielle.

Pour quitter la console locale de la passerelle

- Appuyez sur la séquence de touches `Crtl+]` (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.

Une fois que votre appliance matérielle est activée et configurée, votre appliance s'affiche dans la console. Vous pouvez maintenant poursuivre la procédure d'installation et de configuration de votre passerelle dans la console Storage Gateway. Pour obtenir des instructions, veuillez consulter Configuration de votre Amazon FSx File Gateway.

Suppression du logiciel de passerelle de votre appliance matérielle

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Si vous n'avez plus besoin d'une Storage Gateway spécifique que vous avez déployée sur une appliance matérielle, vous pouvez supprimer le logiciel de passerelle de l'appliance matérielle. Après avoir supprimé le logiciel de passerelle, vous pouvez choisir de déployer une nouvelle passerelle à sa place ou de supprimer l'appliance matérielle elle-même de la console Storage Gateway. Pour supprimer un logiciel de passerelle de votre appliance matérielle, utilisez la procédure suivante.

Pour supprimer une passerelle d’une appliance matérielle

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Choisissez Matériel dans le volet de navigation sur le côté gauche de la page de console, puis choisissez le nom du dispositif matériel dont vous souhaitez supprimer le logiciel de passerelle.
3. Dans le menu déroulant Actions, choisissez Supprimer la passerelle.

   La boîte de dialogue de confirmation s’affiche.
4. Vérifiez que vous souhaitez supprimer le logiciel de passerelle de l'appliance matérielle spécifiée, puis tapez le mot `remove` dans la zone de confirmation.
5. Choisissez Supprimer pour supprimer définitivement le logiciel de passerelle.

   > **Note**
   >
   > Après avoir supprimé le logiciel de passerelle, vous ne pouvez pas annuler l’action. 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 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 AWS de votre appliance matérielle Storage Gateway

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Si vous n'avez plus besoin d'une appliance matérielle AWS Storage Gateway que vous avez déjà activée, vous pouvez la supprimer complètement de votre AWS compte.

> **Note**
>
> Pour déplacer votre appliance vers un autre AWS compte Région AWS, vous devez d'abord la supprimer en suivant la procédure suivante, puis ouvrir le canal d'assistance de la passerelle et contacter Support pour effectuer une réinitialisation logicielle. Pour plus d'informations, voir Activer l' Support accès pour résoudre les problèmes liés à votre passerelle hébergée sur site.

Pour supprimer votre appliance matérielle

1. Si vous avez installé une passerelle sur l'appliance matérielle, vous devez d'abord supprimer la passerelle avant de pouvoir supprimer l'appliance. Pour obtenir des instructions sur la suppression d'une passerelle de votre appliance matérielle, consultez Suppression du logiciel de passerelle de votre appliance matérielle.

2. Sur la page Matériel de la console Storage Gateway, choisissez l’appliance matérielle que vous souhaitez supprimer.
3. Pour Actions, choisissez Delete Appliance (Supprimer l’appliance). La boîte de dialogue de confirmation s’affiche.
4. Vérifiez que vous souhaitez supprimer l’appliance matérielle spécifiée, puis tapez le mot supprimer dans le champ de confirmation et choisissez Supprimer.

   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.

Création de votre passerelle

Les sections de présentation de cette page fournissent un résumé détaillé du fonctionnement du processus de création de Storage Gateway. Pour les step-by-step procédures de création d'un type spécifique de passerelle à l'aide de la console Storage Gateway, consultez les rubriques suivantes :

- Création et activation d’une passerelle de fichiers Amazon S3
- Création et activation d'un Amazon FSx File Gateway
- Création et activation d'une passerelle de bande
- Création et activation d'une passerelle de volume

> **Important**
>
> Amazon FSx File Gateway n'est plus disponible pour les nouveaux clients. Les clients existants de FSx File Gateway peuvent continuer à utiliser le service normalement. Pour des fonctionnalités similaires à FSx File Gateway, consultez ce billet de blog.

Présentation - Activation de la passerelle

L'activation de la passerelle implique de configurer votre passerelle, de la connecter à AWS, puis de revoir vos paramètres et de l'activer.

Configuration d’une passerelle

Pour configurer Storage Gateway, vous devez d’abord choisir le type de passerelle que vous souhaitez créer et la plateforme hôte sur laquelle vous allez exécuter l’appliance virtuelle de la passerelle. Vous téléchargez ensuite le modèle d’appliance virtuelle de passerelle pour la plateforme de votre choix et vous le déployez dans votre environnement sur site. Vous pouvez également déployer votre Storage Gateway en tant qu'appliance matérielle physique que vous commandez auprès de votre revendeur préféré, ou en tant qu'instance Amazon EC2 dans AWS votre environnement cloud. Lorsque vous déployez l’appliance de passerelle, vous allouez de l’espace disque physique local sur l’hôte de virtualisation.

Connect à AWS

L’étape suivante consiste à connecter votre passerelle à AWS. Pour ce faire, vous devez d'abord choisir le type de point de terminaison de service que vous souhaitez utiliser pour les communications entre le dispositif virtuel de passerelle et les AWS services dans le cloud. Ce point de terminaison peut être accessible depuis l’Internet public ou uniquement depuis votre Amazon VPC, où vous avez le contrôle total de la configuration de sécurité du réseau. Vous spécifiez ensuite l’adresse IP de la passerelle ou sa clé d’activation, que vous pouvez obtenir en vous connectant à la console locale de l’appliance de passerelle.

Vérifier et activer

À ce stade, vous aurez la possibilité vérifier les options de passerelle et de connexion que vous avez choisies et d’apporter des modifications si nécessaire. Lorsque tout est configuré comme vous le souhaitez, vous pouvez activer la passerelle. Avant de pouvoir utiliser votre passerelle activée, vous devez configurer certains paramètres supplémentaires et créer vos ressources de stockage.

Présentation - Configuration de la passerelle

Après avoir activé votre Storage Gateway, vous devez procéder à quelques réglages supplémentaires. Au cours de cette étape, vous allouez le stockage physique que vous avez provisionné sur la plateforme hôte de passerelle pour qu’il soit utilisé comme cache ou comme tampon de téléchargement par l’appliance de passerelle. Vous configurez ensuite les paramètres pour surveiller l'état de votre passerelle à l'aide d'Amazon CloudWatch Logs et des CloudWatch alarmes, et vous ajoutez des balises pour aider à identifier la passerelle, si vous le souhaitez. Avant de pouvoir utiliser votre passerelle activée et configurée, vous devez créer vos ressources de stockage.

Présentation - Ressources de stockage

Une fois que vous avez activé et configuré votre Storage Gateway, vous devez créer des ressources de stockage dans le cloud à utiliser. Selon le type de passerelle que vous avez créé, vous utiliserez la console Storage Gateway pour créer des volumes, des bandes ou des partages de FSx fichiers Amazon S3 ou Amazon à associer à celle-ci. Chaque type de passerelle utilise ses ressources respectives pour émuler le type d’infrastructure de stockage réseau correspondant et transfère les données que vous y écrivez dans le cloud AWS .

Création d'un système de fichiers Amazon FSx pour Windows File Server

Pour créer un Amazon FSx File Gateway dans AWS Storage Gateway, la première étape consiste à créer un système de fichiers Amazon FSx pour Windows File Server. Si vous avez déjà créé un système de FSx fichiers Amazon, passez à l'étape suivante,Création et activation d'un Amazon FSx File Gateway.

> **Note**
>
> Les limites suivantes s'appliquent lors de l'écriture sur un système de FSx fichiers Amazon à partir d'une passerelle de FSx fichiers :
>
> - Votre système de FSx fichiers Amazon et votre passerelle de FSx fichiers doivent appartenir au même AWS compte et être situés dans la même AWS région.
> - Chaque passerelle peut prendre en charge cinq systèmes de fichiers joints. Lorsque vous connectez un système de fichiers, la console Storage Gateway vous indique si la passerelle sélectionnée est à pleine capacité. Dans ce cas, vous devez choisir une autre passerelle ou détacher un système de fichiers avant de pouvoir en attacher un autre.
> - FSx File Gateway prend en charge les quotas de stockage souples (émission d'avertissements lorsque les utilisateurs dépassent leurs limites de données), mais pas les quotas stricts (application des limites de données en refusant l'accès en écriture). Les quotas souples sont pris en charge pour tous les utilisateurs, à l'exception de l' FSx administrateur Amazon. Pour plus d'informations sur la configuration des quotas de stockage, consultez la section Quotas de stockage du guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.
> - Nous vous déconseillons d'utiliser Microsoft Distributed File System (DFS) pour rediriger les utilisateurs vers votre système de FSx fichiers Amazon via FSx File Gateway. Configurez plutôt DFS pour qu'il soit redirigé directement vers le système de FSx fichiers Amazon, AWS Cloud comme décrit dans la section Regroupement de plusieurs systèmes de fichiers avec des espaces de noms DFS dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.
> - Certaines opérations sur les fichiers sur la passerelle de FSx fichiers, telles que le changement de nom de dossiers de niveau supérieur ou la modification des autorisations, peuvent entraîner plusieurs opérations sur les fichiers qui entraînent une I/O charge importante sur votre système FSx de fichiers Windows File Server. Si votre système de

fichiers ne dispose pas de ressources de performance suffisantes pour votre charge de travail, il est possible qu'il supprime les clichés instantanés, car il donne la priorité à la disponibilité permanente I/O plutôt qu'à la conservation historique des clichés instantanés.

Dans la FSx console Amazon, consultez la page Surveillance et performances pour voir si votre système de fichiers est sous-approvisionné. Si tel est le cas, vous pouvez passer au stockage SSD, augmenter la capacité de débit ou augmenter le nombre d'IOPS du SSD pour gérer votre charge de travail.

Pour créer un système de fichiers FSx pour Windows File Server

1. Ouvrez AWS Management Console at https://console.aws.amazon.com/fsx/home/ et choisissez la région dans laquelle vous souhaitez créer votre passerelle.
2. Suivez les instructions de la section Getting Started with Amazon FSx dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

Création et activation d'un Amazon FSx File Gateway

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

Rubriques

- Configurer un Amazon FSx File Gateway
- Connectez votre Amazon FSx File Gateway à AWS
- Vérifiez les paramètres et activez votre Amazon FSx File Gateway
- Configuration de votre Amazon FSx File Gateway

Configurer un Amazon FSx File Gateway

Pour configurer une nouvelle passerelle de FSx fichiers

1. Ouvrez AWS Management Console at https://console.aws.amazon.com/storagegateway/home/ et choisissez l' Région AWS endroit où vous souhaitez créer votre passerelle.
2. Choisissez Créer une passerelle pour ouvrir la page Configurer une passerelle.
3. Dans la section Paramètres de la passerelle, procédez comme suit :

a. Pour Gateway name (Nom de la passerelle), entrez le nom de votre passerelle. Une fois votre passerelle créée, vous pouvez rechercher ce nom pour trouver votre passerelle dans les pages de liste de la AWS Storage Gateway console.

b. Pour le Fuseau horaire de la passerelle, choisissez le fuseau horaire local de la partie du monde où vous souhaitez déployer votre passerelle.

4. Dans la section Options de passerelle, pour le type de passerelle, choisissez Amazon FSx File Gateway.

5. Dans la section Options de plateforme, procédez comme suit :

a. Pour Plateforme hôte, choisissez la plate-forme sur laquelle vous souhaitez déployer votre passerelle. Suivez ensuite les instructions spécifiques à la plate-forme affichées sur la page de la console Storage Gateway pour configurer votre plate-forme 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.
- Linux KVM : téléchargez, déployez et configurez la machine virtuelle de passerelle à l'aide de la machine virtuelle basée sur le noyau Linux (KVM). Reportez-vous au fichier aws-storage-gateway .xml fourni pour les configurations de démarrage suggérées. Le mode de démarrage UEFI avec démarrage sécurisé désactivé (loader_secure=no) est requis pour File Gateway 2.x, Volume Gateway 3.x et Tape Gateway 3.x.
- Amazon EC2 — Configurez et lancez une instance Amazon EC2 pour héberger votre passerelle.
- Appliance matérielle : commandez une appliance matérielle physique dédiée AWS pour héberger votre passerelle.

b. Pour Confirmer la configuration de la passerelle, cochez la case pour confirmer que vous avez effectué les étapes de déploiement pour la plateforme hôte que vous avez choisie. Cette étape ne s’applique pas à la plateforme hôte de l’appliance matérielle.

6. Maintenant que votre passerelle est configurée, vous devez choisir la manière dont vous souhaitez qu'elle se connecte et communique avec elle AWS. Choisissez Suivant pour continuer.

Connectez votre Amazon FSx File Gateway à AWS

Pour connecter une nouvelle passerelle de FSx fichiers à AWS

1. Si ce n'est pas déjà fait, suivez la procédure décrite dans Configurer un Amazon FSx File Gateway. Lorsque vous avez terminé, choisissez Next pour ouvrir la AWS page Connect to dans la AWS Storage Gateway console.
2. Dans la section Options du point de terminaison, pour Point de terminaison de service, choisissez le type de point de terminaison avec lequel votre passerelle communiquera AWS. Choisissez parmi les options suivantes :

   - Accessible au public — Votre passerelle communique AWS via l'Internet public. Si vous sélectionnez cette option, cochez la case point de terminaison compatible FIPS pour indiquer si la connexion doit être conforme aux normes FIPS (Federal Information Processing Standards).

     > **Note**
     >
     > Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison conforme à la norme 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 certaines AWS régions. Pour plus d'informations, consultez Points de terminaison et quotas AWS Storage Gateway dans le document Références générales AWS.

   - Hébergé par VPC : votre passerelle communique AWS via une connexion privée avec votre cloud privé virtuel (VPC), ce qui vous permet de contrôler les paramètres de votre 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 le nom ou l'adresse IP du système de noms de domaine (DNS) de son point de terminaison VPC.
3. Dans la section Options de connexion de passerelle, pour les 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 être en mesure de 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 depuis votre client hyperviseur ou en la copiant depuis la page de détails de votre instance Amazon EC2.

- Clé d'activation : saisissez 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 la manière dont vous souhaitez que votre passerelle se connecte AWS, vous devez activer la passerelle. Choisissez Suivant pour continuer.

Vérifiez les paramètres et activez votre Amazon FSx File Gateway

Pour activer une nouvelle passerelle FSx de fichiers

1. Si ce n'est pas déjà fait, suivez les procédures décrites dans les rubriques suivantes :

   - Configurer un Amazon FSx File Gateway
   - Connectez votre Amazon FSx File Gateway à AWS

   Lorsque vous avez terminé, choisissez Suivant pour ouvrir la page Révision et activation dans la AWS Storage Gateway console.
2. Vérifiez les détails de la passerelle initiale pour chaque section de la page.
3. Si une section contient des erreurs, choisissez Modifier pour revenir à la page de paramètres correspondante et apporter des modifications.

   > **Important**
   >
   > Vous ne pouvez pas modifier les options ou les paramètres de connexion de la passerelle une fois celle-ci 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. Choisissez Suivant pour continuer.

Configuration de votre Amazon FSx File Gateway

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

1. Si ce n'est pas déjà fait, suivez les procédures décrites dans les rubriques suivantes :

   - Configurer un Amazon FSx File Gateway
   - Connectez votre Amazon FSx File Gateway à AWS
   - Vérifiez les paramètres et activez votre Amazon FSx File Gateway

   Lorsque vous avez terminé, choisissez Next pour ouvrir la page Configurer la passerelle dans la AWS Storage Gateway console.
2. Dans la section Configurer le stockage, utilisez les listes déroulantes pour allouer au moins un disque local d'une capacité d'au moins 150 Go au cache. Les disques locaux répertoriés dans cette section correspondent au stockage physique que vous avez provisionné sur votre plateforme hôte.
3. Dans la section groupe de CloudWatch journaux, choisissez comment configurer Amazon CloudWatch Logs pour surveiller l'état de votre passerelle. Choisissez parmi les options suivantes :

   - Créer 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.

> **Note**
>
> Pour recevoir les journaux de santé de Storage Gateway, les autorisations suivantes doivent figurer dans la politique de ressources de votre groupe de journaux. Remplacez-les *highlighted section* par les informations ResourceArn du groupe de journaux spécifiques à votre déploiement.
>
> ```
> "Sid": "AWSLogDeliveryWrite20150319",
>       "Effect": "Allow",
> ```

```
      "Principal": {
        "Service": [
          "delivery.logs.amazonaws.com"
        ]
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

L'élément « Ressource » n'est obligatoire que si vous souhaitez que les autorisations s'appliquent explicitement à un groupe de journaux individuel.

4. Dans la section des CloudWatch alarmes, choisissez comment configurer les CloudWatch alarmes Amazon pour vous avertir lorsque les métriques de votre passerelle s'écartent des limites définies. Choisissez parmi les options suivantes :

   - Création des alarmes recommandées par Storage Gateway : créez automatiquement toutes les CloudWatch alarmes recommandées lors de la création de la passerelle. Pour plus d'informations sur les alarmes recommandées, consultez la section Comprendre les CloudWatch alarmes.

     > **Note**
     >
     > Cette fonctionnalité nécessite des autorisations CloudWatch de politique qui ne sont pas automatiquement accordées dans le cadre de la politique d'accès complet préconfigurée de Storage Gateway. Assurez-vous que votre politique de sécurité accorde les autorisations suivantes avant de tenter de créer les CloudWatch alarmes recommandées :
     >
     > - `cloudwatch:PutMetricAlarm` - créer des alarmes
     > - `cloudwatch:DisableAlarmActions` - désactiver les actions d'alarme
     > - `cloudwatch:EnableAlarmActions` - activer les actions d'alarme
     > - `cloudwatch:DeleteAlarms` - supprimer des alarmes

   - Création d'une alarme personnalisée : configurez une nouvelle CloudWatch alarme pour être informé des métriques de votre passerelle. Choisissez Create alarm pour définir les métriques

et spécifier les actions d'alarme dans la CloudWatch console Amazon. Pour obtenir des instructions, consultez la section Utilisation des CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

- Aucune alarme — N'utilisez pas d' CloudWatch alarmes pour être informé des indicateurs de votre passerelle.

5. (Facultatif) Dans la section Balises, choisissez Ajouter une nouvelle balise, puis entrez une paire clé-valeur en distinguant majuscules et minuscules pour vous aider à rechercher et à filtrer votre passerelle sur les pages de liste de la console. AWS Storage Gateway Répétez cette étape pour ajouter autant de balises que vous désirez.
6. (Facultatif) Dans la section Vérifier la configuration de VMware haute disponibilité, si votre passerelle est déployée sur un VMware hôte faisant partie d'un cluster de VMware haute disponibilité (HA), choisissez Verify VMware HA pour tester si la configuration HA fonctionne correctement.

   > **Note**
   >
   > Cette section s'affiche uniquement pour les passerelles qui s'exécutent sur la plate-forme VMware hôte.
   > Cette étape n'est pas obligatoire 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 Configurer pour terminer la création de votre passerelle.

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

Maintenant que vous avez créé votre passerelle, vous devez joindre un système de fichiers pour qu'elle puisse l'utiliser. Pour obtenir des instructions, voir Joindre un système de fichiers Amazon FSx pour Windows File Server.

Si vous n'avez pas de système de FSx fichiers Amazon existant à joindre, vous devez en créer un. Pour obtenir des instructions, consultez Getting started with Amazon FSx.

Activation d'une passerelle dans un cloud privé virtuel

Vous pouvez créer une connexion privée entre votre appliance de passerelle sur site et une infrastructure de stockage basée sur le cloud. Vous pouvez utiliser cette connexion pour activer votre passerelle et la configurer pour transférer des données vers des services AWS de stockage sans communiquer via l'Internet public. À l'aide du service Amazon VPC, vous pouvez lancer AWS des ressources, notamment des points de terminaison d'interface réseau privés privés, dans un cloud privé virtuel (VPC) personnalisé. Un VPC vous permet de contrôler vos paramètres réseau, tels que la plage d'adresses IP, les sous-réseaux, les tables de routage et les passerelles de réseau. Pour plus d'informations VPCs, consultez Qu'est-ce qu'Amazon VPC ? dans le guide de l'utilisateur Amazon VPC.

Pour activer votre passerelle dans un VPC, utilisez la console Amazon VPC pour créer un point de terminaison VPC pour Storage Gateway, créez et obtenez l'ID de point de terminaison VPC, puis spécifiez cet identifiant de point de terminaison VPC lorsque vous créez et activez la passerelle. Pour plus d'informations, consultez connecter votre Amazon FSx File Gateway à AWS.

Pour configurer votre passerelle de FSx fichiers afin de transférer des données via le VPC, vous devez établir un VPN ou un AWS DirectConnect lien entre le VPC Amazon FSx pour Windows File Server et le réseau sur lequel votre passerelle est déployée.

> **Note**
>
> Vous devez activer votre passerelle dans la même région que celle où vous avez créé le point de terminaison VPC pour Storage Gateway.

Création d'un point de terminaison VPC pour Storage Gateway

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

Pour créer un point de terminaison de VPC pour Storage Gateway

1. Connectez-vous à la console Amazon VPC AWS Management Console et ouvrez-la 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. Sur la page Créer un point de terminaison, choisissez Services AWS en tant que Catégorie de service.
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 l'option Activer le nom DNS n'est pas sélectionnée.
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 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 l'onglet Détails du point de terminaison de la passerelle de stockage sélectionné, sous Noms DNS, utilisez le premier nom DNS qui ne spécifie pas de zone de disponibilité. Votre nom DNS doit ressembler à l'exemple suivant : `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Maintenant que vous disposez d'un point de terminaison VPC, vous pouvez créer et activer votre passerelle. Pour plus d'informations, consultez Créer et activer une passerelle de FSx fichiers Amazon.

Pour plus d'informations sur l'obtention d'une clé d' Obtenir une clé d'activation pour votre passerelle.

Configuration des paramètres d'accès au domaine Microsoft Active Directory

Au cours de cette étape, vous configurez les paramètres d'accès pour associer votre Amazon FSx File Gateway à un domaine Microsoft Active Directory.

Pour configurer les paramètres Active Directory

1. Dans la console Storage Gateway, choisissez les systèmes de FSx fichiers dans le menu de navigation.
2. Choisissez Joindre FSx le système de fichiers.
3. Sur la page Confirmer la passerelle, choisissez la passerelle que vous souhaitez associer à votre domaine Active Directory dans le menu déroulant.

   Si vous n'avez pas de passerelle, vous devez en créer une. Assurez-vous que votre passerelle peut résoudre le nom de votre contrôleur de domaine Active Directory. Pour plus d'informations, consultez Conditions préalables.
4. Entrez les valeurs des paramètres Active Directory :

   > **Note**
   >
   > Si votre passerelle est déjà associée à un domaine, vous n'avez pas besoin de le rejoindre à nouveau. Passez à l'étape suivante.

   - Dans Nom de domaine, entrez le nom de domaine de l'Active Directory que vous souhaitez utiliser.
   - Pour Utilisateur du domaine, entrez le nom d'utilisateur de l'utilisateur Active Directory que vous souhaitez utiliser pour rejoindre la passerelle vers le domaine. Cet utilisateur doit disposer des autorisations nécessaires. Pour plus d'informations, voir Exigences relatives aux autorisations relatives aux aux comptes de service Active Directory.
   - Dans le champ Mot de passe du domaine, entrez le mot de passe de l'utilisateur.
   - Pour Unité organisationnelle (facultatif), vous pouvez spécifier une unité organisationnelle à laquelle appartient Active Directory.

> **Note**
>
> Si vous laissez ce champ vide, l'adhésion à un domaine crée un compte d'ordinateur Active Directory dans le conteneur d'ordinateurs par défaut (qui n'est pas une unité d'organisation), en utilisant l'ID de passerelle de la passerelle comme nom de compte (par exemple, SGW-1234ADE). Il n'est pas possible de personnaliser le nom de ce compte.
>
> Si votre environnement Active Directory exige que vous préséliciez des comptes pour faciliter le processus d'adhésion à un domaine, vous devez créer ce compte à l'avance.
>
> Si votre environnement Active Directory dispose d'une unité d'organisation désignée pour les nouveaux objets informatiques, vous devez spécifier cette unité d'organisation lorsque vous rejoignez le domaine.

- Entrez une valeur pour le (s) contrôleur (s) de domaine (facultatif).

5. Choisissez Suivant pour ouvrir la page du système de pièces FSx jointes.

Étape suivante

Joindre un système de fichiers Amazon FSx pour Windows File Server

Joindre un système de fichiers Amazon FSx pour Windows File Server

Vous devez disposer d'un système de fichiers FSx pour Windows File Server avant de pouvoir le joindre à une passerelle de FSx fichiers. Si vous n'avez pas de système de fichiers, vous devez en créer un. Pour obtenir des instructions, consultez l'étape 1 : créer votre système de fichiers dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

L'étape suivante consiste à associer un système de FSx fichiers Amazon à la passerelle. Lorsque vous attachez un système de FSx fichiers Amazon, tous les partages de fichiers du système de fichiers sont mis à la disposition d'Amazon FSx File Gateway (FSx File Gateway) pour que vous puissiez les monter.

> **Note**
>
> Les limites suivantes s'appliquent lors de l'écriture dans un système de FSx fichiers Amazon depuis Amazon FSx File Gateway :
>
> - Votre système de FSx fichiers Amazon et votre passerelle de FSx fichiers doivent être la propriété de la même entreprise Compte AWS et se trouver dans le même emplacement Région AWS.
> - Chaque passerelle peut prendre en charge jusqu'à cinq systèmes de fichiers joints. Lorsque vous attachez un système de fichiers, la console Storage Gateway vous indique si la passerelle sélectionnée est à pleine capacité. Dans ce cas, vous devez choisir une autre passerelle ou détacher un système de fichiers avant de pouvoir en attacher un autre.
> - FSx File Gateway prend en charge les quotas de stockage souples (qui vous avertissent lorsque les utilisateurs dépassent leurs limites de données), mais pas les quotas stricts (qui appliquent les limites de données en refusant l'accès en écriture). Les quotas souples sont pris en charge pour tous les utilisateurs, à l'exception de l' FSx administrateur Amazon. Pour plus d'informations sur la configuration des quotas de stockage, consultez la section Quotas de stockage dans le guide de FSx l'utilisateur Amazon.
> - Nous vous déconseillons d'utiliser Microsoft Distributed File System (DFS) pour rediriger les utilisateurs vers votre système de FSx fichiers Amazon via FSx File Gateway. Configurez plutôt DFS pour qu'il soit redirigé directement vers le système de FSx fichiers Amazon, AWS Cloud comme décrit dans la section Regroupement de plusieurs systèmes

de fichiers avec des espaces de noms DFS dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

Pour joindre un système de FSx fichiers Amazon

1. Dans la console Storage Gateway, sur la page Systèmes de FSx fichiers > Joindre un système de FSx fichiers, renseignez les champs suivants dans la section des paramètres du système de FSx fichiers :

   - Pour FSx le nom du système de fichiers, choisissez le système de fichiers que vous souhaitez joindre dans la liste déroulante.
   - Pour l'adresse IP du point de terminaison local, entrez l'adresse IP de passerelle que les clients utiliseront pour parcourir les partages de fichiers sur le système de FSx fichiers.

   > **Note**
   >
   > - Vous devez spécifier une adresse IP pour chaque système de fichiers rattaché à la passerelle.
   > - Pour les EC2 passerelles Amazon, vous pouvez spécifier l'adresse IP privée de l' EC2 instance, sauf si elle est déjà utilisée par un autre système de fichiers, auquel cas vous devez ajouter une nouvelle adresse privée à la passerelle, puis la redémarrer. Pour plus d'informations, consultez la section Adresses IP multiples dans le guide de EC2 l'utilisateur Amazon.
   > - Pour les passerelles locales, vous pouvez spécifier l'adresse IP de l'interface réseau principale (statique ou DHCP), sauf si elle est déjà utilisée par un autre système de fichiers, auquel cas vous devez fournir une adresse IP différente provenant du même sous-réseau que l'interface principale, qui sera mise à disposition sous forme d'adresse IP virtuelle. N'utilisez pas d'adresse IP attribuée à une interface réseau autre que l'interface principale.

2. Dans la section Paramètres du compte de service, fournissez les informations d'identification du compte de service associées au système de FSx fichiers Amazon.

> **Note**
>
> Ce compte de service doit disposer des privilèges d'opérateur de sauvegarde du service Active Directory associé à vos systèmes de FSx fichiers Amazon ou disposer d'autorisations équivalentes.

> **Important**
>
> Pour garantir des autorisations suffisantes sur les fichiers, les dossiers et les métadonnées des fichiers, nous vous recommandons de faire du compte de service un membre du groupe des administrateurs du système de fichiers.
> Si vous utilisez AWS Directory Service Microsoft Active Directory avec Amazon FSx pour Windows File Server, le compte de service doit être membre du groupe des FSx administrateurs AWS délégués.
> Si vous utilisez un Active Directory autogéré avec Amazon FSx pour Windows File Server, nous recommandons que le compte de service soit membre du groupe d'administrateurs de système de fichiers délégués personnalisé que vous avez spécifié pour l'administration du système de fichiers lorsque vous avez créé votre système de FSx fichiers Amazon.
> Si vous avez choisi de ne pas créer de groupe d'administrateurs de système de fichiers délégués personnalisé lors de la création du FSx système de fichiers Amazon, le groupe par défaut est Domain Admins. Bien que vous puissiez faire du compte de service un membre de ce groupe à la place, cela n'est pas recommandé en tant que bonne pratique.
> Pour plus d'informations, consultez la section Délégation de privilèges à votre compte de FSx service Amazon dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

3. Dans la section Journaux d'audit, choisissez Groupes de journaux existants, puis choisissez le journal que vous souhaitez utiliser pour surveiller l'accès à votre système de FSx fichiers Amazon. Vous pouvez en créer un nouveau. Si vous ne souhaitez pas surveiller votre système, choisissez Désactiver la journalisation.
4. Pour le paramètre d'actualisation automatique du cache, si vous souhaitez que votre cache soit actualisé automatiquement, choisissez Définir l'intervalle d'actualisation et spécifiez un intervalle compris entre 5 minutes et 30 jours.

5. (Facultatif) Dans la section Balises, choisissez Ajouter une nouvelle balise pour ajouter une ou plusieurs clés et une valeur pour baliser vos paramètres.
6. Choisissez Suivant, puis vérifiez les paramètres. Pour modifier vos paramètres, vous pouvez sélectionner Modifier dans chaque section.
7. Lorsque vous avez terminé, choisissez Finish.

Étape suivante

Montez et utilisez votre partage de FSx fichiers Amazon

Montez et utilisez votre partage de FSx fichiers Amazon

Avant de monter votre partage de fichiers sur le client, attendez que le statut du système de FSx fichiers Amazon passe à Disponible. Une fois votre partage de fichiers monté, vous pouvez commencer à utiliser votre Amazon FSx File Gateway (FSx File Gateway).

Rubriques

- Montez votre partage de fichiers SMB sur votre client
- Testez votre passerelle FSx de fichiers

Montez votre partage de fichiers SMB sur votre client

Au cours de cette étape, vous devez monter votre partage de fichiers SMB et le mapper sur un lecteur accessible à votre client. La section File Gateway de la console présente les commandes de montage prises en charge que vous pouvez utiliser pour les clients SMB. Voici quelques options supplémentaires à essayer.

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

- La `net use` commande : elle ne persiste pas après le redémarrage du système, sauf si vous utilisez le `/persistent:(yes:no)` commutateur.
- Utilitaire de ligne de `CmdKey` commande : crée une connexion permanente à un partage de fichiers SMB monté qui est maintenue après un redémarrage.
- Un lecteur réseau mappé dans l'explorateur de fichiers : configure le partage de fichiers monté pour qu'il se reconnecte lors de la connexion et pour que vous deviez saisir vos informations d'identification réseau.
- PowerShell script — Peut être persistant et peut être visible ou invisible pour le système d'exploitation pendant le montage.

> **Note**
>
> Si vous êtes un utilisateur de Microsoft Active Directory, vérifiez auprès de votre administrateur que vous avez accès au partage de fichiers SMB avant de monter le partage de fichiers sur votre système local.

Amazon FSx File Gateway ne prend pas en charge le verrouillage SMB ni les attributs étendus SMB.

Pour monter un partage de fichiers SMB pour les utilisateurs d'Active Directory à l'aide de la commande net use

1. Assurez-vous que vous avez accès au partage de fichiers SMB avant de monter le partage de fichiers sur votre système local.
2. Pour les clients Microsoft Active Directory, entrez la commande suivante à l'invite de commande :

   ```
   net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
   ```

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

1. Appuyez sur la touche Windows et entrez **cmd** pour afficher l'élément de menu de l'invite de commande.
2. Ouvrez le menu contextuel (clic droit) de l'invite de commande, puis choisissez Exécuter en tant qu'administrateur.
3. Entrez la commande suivante :

   ```
   C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
   ```

> **Note**
>
> Lorsque vous montez des partages de fichiers, vous devrez peut-être remonter votre partage de fichiers après avoir redémarré votre client.

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

1. Appuyez sur la touche Windows et entrez **File Explorer** dans la zone Rechercher dans Windows, ou appuyez sur**Win+E**.

2. Dans le volet de navigation, sélectionnez Ce PC. Ensuite, dans l'onglet Ordinateur, choisissez Cartographier le lecteur réseau.
3. Dans la boîte de dialogue Cartographier le lecteur réseau, choisissez une lettre de lecteur pour Drive.
4. Dans le champ Dossier***[File Gateway IP]**[SMB File Share Name]***, entrez 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 Active Directory ou le mot de passe utilisateur du compte invité.
7. Choisissez Terminer pour terminer votre point de montage.

Testez votre passerelle FSx de fichiers

Vous pouvez copier des fichiers et des répertoires sur votre lecteur mappé. Les fichiers sont automatiquement téléchargés sur votre système de fichiers FSx pour Windows File Server.

Pour télécharger des fichiers depuis votre client Windows vers Amazon FSx

1. Sur votre client Windows, accédez au lecteur sur lequel vous avez monté votre système de fichiers. Le nom du lecteur est précédé du nom de votre système de fichiers.
2. Copiez des fichiers ou un répertoire sur le lecteur.

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

Gestion de vos ressources Amazon FSx File Gateway

Les sections suivantes fournissent des informations sur la façon de gérer vos ressources Amazon FSx File Gateway (FSx File Gateway), y compris l'attachement et le détachement de systèmes de FSx fichiers Amazon et la configuration des paramètres Microsoft Active Directory.

Rubriques

- Comprendre l'état de la passerelle
- Comprendre l'état du système de fichiers
- Modifier les informations de base d'une passerelle de FSx fichiers
- Définissez un niveau de sécurité pour votre passerelle
- Modification des paramètres Active Directory pour n FSx File Gateway
- Modification des paramètres d'un système de FSx fichiers Amazon
- Détacher un système de FSx fichiers Amazon

Comprendre l'état de la passerelle

Chaque passerelle de votre déploiement AWS Storage Gateway possède un statut associé qui vous indique en un coup d'œil son état de santé. La plupart du temps, le statut indique que la passerelle fonctionne normalement et qu'aucune action n'est nécessaire de votre part. Dans certains cas, l'état indique un problème qui exige ou non une action de votre part.

Vous pouvez consulter l'état de chaque passerelle de votre déploiement sur la page Gateways de la console Storage Gateway. L'état de la passerelle apparaît dans la colonne État à côté du nom de la passerelle. Une passerelle qui fonctionne normalement a un statut de`RUNNING`.

Dans le tableau suivant, vous trouverez une description de l'état de chaque passerelle et vous indiquerez si vous devez agir en fonction de ce statut. Une passerelle doit avoir un `RUNNING` statut tout le temps ou la plupart du temps lorsqu'elle est utilisée.

Statut	Signification
`RUNNING`	La passerelle est correctement configurée et peut être utilisée.

Statut	Signification
`OFFLINE`	Votre passerelle peut avoir un `OFFLINE` statut pour une ou plusieurs des raisons suivantes : • La passerelle ne peut pas atteindre les points de terminaison du service Storage Gateway. • La passerelle s'est arrêtée de façon inattendue. • La passerelle possède un disque de cache associé qui est déconnect é, a été modifié ou est défaillant.

Comprendre l'état du système de fichiers

Vous pouvez visualiser l'état d'un système de fichiers en un coup d'œil en consultant son état. Si l'état indique que le système de fichiers fonctionne normalement, aucune action n'est requise de votre part. Si le statut indique l'existence d'un problème, vous pouvez examiner la situation afin de déterminer si une action est nécessaire.

Vous pouvez consulter l'état d'un système de fichiers sur la console Storage Gateway dans la colonne Status. Un système de fichiers qui fonctionne correctement affiche le statut DISPONIBLE. Ce devrait être le statut la plupart du temps.

Le tableau suivant décrit les statuts des partages de fichiers, leur signification et indique si des mesures peuvent être nécessaires.

Statut	Signification
DISPONIBLE	Le système de fichiers est correctement configuré et peut être utilisé. Il s'agit de l'état standard d'un système de fichiers qui fonctionne correctem ent.
CREAtioN	Le système de fichiers n'est pas encore complètement créé et n'est pas prêt à être utilisé. L'état CREATION est transitionnel. Aucune action n’est requise. Si le système de fichiers reste bloqué dans cet état, c'est probablement parce que la machine virtuelle de passerelle a perdu la connexion à AWS.

Statut	Signification
MISE À JOUR	La configuration du système de fichiers est en cours de mise à jour. Le statut de MISE À JOUR est transitoire. Aucune action n'est requise. Si un système de fichiers reste bloqué dans cet état, c'est probablement parce que la machine virtuelle de passerelle a perdu la connexion à AWS.
SUPPRESSION	Le système de fichiers est en cours de suppression. Le système de fichiers n'est pas supprimé tant que toutes les données ne sont pas téléchargées vers AWS. L'état DELETING est transitionnel et aucune action est requise.
FORCE_DELETING	Le système de fichiers est supprimé de force. Le système de fichiers est immédiatement supprimé et les données ne sont pas téléchargées vers AWS. L'état FORCE_DELETING est transitionnel et aucune action n'est requise.
ERROR	Le système de fichiers est en mauvais état. Il faut agir. Parmi les causes possibles, citons des problèmes liés aux informations d'identification ou aux privilèges d'accès, des problèmes de connectivité ou un espace de stockage insuffisant sur le système de fichiers. Lorsque le problème à l'origine de l'état défectueux est résolu, le système de fichiers revient à l'état DISPONIBLE.

Modifier les informations de base d'une passerelle de FSx fichiers

Vous pouvez utiliser la console Storage Gateway pour modifier les informations de base d'une passerelle existante, notamment le nom de la passerelle, le fuseau horaire et le groupe de CloudWatch journaux.

Pour modifier les informations de base d'une passerelle existante

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Sélectionnez Passerelles, puis sélectionnez la passerelle dont vous souhaitez modifier les informations de base.
3. Dans le menu déroulant Actions, choisissez Modifier les informations de la passerelle.

4. Pour Gateway name (Nom de la passerelle), entrez le nom de votre passerelle. Vous pouvez rechercher ce nom pour trouver votre passerelle sur les pages de liste de la console Storage Gateway.

   > **Note**
   >
   > Les noms de passerelle doivent comporter entre 2 et 255 caractères et ne peuvent pas inclure de barre oblique (\ou/).
   > La modification du nom d'une passerelle déconnecte toutes les CloudWatch alarmes configurées pour surveiller la passerelle. Pour reconnecter les alarmes, mettez à jour le GatewayNamepour chaque alarme dans la CloudWatch console.

5. Pour le Fuseau horaire de la passerelle, choisissez le fuseau horaire local de la partie du monde où vous souhaitez déployer votre passerelle.
6. Pour Choisir comment configurer un groupe de journaux, choisissez comment configurer Amazon CloudWatch Logs pour surveiller l'état de votre passerelle. Choisissez parmi les options suivantes :

   - Créer 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.

7. Lorsque vous avez fini de modifier les paramètres que vous souhaitez modifier, choisissez Enregistrer les modifications.

Définissez un niveau de sécurité pour votre passerelle

Vous pouvez configurer le niveau de sécurité SMB de votre passerelle de FSx fichiers afin de spécifier si la passerelle doit exiger la signature SMB (Server Message Block) ou le chiffrement SMB.

Pour configurer un niveau de sécurité

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.

2. Choisissez Gateways, puis choisissez la passerelle pour laquelle vous souhaitez modifier les paramètres SMB.
3. Dans le menu déroulant Actions, choisissez Modifier les paramètres SMB, puis sélectionnez Paramètres de sécurité SMB.
4. Pour Security level (Niveau de sécurité), choisissez l'une des actions suivantes :

> **Note**
>
> Pour plus d'informations sur la configuration de ce paramètre à l'aide de l' AWS API, consultez la section SMBSecurityStratégie de mise à jour dans le Guide de référence des AWS Storage Gateway API.
> Un niveau de sécurité plus élevé peut affecter les performances de la passerelle.

- Chiffrement obligatoire — Si vous choisissez cette option, FSx File Gateway autorise uniquement les connexions provenant de SMBv3 clients utilisant des algorithmes de chiffrement AES 256 bits. Les algorithmes 128 bits ne sont pas autorisés. Cette option est recommandée pour les environnements qui traitent des données sensibles. Il fonctionne avec les clients SMB sous Microsoft Windows 8, Windows Server 2012 ou version ultérieure.
- Appliquer le chiffrement : si vous choisissez cette option, FSx File Gateway autorise uniquement les connexions provenant de SMBv3 clients dont le chiffrement est activé. Les algorithmes 256 bits et 128 bits sont autorisés. Cette option est recommandée pour les environnements qui traitent des données sensibles. Il fonctionne avec les clients SMB sous Microsoft Windows 8, Windows Server 2012 ou version ultérieure.
- Appliquer la signature : si vous choisissez cette option, FSx File Gateway autorise uniquement les connexions depuis SMBv2 ou depuis des SMBv3 clients dont la signature est activée. Cette option fonctionne avec les clients SMB sous Microsoft Windows Vista, Windows Server 2008 ou version ultérieure.

> **Note**
>
> Le niveau de sécurité par défaut pour FSx File Gateway est Appliquer le chiffrement.

5. Choisissez Enregistrer.

Modification des paramètres Active Directory pour n FSx File Gateway

Pour utiliser Microsoft Active Directory de votre entreprise ou AWS Managed Microsoft AD pour un accès authentifié à votre système de FSx fichiers Amazon, modifiez les paramètres SMB de votre passerelle et fournissez vos informations d'identification de domaine Active Directory. Cela permet à votre passerelle de rejoindre votre domaine Active Directory et aux membres du domaine d'accéder au système de fichiers.

> **Note**
>
> À l'aide de Directory Service, vous pouvez créer un service de domaine Active Directory hébergé dans le AWS Cloud.
> Pour l'utiliser AWS Managed Microsoft AD avec une passerelle Amazon EC2, vous devez créer l'instance Amazon EC2 dans le même VPC que AWS Managed Microsoft AD le, ajouter le groupe de sécurité _WorkspaceMembers à l'instance Amazon EC2 et rejoindre le domaine AD à l'aide des informations d'identification d'administrateur du. AWS Managed Microsoft AD
> Pour plus d'informations à ce sujet AWS Managed Microsoft AD, consultez le Guide AWS Directory Service d'administration.
> Pour plus d'informations sur Amazon EC2, consultez la documentation Amazon Elastic Compute Cloud.

Pour activer l'authentification Active Directory

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Choisissez Gateways, puis choisissez la passerelle pour laquelle vous souhaitez modifier les paramètres SMB.
3. Dans le menu déroulant Actions, choisissez Modifier les paramètres SMB, puis sélectionnez les paramètres Active Directory.
4. Dans Nom de domaine, entrez le nom du domaine Active Directory auquel vous souhaitez que votre passerelle rejoigne.

> **Note**
>
> L'état Active Directory indique Detached (Détaché) lorsqu'une passerelle n'a jamais rejoint un domaine.
>
> Votre compte de service Active Directory doit disposer des autorisations requises. Pour plus d'informations, voir Exigences relatives aux autorisations relatives aux aux comptes de service Active Directory.
>
> L'adhésion à un domaine crée un compte d'ordinateur Active Directory dans le conteneur d'ordinateurs par défaut (qui n'est pas une unité d'organisation), en utilisant l'ID de passerelle de la passerelle comme nom de compte (par exemple, SGW-1234ADE). Il n'est pas possible de personnaliser le nom de ce compte.
>
> Si votre environnement Active Directory exige que vous préséliciez des comptes pour faciliter le processus d'adhésion à un domaine, vous devez créer ce compte à l'avance.
>
> Si votre environnement Active Directory dispose d'une unité d'organisation désignée pour les nouveaux objets informatiques, vous devez spécifier cette unité d'organisation lorsque vous rejoignez le domaine.
>
> Si votre passerelle ne parvient pas à rejoindre un annuaire Active Directory, essayez de le rejoindre avec l'adresse IP de l'annuaire en utilisant l'opération JoinDomainAPI.

5. Pour l'utilisateur du domaine et le mot de passe du domaine, entrez les informations d'identification du compte de service Active Directory que la passerelle utilisera pour rejoindre le domaine.
6. (Facultatif) Pour Unité d'organisation (UO), entrez l'UO désignée que votre Active Directory utilise pour les nouveaux objets informatiques.
7. (Facultatif) Pour Contrôleur (s) de domaine (DC), entrez le nom d'un ou de plusieurs contrôleurs DCs par lesquels votre passerelle se connectera à Active Directory. Vous pouvez en saisir plusieurs DCs sous forme de liste séparée par des virgules. Vous pouvez laisser ce champ vide pour permettre au DNS de sélectionner automatiquement un contrôleur de domaine.
8. Sélectionnez Enregistrer les modifications.

Modification des paramètres d'un système de FSx fichiers Amazon

Après avoir créé un système de fichiers Amazon FSx pour Windows File Server, vous pouvez modifier les paramètres relatifs aux CloudWatch journaux, à l'actualisation automatique du cache et aux informations d'identification du compte de FSx service Amazon.

Pour modifier les paramètres FSx du système de fichiers Amazon

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Système de fichiers, puis le système de fichiers dont vous souhaitez modifier les paramètres.
3. Pour Actions, choisissez Modifier les paramètres du système de fichiers.
4. Dans la section des paramètres du système de fichiers, vérifiez les informations relatives à la passerelle, à FSx l'emplacement Amazon et à l'adresse IP.

   > **Note**
   >
   > Vous ne pouvez pas modifier l'adresse IP d'un système de fichiers une fois celui-ci connecté à une passerelle. Pour modifier l'adresse IP, vous devez détacher et reconnecter le système de fichiers.

5. Dans la section Journaux d'audit, choisissez une option permettant d'utiliser des groupes de CloudWatch journaux pour surveiller l'accès aux systèmes de FSx fichiers Amazon. Vous pouvez utiliser un groupe de journaux existant.
6. Pour les paramètres d'actualisation automatique du cache, choisissez une option. Si vous choisissez Définir l'intervalle d'actualisation, définissez la durée en jours, heures et minutes pour actualiser le cache du système de fichiers à l'aide de Time To Live (TTL).

   TTL est le temps écoulé depuis la dernière actualisation. Lorsque le répertoire est consulté après cette période, la passerelle de fichiers actualise le contenu de ce répertoire à partir du système de FSx fichiers Amazon.

   > **Note**
   >
   > Les valeurs d'intervalle d'actualisation valides sont comprises entre 5 minutes et 30 jours.

7. Dans la section Paramètres du compte de service - facultatif, entrez un nom d'utilisateur et un mot de passe. Ces informations d'identification sont destinées à un utilisateur ayant le rôle Backup Administrator du service Active Directory associé à vos systèmes de FSx fichiers Amazon.
8. Sélectionnez Enregistrer les modifications.

Détacher un système de FSx fichiers Amazon

Le détachement d'un système de fichiers ne supprime pas vos données dans FSx Windows File Server. Les données enregistrées dans ces systèmes de fichiers avant que vous ne les détachiez seront toujours téléchargées sur votre serveur de fichiers FSx pour Windows.

Pour détacher un système de FSx fichiers Amazon

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Choisissez les systèmes de FSx fichiers, puis sélectionnez un ou plusieurs systèmes de fichiers à détacher.
3. Pour Actions, choisissez Détacher le système de fichiers. La boîte de dialogue de confirmation s’affiche.
4. Vérifiez que vous souhaitez détacher les systèmes de fichiers spécifiés, puis tapez le mot détacher dans la zone de confirmation et choisissez Détacher.

Surveillance de Storage Gateway

Les rubriques de cette section décrivent comment surveiller une passerelle à l'aide d'Amazon CloudWatch, y compris la surveillance du stockage en cache et des autres ressources associées à la passerelle. Vous utilisez la console Storage Gateway pour afficher les métriques et les alarmes de votre passerelle. Par exemple, vous pouvez consulter le nombre d'octets utilisés dans les opérations de lecture et d'écriture, le temps passé dans les opérations de lecture et d'écriture et le temps nécessaire pour récupérer des données depuis le AWS Cloud. Avec les métriques, vous pouvez suivre l'intégrité de la passerelle et configurer des alarmes pour vous avertir lorsqu'une ou plusieurs métriques dépassent un seuil défini.

Storage Gateway fournit CloudWatch des métriques sans frais supplémentaires. Les métriques de Storage Gateway sont enregistrées pendant une période de deux semaines. En utilisant ces indicateurs, vous pouvez accéder à des informations historiques et avoir une meilleure idée des performances de vos passerelles. Storage Gateway fournit également des CloudWatch alarmes, à l'exception des alarmes haute résolution, sans frais supplémentaires. Pour plus d'informations sur CloudWatch les tarifs, consultez les CloudWatch tarifs Amazon. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Rubriques

- Comprendre les CloudWatch alarmes- Découvrez les informations de base sur les CloudWatch alarmes, y compris les états des alarmes et les configurations recommandées.
- Créez des CloudWatch alarmes recommandées- Découvrez comment configurer rapidement et automatiquement toutes les CloudWatch alarmes recommandées dans le cadre du processus de configuration initial de File Gateway.
- Création d'une CloudWatch alarme personnalisée- Découvrez comment créer une CloudWatch alarme personnalisée pour surveiller une métrique spécifique à l'aide de critères d'évaluation spécifiques pour déclencher des états d'alarme et envoyer des notifications.
- Surveillance de votre passerelle de - Apprenez à consulter les CloudWatch journaux et les journaux d'audit, et à trouver des informations sur les métriques spécifiques de la passerelle et du système de fichiers de partage de fichiers signalées par votre passerelle.

Comprendre les CloudWatch alarmes

CloudWatch les alarmes surveillent les informations relatives à votre passerelle en fonction de métriques et d'expressions. Vous pouvez ajouter des CloudWatch alarmes à votre passerelle et consulter leur statut dans la console Storage Gateway. Pour plus d'informations sur les métriques utilisées pour surveiller la passerelle de , voir de passerelle et Comprendre les métriques de système de fichiers. Pour chaque alarme, vous spécifiez les conditions qui activeront son état d'alarme. Les indicateurs de statut des alarmes de la console Storage Gateway deviennent rouges lorsque leur état est ALARME, ce qui facilite la surveillance proactive du statut. Vous pouvez configurer les alarmes pour qu'elles invoquent automatiquement des actions en fonction de changements d'état soutenus. Pour plus d'informations sur les CloudWatch alarmes, consultez la section Utilisation des CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.

> **Note**
>
> Si vous n'êtes pas autorisé à consulter CloudWatch, vous ne pouvez pas voir les alarmes.

Pour chaque passerelle activée, nous vous recommandons de créer les alarmes CloudWatch suivantes :

- Attente d'E/S élevée : `IoWaitpercent` >= 20 pour 3 points de données en 15 minutes
- Pourcentage de cache corrompu : `CachePercentDirty` > 80 pour 4 points de données en 20 minutes
- Échec du téléchargement des fichiers : `FilesFailingUpload` >= 1 pour 1 point de données dans les 5 minutes
- Erreur du système de fichiers : `FileSystem-ERROR` >= 1 pour 1 point de données dans les 5 minutes
- Notifications de santé : `HealthNotifications` >= 1 point de données pour 1 dans les 5 minutes. Lors de la configuration de cette alarme, définissez le Traitement des données manquantes sur notBreaching.

> **Note**
>
> Vous pouvez définir une alarme de notification d'intégrité seulement si la passerelle avait une notification d'intégrité antérieure dans CloudWatch.

Pour les passerelles situées sur des plateformes VMware hôtes faisant partie d'un cluster de VMware haute disponibilité, nous recommandons également cette CloudWatch alarme supplémentaire :

- Notifications de disponibilité : `AvailabilityNotifications` >= 1 point de données pour 1 dans les 5 minutes. Lors de la configuration de cette alarme, définissez le Traitement des données manquantes sur notBreaching.

Le tableau suivant décrit les états des CloudWatch alarmes.

State	Description
OK	La métrique ou l'expression se trouve dans le seuil défini.
Alarme	La métrique ou l'expression se trouve en dehors du seuil défini.
Données insuffisantes	L'alarme vient de démarrer, la métrique n'est pas disponible, ou la quantité de données n'est pas suffisante pour permettre à la métrique de déterminer l'état de l'alarme.
Aucun	Aucune alarme n'est créée pour la passerelle. Pour créer une nouvelle alarme, veuillez consulter Créez une CloudWatch alarme personnalisée pour votre passerelle.
Unavailable	L'état de l'alarme est inconnu. Choisissez Non disponible pour afficher les informations d'erreur dans l'onglet Surveillance.

Création d' CloudWatch alarmes recommandées pour votre passerelle

Lorsque vous créez une nouvelle passerelle à l'aide de la console Storage Gateway, vous pouvez choisir de créer automatiquement toutes les CloudWatch alarmes recommandées dans le cadre du processus de configuration initiale. Pour plus d'informations, consultez Configurer votre Amazon FSx

File Gateway. Si vous souhaitez ajouter ou mettre à jour les CloudWatch alarmes recommandées pour une passerelle existante après avoir terminé la première configuration, suivez la procédure suivante.

Pour ajouter ou mettre à jour les CloudWatch alarmes recommandées pour une passerelle existante

> **Note**
>
> Cette fonctionnalité nécessite des autorisations CloudWatch de politique, qui ne sont pas automatiquement accordées dans le cadre de la politique d'accès complet préconfigurée de Storage Gateway. Assurez-vous que votre politique de sécurité accorde les autorisations suivantes avant de tenter de créer les CloudWatch alarmes recommandées :
>
> - `cloudwatch:PutMetricAlarm` - créer des alarmes
> - `cloudwatch:DisableAlarmActions` - désactiver les actions d'alarme
> - `cloudwatch:EnableAlarmActions` - activer les actions d'alarme
> - `cloudwatch:DeleteAlarms` - supprimer des alarmes

1. Ouvrez la console Storage Gateway à l'adresse https://console.aws.amazon.com/storagegateway/home/.
2. Dans le volet de navigation sur le côté gauche de la page, choisissez Gateways, puis choisissez la passerelle pour laquelle vous souhaitez créer des CloudWatch alarmes recommandées.
3. Sur la page Détails de la passerelle, choisissez l'onglet Surveillance.
4. Sous Alarmes, choisissez Créer des alarmes recommandées. Les alarmes recommandées sont créées automatiquement.

   La section Alarmes répertorie toutes les CloudWatch alarmes pour une passerelle spécifique. À partir de là, vous pouvez sélectionner et supprimer une ou plusieurs alarmes, activer ou désactiver les actions d'alarme et créer de nouvelles alarmes.

Créez une CloudWatch alarme personnalisée pour votre passerelle

CloudWatch utilise Amazon Simple Notification Service (Amazon SNS) pour envoyer des notifications d'alarme lorsqu'une alarme change d'état. Une alarme surveille une seule métrique pendant une durée que vous définissez et exécute une ou plusieurs actions en fonction de la valeur de la métrique

par rapport à un seuil donné pendant un certain nombre de périodes. L'action est une notification qui est envoyée à une rubrique Amazon SNS. Vous pouvez créer une rubrique Amazon SNS lorsque vous créez une CloudWatch alarme. Pour plus d'informations sur Amazon SNS, consultez Qu'est-ce qu'Amazon SNS ? dans le Guide du développeur Amazon Simple Notification Service.

Pour créer une CloudWatch alarme dans 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 Passerelles, puis sélectionnez la passerelle pour laquelle vous souhaitez créer une alarme.
3. Sur la page de détails de la passerelle, choisissez l'onglet Surveillance.
4. Sous Alarmes, choisissez Créer une alarme pour ouvrir la CloudWatch console.
5. Utilisez la CloudWatch console pour créer le type d'alarme que vous souhaitez. Vous pouvez créer les types d'alarmes suivants :

   - Alarme de seuil statique : alarme basée sur un seuil défini pour une métrique choisie. L'alarme passe à l'état ALARM lorsque la métrique dépasse le seuil pendant un certain nombre de périodes d'évaluation.

     Pour créer une alarme à seuil statique, consultez la section Création CloudWatch d'une alarme basée sur un seuil statique dans le guide de CloudWatch l'utilisateur Amazon.
   - Alarme de détection d'anomalie : la détection d'anomalie exploite les données de métriques antérieures et crée un modèle de valeurs attendues. Vous définissez une valeur pour le seuil de détection des anomalies et vous CloudWatch utilisez ce seuil avec le modèle pour déterminer la plage de valeurs « normale » de la métrique. Une valeur plus élevée pour le seuil produit une bande plus épaisse de valeurs « normales ». Vous pouvez choisir d'activer l'alarme uniquement lorsque la valeur de la métrique dépasse le groupe de valeurs attendues, uniquement lorsqu'elle se situe sous le groupe ou lorsqu'elle est supérieure ou inférieure au groupe.

     Pour créer une alarme de détection d'anomalie, consultez la section Création CloudWatch d'une alarme basée sur la détection d'anomalies dans le guide de CloudWatch l'utilisateur Amazon.
   - Alarme d'expression mathématique basée sur une métrique : alarme basée sur une ou plusieurs métriques utilisées dans une expression mathématique. Vous spécifiez l'expression, le seuil et les périodes d'évaluation.

Pour créer une alarme d'expression mathématique métrique, consultez la section Création CloudWatch d'une alarme basée sur une expression mathématique métrique dans le guide de CloudWatch l'utilisateur Amazon.

- Alarme composite : alarme qui détermine son état en regardant l'état des autres alarmes. Une alarme composite peut aider à réduire le bruit de l'alarme.

  Pour créer une alarme composite, consultez la section Création d'une alarme composite dans le guide de CloudWatch l'utilisateur Amazon.

6. Après avoir créé l'alarme dans la CloudWatch console, revenez à la console Storage Gateway. Vous pouvez afficher l'alarme en procédant de l'une des manières suivantes :

   - Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle pour laquelle vous souhaitez afficher les alarmes. Dans l'onglet Détails, sous Alarmes, sélectionnez CloudWatch Alarmes.
   - Dans le volet de navigation, choisissez Passerelles, sélectionnez la passerelle pour laquelle vous souhaitez afficher les alarmes, puis choisissez l'onglet Surveillance.

     La section Alarmes répertorie toutes les CloudWatch alarmes pour une passerelle spécifique. À partir de là, vous pouvez sélectionner et supprimer une ou plusieurs alarmes, activer ou désactiver les actions d'alarme et créer de nouvelles alarmes.
   - Dans le volet de navigation, choisissez Passerelles, puis choisissez l'état d'alarme de la passerelle pour laquelle vous souhaitez afficher les alarmes.

Pour plus d'informations sur la modification ou la suppression d'une alarme, consultez la section Modification ou suppression d'une CloudWatch alarme.

> **Note**
>
> Lorsque vous supprimez une passerelle à l'aide de la console Storage Gateway, toutes les CloudWatch alarmes associées à la passerelle sont également automatiquement supprimées.

Surveillance de votre passerelle de

Vous pouvez surveiller votre passerelle de et les ressources associées à l'aide AWS Storage Gateway des CloudWatch métriques et des journaux d'audit Amazon. Vous pouvez également utiliser CloudWatch les événements pour être averti lorsque les opérations sur les fichiers sont terminées.

Rubriques

- Obtenir les journaux d'état de File Gateway avec des CloudWatch groupes de journaux
- Utilisation des CloudWatch métriques Amazon
- Présentation des métriques de la passerelle
- Comprendre les métriques du système de fichiers
- Comprendre les journaux d'audit de File Gateway

Obtenir les journaux d'état de File Gateway avec des CloudWatch groupes de journaux

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir des informations sur l'état de votre passerelle de et des ressources associées. Vous pouvez utiliser les journaux pour surveiller votre passerelle afin de détecter les erreurs qu'elle rencontre. En outre, vous pouvez utiliser les filtres CloudWatch d'abonnement Amazon pour automatiser le traitement des informations du journal en temps réel. Pour plus d'informations, consultez la section Traitement en temps réel des données de journal avec les abonnements dans le guide de CloudWatch l'utilisateur Amazon.

Par exemple, vous pouvez configurer un groupe de CloudWatch journaux pour surveiller votre passerelle et être averti lorsque votre passerelle de FSx fichiers ne parvient pas à télécharger des fichiers vers un système de FSx fichiers Amazon. Vous pouvez configurer le groupe soit lorsque vous activez la passerelle, soit une fois celle-ci 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 Configuration de votre Amazon FSx File Gateway. Pour obtenir des informations générales sur les groupes de CloudWatch journaux, consultez la section Working with Log Groups and Log Streams dans le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations sur la façon de résoudre les erreurs susceptibles d'être signalées par File Gateway, consultezRésolution des problèmes : problèmes liés à la passerelle de fichiers.

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

La procédure suivante explique comment configurer un groupe de CloudWatch journaux après l'activation de votre passerelle.

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

1. Connectez-vous à la console Storage Gateway AWS Management Console et ouvrez-la https://console.aws.amazon.com/storagegateway/chez vous.
2. Dans le volet de navigation, choisissez Gateways, puis choisissez la passerelle pour laquelle vous souhaitez configurer le groupe de CloudWatch journaux.
3. Pour Actions, choisissez Modifier les informations de la passerelle.
4. Pour Choisir le mode de configuration du groupe de journaux, sélectionnez l'une des options suivantes :

   - Créez un nouveau groupe de journaux pour créer un nouveau groupe de CloudWatch journaux.
   - Utilisez un groupe de journaux existant pour utiliser un groupe de CloudWatch journaux qui existe déjà.

     Choisissez un groupe de journaux dans la Liste de groupes de journaux existants.
   - Désactivez la journalisation si vous ne souhaitez pas surveiller votre passerelle à l'aide de groupes de CloudWatch journaux.
5. Sélectionnez Enregistrer les modifications.
6. Pour afficher les journaux d'intégrité de votre passerelle, procédez comme suit :

   1. Dans le volet de navigation, choisissez Gateways, puis choisissez la passerelle pour laquelle vous avez configuré le groupe de CloudWatch journaux.
   2. Choisissez l'onglet Détails, puis sous Health logs, sélectionnez CloudWatchLogs. La page des détails du groupe de journaux s'ouvre dans la CloudWatch console.

Utilisation des CloudWatch métriques Amazon

Vous pouvez obtenir des données de surveillance pour votre passerelle de à l'aide de l'API AWS Management Console ou de l' CloudWatch API. La console affiche une série de graphiques basés

sur les données brutes de l' CloudWatch API. L' CloudWatch API peut également être utilisée via l'un des outils AWS SDKsd' CloudWatch API Amazon. 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 CloudWatch console, vous pouvez utiliser la `Gateway Metrics` vue pour sélectionner des dimensions spécifiques à la passerelle. Pour plus d'informations sur les dimensions, consultez la section Dimensions du guide de CloudWatch l'utilisateur Amazon.
- Le nom de la métrique, par exemple `ReadBytes`.

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

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

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 :

- Afficher les métriques disponibles
- Obtenir des statistiques pour une métrique
- Création d'alarmes CloudWatch

Présentation des métriques de la passerelle

Le tableau suivant décrit les mesures qui couvrent les passerelles de FSx fichiers. Chaque passerelle est associée à un ensemble de métriques. Certaines métriques spécifiques à la passerelle portent le même nom que certaines métriques. file-system-specific Ces métriques représentent les mêmes types de mesures, mais elles sont limitées à la passerelle plutôt qu'au système de fichiers.

Spécifiez toujours si vous souhaitez travailler avec une passerelle ou un système de fichiers lorsque vous travaillez avec une métrique particulière. Plus précisément, lorsque vous travaillez avec des métriques de passerelle, vous devez spécifier celles `Gateway Name` de la passerelle dont vous souhaitez consulter les données métriques. Pour de plus amples informations, veuillez consulter Utilisation des CloudWatch métriques Amazon.

> **Note**
>
> Certaines métriques renvoient des points de données uniquement lorsque de nouvelles données ont été générées au cours de la période de surveillance la plus récente.

Le tableau suivant décrit les métriques que vous pouvez utiliser pour obtenir des informations sur vos passerelles de fichiers .

Métrique	Description
`AvailabilityNotifications`	Cette métrique indique le nombre de notificat ions de santé liées à la disponibilité qui ont été générées par la passerelle au cours de la période de référence. Unités : nombre
`CacheDirectorySize`	Cette métrique permet de suivre la taille des dossiers dans le cache de la passerell

Métrique	Description
	e. La taille du dossier est déterminée par le nombre de fichiers et de sous-dossiers de son premier niveau, cela ne compte pas de manière récursive dans les sous-dossiers. Utilisez cette métrique avec la `Average` statistique pour mesurer la taille moyenne d'un dossier dans le cache de la passerelle. Utilisez cette métrique avec la `Max` statistique pour mesurer la taille maximale d'un dossier dans le cache de la passerelle. Unités : nombre
`CacheFileSize`	Cette métrique permet de suivre la taille des fichiers dans le cache de la passerelle. Utilisez cette métrique avec la `Average` statistique pour mesurer la taille moyenne d'un fichier dans le cache de la passerelle. Utilisez cette métrique avec la `Max` statistique pour mesurer la taille maximale d'un fichier dans le cache de la passerelle. Unités : octets
`CacheFree`	Cette métrique indique le nombre d'octets disponibles dans le cache de la passerelle. Unités : octets

Métrique	Description
`CacheHitPercent`	Pourcentage des opérations de lecture d'applications depuis la passerelle qui sont servies à partir du cache. L'exemple est pris à la fin de la période de génération de rapport. Lorsqu'aucune opération de lecture d'applica tion n'est effectuée depuis la passerelle, cette métrique indique 100 %. Unités : pourcentage
`CachePercentDirty`	Pourcentage global du cache de passerelle qui n'a pas été conservé. AWS L'exemple est pris à la fin de la période de génération de rapport. Unités : pourcentage
`CachePercentUsed`	Pourcentage global du stockage du cache de passerelle utilisé. L'exemple est pris à la fin de la période de génération de rapport. Unités : pourcentage
`CacheUsed`	Cette métrique indique le nombre d'octets utilisés dans le cache de la passerelle. Unités : octets
`CloudBytesDownloaded`	Nombre total d'octets à partir desquels la passerelle a effectué le téléchargement AWS au cours de la période de référence. Utilisez cette métrique avec la statistique `Sum` pour mesurer le débit et avec la statistique `Samples` pour mesurer les IOPS. Unités : octets

Métrique	Description
`CloudBytesUploaded`	Nombre total d'octets vers lesquels la passerell e s'est chargée au AWS cours de la période de référence. Utilisez cette métrique avec la `Sum` statistiq ue pour mesurer le débit et avec la `Samples` statistique pour mesurer les input/output opérations par seconde (IOPS). Unités : octets
`FilesFailingUpload`	Cette métrique permet de suivre le nombre de fichiers vers lesquels le téléchargement échoue AWS. Ces fichiers généreront des notifications de santé contenant plus d'informations sur le problème. Utilisez cette métrique avec la `Sum` statistique pour indiquer le nombre de fichiers sur lesquels le téléchargement échoue actuellement. AWS Unités : nombre
`FileShares`	Cette métrique indique le nombre de partages de fichiers sur la passerelle. Unités : nombre

Métrique	Description
`FileSystem-ERROR`	Cette métrique indique le nombre d'associations de systèmes de fichiers sur ces passerelles qui sont dans l'état ERROR. Si cette métrique indique que des associations de systèmes de fichiers sont à l'état ERROR, il est probable qu'il y ait un problème avec la passerelle susceptible de perturber votre flux de travail. Il est recommandé de créer une alarme lorsque cette métrique indique une valeur différente de zéro. Unités : nombre
`HealthNotifications`	Cette métrique indique le nombre de notifications de santé générées par cette passerelle au cours de la période de référence. Unités : nombre
`IndexEvictions`	Cette métrique indique le nombre de fichiers dont les métadonnées ont été supprimées de l'index des métadonnées des fichiers mis en cache pour faire de la place à de nouvelles entrées. La passerelle gère cet index de métadonnées, qui est renseigné à la demande à partir du AWS Cloud. Unités : nombre

Métrique	Description
`IndexFetches`	Cette métrique indique le nombre de fichiers pour lesquels des métadonnées ont été extraites. La passerelle gère un index en cache des métadonnées des fichiers, qui est renseigné à la demande à partir du AWS Cloud. Unités : nombre
`IoWaitPercent`	Cette métrique indique le pourcentage de temps pendant lequel le processeur attend une réponse du disque local. Unités : pourcentage
`MemTotalBytes`	Cette métrique indique la quantité totale de mémoire sur la passerelle. Unités : octets
`MemUsedBytes`	Cette métrique indique la quantité de mémoire utilisée sur la passerelle. Unités : octets

Métrique	Description
`RootDiskFreeBytes`	Cette métrique indique le nombre d'octets disponibles sur le disque racine de la passerelle. Si cette métrique indique que moins de 20 Go sont disponibles, vous devez augmenter la taille du disque racine. Pour augmenter la taille du disque racine, vous pouvez augmenter la taille du disque racine existant sur la machine virtuelle. Lorsque la machine virtuelle est redémarrée, la passerelle reconnaît l'augmentation de la taille du disque racine. Unités : octets
`SmbV2Sessions`	Cette métrique indique le nombre de SMBv2 sessions actives sur la passerelle. Cette métrique est émise une fois pour chaque système de fichiers associé à la passerelle. Utilisez la statistique SUM pour calculer le nombre total de SMBv2 sessions actives dans tous les systèmes de fichiers. Unités : nombre
`SmbV3Sessions`	Cette métrique indique le nombre de SMBv3 sessions actives sur la passerelle. Cette métrique est émise une fois pour chaque système de fichiers associé à la passerelle. Utilisez la statistique SUM pour calculer le nombre total de SMBv3 sessions actives dans tous les systèmes de fichiers. Unités : nombre

Métrique	Description
`TotalCacheSize`	Cette métrique indique la taille totale du cache. Unités : octets
`UserCpuPercent`	Cette métrique indique le pourcentage de temps consacré au traitement de la passerelle. Unités : pourcentage

Comprendre les métriques du système de fichiers

Vous trouverez ci-dessous des informations sur les métriques de Storage Gateway qui couvrent les systèmes de fichiers. Chaque système de fichiers est associé à un ensemble de métriques. Certaines métriques spécifiques au système de fichiers portent le même nom que certaines métriques spécifiques à la passerelle. Ces métriques représentent les mêmes types de mesures, mais elles sont limitées au système de fichiers.

Spécifiez toujours si vous souhaitez utiliser une métrique de passerelle ou de système de fichiers avant de travailler avec une métrique. Plus précisément, lorsque vous travaillez avec des métriques de système de fichiers, vous devez spécifier celles `File system ID` qui identifient le système de fichiers pour lequel vous souhaitez consulter les métriques. Pour de plus amples informations, veuillez consulter Utilisation des CloudWatch métriques Amazon.

> **Note**
>
> Certaines métriques renvoient des points de données uniquement lorsque de nouvelles données ont été générées au cours de la période de surveillance la plus récente.

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

Métrique	Description
`CacheHitPercent`	Pourcentage d'opérations de lecture d'applica tions à partir des partages de fichiers servis à

Métrique	Description
	partir du cache. L'exemple est pris à la fin de la période de génération de rapport. Lorsqu'aucune opération de lecture d'application n'est effectuée depuis le partage de fichiers, cette métrique indique 100 %. Unités : pourcentage
`CachePercentDirty`	Contribution du partage de fichiers au pourcentage global du cache de la passerelle qui n'a pas été conservé. AWS L'exemple est pris à la fin de la période de génération de rapport. Utilisez cette métrique avec la `Sum` statistique. Idéalement, cette métrique devrait rester faible. **Note** Utilisez la `CachePercentDirty` métrique de la passerelle pour afficher le pourcentage global du cache de la passerelle qui n'a pas été conservé. AWS Unités : pourcentage

Métrique	Description
`CachePercentUsed`	Pourcentage du cache de données utilisé sur l'ensemble de la passerelle. L'exemple est pris à la fin de la période de génération de rapport. Cette métrique spécifique au partage de fichiers indique la même valeur que la métrique spécifique à la passerelle correspon dante. Unités : pourcentage
`CloudBytesUploaded`	Nombre total d'octets vers lesquels la passerell e s'est chargée au AWS cours de la période de référence. Utilisez cette métrique avec la statistique `Sum` pour mesurer le débit et avec la statistique `Samples` pour mesurer les IOPS. Unités : octets
`CloudBytesDownloaded`	Nombre total d'octets à partir desquels la passerelle a effectué le téléchargement AWS au cours de la période de référence. Utilisez cette métrique avec la `Sum` statistiq ue pour mesurer le débit et avec la `Samples` statistique pour mesurer les input/output opérations par seconde (IOPS). Unités : octets

Métrique	Description
`FilesFailingUpload`	Cette métrique permet de suivre le nombre de fichiers vers lesquels le téléchargement échoue AWS. Ces fichiers généreront des notifications de santé contenant plus d'informations sur le problème. Utilisez cette métrique avec la `Sum` statistique pour indiquer le nombre de fichiers sur lesquels le téléchargement échoue actuellement. AWS Unités : nombre
`ReadBytes`	Nombre total d’octets lus depuis vos applicati ons sur site au cours de la période de générati o n de rapport pour un partage de fichier. Utilisez cette métrique avec la statistique `Sum` pour mesurer le débit et avec la statistique `Samples` pour mesurer les IOPS. Unités : octets
`WriteBytes`	Nombre total d’octets écrits dans vos applicati ons sur site au cours de la période de générati o n de rapport. Utilisez cette métrique avec la statistique `Sum` pour mesurer le débit et avec la statistique `Samples` pour mesurer les IOPS. Unités : octets

Comprendre les journaux d'audit de File Gateway

Les journaux d'audit d'Amazon FSx FSx File Gateway (File Gateway) vous fournissent des informations sur l'accès des utilisateurs aux fichiers et aux dossiers au sein d'une association de

systèmes de fichiers. Vous pouvez utiliser les journaux d'audit pour surveiller les activités des utilisateurs et prendre des mesures si des modèles d'activité inappropriés sont identifiés. Les journaux sont formatés de la même manière que les événements des journaux de sécurité de Windows Server, afin de garantir la compatibilité avec les outils de traitement des journaux existants pour les événements de sécurité Windows.

Opérations

Le tableau suivant décrit les opérations d'accès aux FSx fichiers journaux d'audit de File Gateway.

Nom de l’opération	Définition
Lire des données	Lisez le contenu d'un fichier.
Écrire des données	Modifiez le contenu d'un fichier.
Créer	Créer un nouveau fichier ou dossier.
Rename	Renommer un fichier ou un dossier existant.
Suppression	Supprimer un fichier ou un dossier.
Écrire des attributs	Mettez à jour les métadonnées d'un fichier ou d'un dossier (propriétaireACLs, groupe, autorisations).

Attributs

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

Attribut	Définition
`securityDescriptor`	Affiche la liste ACL discrétionnaire (DACL) définie sur un objet, au format SDDL.
`sourceAddress`	Adresse IP de la machine cliente de partage de fichiers.

Attribut	Définition
`SubjectDomainName`	Domaine Active Directory (AD) auquel appartient le compte du client.
`SubjectUserName`	Le nom d'utilisateur Active Directory du client.
`source`	ID du Storage Gateway `FileSyste mAssociation` en cours d'audit.
`mtime`	Moment où le contenu de l'objet a été modifié, défini par le client.
`version`	Version du format du journal d'audit.
`ObjectType`	Définit si l'objet est un fichier ou un dossier.
`locationDnsName`	Le nom DNS du système FSx File Gateway.
`objectName`	Chemin d'accès complet à l'objet.
`ctime`	Moment où le contenu ou les métadonnées de l'objet a été modifié, défini par le client.
`shareName`	Nom du partage auquel vous accédez.
`operation`	Nom de l'opération d'accès à l'objet.
`newObjectName`	Chemin d'accès complet au nouvel objet après qu'il a été renommé.
`gateway`	ID de la passerelle de stockage.
`status`	L'état de l'opération. Seul le succès est enregistré (les échecs sont enregistrés à l'exception des échecs liés au refus d'autoris ations).
`fileSizeInBytes`	Taille du fichier en octets, définie par le client au moment de la création du fichier.

Attributs enregistrés par opération

Le tableau suivant décrit les attributs du journal d'audit de FSx File Gateway enregistrés lors de chaque opération d'accès aux fichiers.

	Lire les données	Écrire des données	Créer un dossier	Créer un fichier	Renomme le fichier/ dossier	Supprime un fichier/ dossier	Écrire des attributs (modifier l'ACL)	Écrire des attributs (chown)	Écrire des attributs (chmod)	Écrire des attributs (chgrp)
securi escrip							X			
source ress	X	X	X	X	X	X	X	X	X	X
Subjec mainNa	X	X	X	X	X	X	X	X	X	X
Subjec erName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
versio	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
locati nsName	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
ctime			X	X						

	Lire les données	Écrire des données	Créer un dossier	Créer un fichier	Renomme le fichier/ d ossier	Supprime un fichier/ d ossier	Écrire des attributs (modifier l'ACL)	Écrire des attributs (chown)	Écrire des attributs (chmod)	Écrire des attributs (chgrp)
shareN	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
newObj Name					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSi nBytes				X						

Maintenance de votre passerelle

Maintenance de votre Amazon FSx File Gateway implique d'effectuer une maintenance générale afin d'optimiser les performances de votre passerelle. Ces tâches sont communes à tous les types de passerelle.

Cette section contient les rubriques suivantes, qui décrivent les concepts et les procédures liés à la maintenance de votre Amazon FSx File Gateway () :

Rubriques

- Gestion des mises à jour de passerelle— Découvrez comment activer ou désactiver les mises à jour de maintenance et comment modifier le calendrier des fenêtres de maintenance pour votre passerelle de fichiers.
- Exécution de tâches de maintenance à l'aide de la console locale— Découvrez comment effectuer des tâches de maintenance à l'aide de la console locale de la passerelle.
- Arrêt de votre machine virtuelle de passerelle— Découvrez ce qu'il convient de faire si vous devez arrêter ou redémarrer votre machine virtuelle de passerelle pour des raisons de maintenance, par exemple lorsque vous appliquez un correctif à votre hyperviseur.
- Remplacement de votre passerelle de existante par une nouvelle instance— Découvrez comment remplacer votre passerelle de par une nouvelle instance lorsque vous souhaitez améliorer les performances ou répondre à une notification de migration de la passerelle.
- Suppression de votre passerelle et suppression des ressources associées— Découvrez comment supprimer votre passerelle à l'aide de la AWS Storage Gateway console et nettoyer les ressources associées pour éviter d'être facturées pour leur utilisation continue.

Gestion des mises à jour de passerelle

Storage Gateway se compose d'un composant de services cloud gérés et d'un composant d'appliance de passerelle que vous déployez sur site ou sur une instance Amazon EC2 dans AWS le cloud. Les deux composants font l'objet de mises à jour régulières. Les rubriques de cette section décrivent la cadence de ces mises à jour, la manière dont elles sont appliquées et comment configurer les paramètres liés aux mises à jour sur les passerelles de votre déploiement.

> **Important**
>
> Vous devez traiter l'appliance Storage Gateway comme une machine virtuelle gérée et ne pas tenter d'accéder à son installation ou à son contenu ou de les modifier de quelque manière que ce soit. Toute tentative d'installation ou de mise à jour de progiciels à l'aide de méthodes autres que le mécanisme normal de mise à jour de la AWS passerelle (par exemple, les outils SSM ou d'hyperviseur) peut entraîner un dysfonctionnement de la passerelle.
>
> Storage Gateway applique automatiquement et régulièrement des correctifs à l'appliance pour garantir la sécurité et la stabilité. Les appliances Storage Gateway utilisent Amazon Linux comme système d'exploitation de base. Vous pouvez vérifier l'état des problèmes CVE (Common Vulnerabilities and Exposures) détectés sur le Amazon Linux Security Center. Les correctifs CVE sont automatiquement appliqués dans les 30 jours suivant leur publication, comme indiqué sur le Amazon Linux Security Center. Les correctifs sont installés pendant le calendrier de maintenance de votre passerelle, à condition que celle-ci soit en ligne.
>
> Storage Gateway ne prend pas en charge la mise à jour manuelle d'une passerelle Amazon EC2 à l'aide des directives cloud-init. Si vous utilisez cette méthode pour mettre à jour une passerelle, vous pouvez rencontrer des problèmes d'interopérabilité qui vous empêchent d'activer ou d'utiliser le dispositif de passerelle.

Fréquence de mise à jour et comportement attendu

AWS met à jour le composant des services cloud selon les besoins sans perturber les passerelles déployées. Vos dispositifs de passerelle déployés reçoivent les types de mises à jour suivants :

- Maintenance : mises à jour régulières pouvant inclure des mises à niveau du système d'exploitation et du logiciel, des correctifs pour améliorer la stabilité, les performances et la sécurité, ainsi que l'accès aux nouvelles fonctionnalités.
- Urgent : mises à jour critiques qui incluent les correctifs requis pour les problèmes ayant un impact immédiat sur la sécurité, les performances ou la durabilité de votre passerelle. Des mises à jour urgentes peuvent être publiées à tout moment, en dehors du rythme normal de maintenance mensuelle et de mise à jour des fonctionnalités.

Toutes les mises à jour sont cumulatives et mettent à niveau les passerelles vers la version actuelle lorsqu'elles sont appliquées. Pour plus d'informations sur les modifications spécifiques incluses dans chaque mise à jour, consultez les .

Toutes les mises à jour de l'appliance Gateway peuvent provoquer une brève interruption de service. L'hôte de la machine virtuelle de la passerelle n'a pas besoin de redémarrer pendant les mises à jour, mais la passerelle sera indisponible pendant une courte période pendant la mise à jour et le redémarrage de l'appliance de passerelle.

Lorsque vous déployez et activez votre passerelle, un calendrier de maintenance par défaut est défini. Vous pouvez modifier le calendrier de la fenêtre de maintenance à tout moment. Vous pouvez également désactiver les mises à jour de maintenance, mais nous vous recommandons de les laisser activées.

> **Note**
>
> Les mises à jour urgentes seront appliquées conformément au calendrier de la fenêtre de maintenance, même si les mises à jour de maintenance régulières sont désactivées.

Avant qu'une mise à jour ne soit appliquée à votre passerelle, vous en AWS informe par un message sur la console Storage Gateway et sur votre Tableau de bord AWS Health. Pour de plus amples informations, veuillez consulter Tableau de bord AWS Health. Pour modifier l'adresse e-mail à laquelle les notifications de mise à jour logicielle sont envoyées, voir Mettre à jour les contacts secondaires de votre AWS compte dans le Guide de référence de gestion des AWS comptes.

Lorsque des mises à jour sont disponibles, l'onglet Détails de la passerelle affiche un message de maintenance. Vous pouvez également voir la date et l'heure auxquelles la dernière mise à jour réussie a été appliquée dans l'onglet Détails.

Activer ou désactiver les mises à jour de maintenance

Lorsque les mises à jour de maintenance sont activées, votre passerelle les applique automatiquement en fonction du calendrier de fenêtre de maintenance configuré. Pour plus d'informations, voir de la fenêtre de maintenance de la passerelle.

Si les mises à jour de maintenance sont désactivées, la passerelle ne les appliquera pas automatiquement, mais vous pouvez toujours les appliquer manuellement à l'aide de la console, de l'API ou de la CLI de Storage Gateway. Des mises à jour urgentes seront parfois appliquées pendant la fenêtre de maintenance configurée, quel que soit ce paramètre.

> **Note**
>
> La procédure suivante décrit comment activer ou désactiver les mises à jour de passerelle à l'aide de la console Storage Gateway. Pour modifier ce paramètre par programmation à l'aide de l'API, consultez UpdateMaintenanceStartTimele manuel Storage Gateway API Reference.

Pour activer ou désactiver les mises à jour de maintenance à l'aide de la console Storage Gateway :

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Gateways, puis choisissez la passerelle pour laquelle vous souhaitez configurer les mises à jour de maintenance.
3. Choisissez Actions, puis sélectionnez Modifier les paramètres de maintenance.
4. Pour les mises à jour de maintenance, sélectionnez Activé ou Désactivé.
5. Choisissez Enregistrer les modifications lorsque vous avez terminé.

Vous pouvez vérifier le paramètre mis à jour dans l'onglet Détails de la passerelle sélectionnée dans la console Storage Gateway.

Modifier le calendrier de la fenêtre de maintenance de la passerelle

Si les mises à jour de maintenance sont activées, votre passerelle applique automatiquement ces mises à jour conformément au calendrier de la fenêtre de maintenance. Des mises à jour urgentes seront parfois appliquées pendant la fenêtre de maintenance que vous avez configurée, quel que soit le paramètre des mises à jour de maintenance.

> **Note**
>
> La procédure suivante explique comment modifier le calendrier de la fenêtre de maintenance à l'aide de la console Storage Gateway. Pour modifier ce paramètre par programmation à l'aide de l'API, consultez UpdateMaintenanceStartTimele manuel Storage Gateway API Reference.

Pour modifier le calendrier de la fenêtre de maintenance à l'aide de la console Storage Gateway :

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Gateways, puis choisissez la passerelle pour laquelle vous souhaitez configurer les mises à jour de maintenance.
3. Choisissez Actions, puis sélectionnez Modifier les paramètres de maintenance.
4. Sous Heure de début de la fenêtre de maintenance, procédez comme suit :

   a. Pour Planifier, choisissez Hebdomadaire ou Mensuel pour définir la cadence de la fenêtre de maintenance.

   b. Si vous choisissez Hebdomadaire, modifiez les valeurs du jour de la semaine et de l'heure afin de définir le point précis de chaque semaine où la fenêtre de maintenance débutera.

      Si vous choisissez Mensuel, modifiez les valeurs du jour du mois et de l'heure afin de définir le point précis de chaque mois où la fenêtre de maintenance débutera.

      > **Note**
      >
      > La valeur maximale pouvant être définie pour le jour du mois est 28. Il est impossible de définir le calendrier de maintenance de façon à ce qu'il commence les jours 29 à 31.
      > Si vous recevez un message d'erreur lors de la configuration de ce paramètre, cela signifie peut-être que votre logiciel de passerelle n'est pas à jour. Envisagez d'abord de mettre à jour votre passerelle manuellement, puis de réessayer de configurer le calendrier de la fenêtre de maintenance.

5. Choisissez Enregistrer les modifications lorsque vous avez terminé.

Vous pouvez vérifier les paramètres mis à jour dans l'onglet Détails de la passerelle sélectionnée dans la console Storage Gateway.

Appliquer une mise à jour manuellement

Si une mise à jour logicielle est disponible pour votre passerelle, vous pouvez l'appliquer manuellement en suivant la procédure ci-dessous. Ce processus de mise à jour manuelle ignore le

calendrier de la fenêtre de maintenance et applique la mise à jour immédiatement, même si les mises à jour de maintenance sont désactivées.

> **Note**
>
> La procédure suivante décrit comment appliquer manuellement une mise à jour à l'aide de la console Storage Gateway. Pour effectuer cette action par programmation à l'aide de l'API, reportez-vous UpdateGatewaySoftwareNowà la section Storage Gateway API Reference.

Pour appliquer manuellement une mise à jour logicielle de passerelle à l'aide de la console Storage Gateway :

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Gateways, puis choisissez la passerelle que vous souhaitez mettre à jour.

   Si une mise à jour est disponible, la console affiche une bannière de notification bleue dans l'onglet Détails de la passerelle, qui inclut une option permettant d'appliquer la mise à jour.
3. Choisissez Appliquer la mise à jour maintenant pour mettre immédiatement à jour la passerelle.

   > **Note**
   >
   > Cette opération entraîne une interruption temporaire des fonctionnalités de la passerelle pendant l'installation de la mise à jour. Pendant ce temps, l'état de la passerelle apparaît OFFLINE dans la console Storage Gateway. Une fois l'installation de la mise à jour terminée, la passerelle reprend son fonctionnement normal et son statut passe à RUNNING.

Vous pouvez vérifier que le logiciel de passerelle a été mis à jour avec la dernière version en consultant l'onglet Détails de la passerelle sélectionnée dans la console Storage Gateway.

Exécution de tâches de maintenance à l'aide de la console locale

Cette section contient les rubriques suivantes, qui fournissent des informations sur la façon d'effectuer des tâches de maintenance à l'aide de la console locale de l'appliance Gateway. Vous

pouvez effectuer ces tâches en accédant à la console locale par le biais de la machine virtuelle locale ou de l'instance Amazon EC2 qui héberge votre dispositif de passerelle. La plupart des tâches sont communes aux différentes plateformes hôtes, mais elles présentent également certaines différences.

Rubriques

- Accès à la console locale de la passerelle- Découvrez comment vous connecter à la console locale d'une passerelle sur site hébergée sur une machine virtuelle basée sur un noyau Linux (KVM) VMware ESXi ou sur une plateforme Microsoft Hyper-V Manager.
- Exécution de tâches sur la console locale de la machine virtuelle- Apprenez à utiliser la console locale pour effectuer des tâches de configuration de base et avancées pour une passerelle locale, telles que la configuration d'un proxy HTTP, l'affichage de l'état des ressources système ou l'exécution de commandes de terminal.
- Exécution de tâches sur la console locale de la passerelle Amazon EC2- Apprenez à vous connecter à la console locale pour effectuer des tâches de configuration de base et avancées pour une passerelle Amazon EC2, telles que la configuration d'un proxy HTTP, l'affichage de l'état des ressources système ou l'exécution de commandes de terminal.

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 la machine virtuelle basée sur le noyau Linux (KVM) 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 Gateway 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 ceux VMs qui sont actuellement disponibles dans KVM.

   ```
   # virsh list
   ```

   La commande renvoie une liste VMs avec les informations d'identifiant, de nom et d'état pour chacune d'entre elles. Notez le `Id` nom de la machine virtuelle pour laquelle vous souhaitez lancer la console locale de la passerelle.
2. Utilisez la commande suivante pour accéder à la console locale.

   ```
   # virsh console Id
   ```

   *Id*Remplacez-le par l'ID de la machine virtuelle que vous avez noté à l'étape précédente.

   La console locale de l' AWS Appliance Gateway vous invite à vous connecter pour modifier la configuration de votre réseau et d'autres paramètres.
3. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter à la console locale de la passerelle. Pour plus d'informations, voir Connexion à la console locale de File Gateway.

   Une fois connecté, le menu Activation de l'AWS appliance - Configuration apparaît. Vous pouvez sélectionner les options du menu pour effectuer des tâches de configuration de passerelle. Pour plus d'informations, voir Exécution de tâches sur la console locale de la machine virtuelle.

Accès à la console locale de Gateway avec VMware ESXi

Pour accéder à la console locale de votre passerelle avec VMware ESXi

1. Dans le client VMware vSphere, sélectionnez votre machine virtuelle de passerelle.
2. Assurez-vous que la machine virtuelle de passerelle est activée.

   > **Note**
   >
   > Si votre machine virtuelle de passerelle est activée, une icône en forme de flèche verte apparaît avec l'icône de machine virtuelle dans le panneau du navigateur de machine virtuelle sur le côté gauche de la fenêtre de l'application. Si votre machine virtuelle

de passerelle n'est pas activée, vous pouvez l'activer en cliquant sur l'icône verte d'alimentation sur la barre d'outils en haut de la fenêtre de l'application.

3. Choisissez l'onglet Console dans le panneau d'informations principal sur le côté droit de la fenêtre de l'application.

   Après quelques instants, la console locale de l' AWS Appliance Gateway vous invite à vous connecter pour modifier la configuration de votre réseau et d'autres paramètres.

   > **Note**
   >
   > Pour libérer le curseur de la fenêtre de console, appuyez sur Ctrl+Alt.

4. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter à la console locale de la passerelle. Pour plus d'informations, voir Connexion à la console locale de File Gateway.

   Une fois connecté, le menu Activation de l'AWS appliance - Configuration apparaît. Vous pouvez sélectionner les options du menu pour effectuer des tâches de configuration de passerelle. Pour plus d'informations, voir Exécution de tâches sur la console locale de la machine virtuelle.

Accéder à la console locale de passerelle avec Microsoft Hyper-V

Pour accéder à la console locale de votre passerelle (Microsoft Hyper-V)

1. Sélectionnez la machine virtuelle de votre dispositif de passerelle dans le panneau Machines virtuelles situé sur le côté gauche de la fenêtre de l'application Microsoft Hyper-V Manager.
2. Vérifiez que la passerelle est activée.

   > **Note**
   >
   > Si votre machine virtuelle de passerelle est activée, elle `Running` est affichée dans la colonne État de la machine virtuelle du panneau Machines virtuelles sur le côté gauche de la fenêtre de l'application. Si votre machine virtuelle de passerelle n'est pas activée, vous pouvez l'activer en choisissant Démarrer dans le panneau Actions situé sur le côté droit de la fenêtre de l'application.

3. Choisissez Connect dans le panneau Actions.

La fenêtre Connexion de la machine virtuelle s’affiche. Si une fenêtre d’authentification s’affiche, tapez les informations d’identification fournies par l’administrateur de l’hyperviseur.

Après quelques instants, la console locale de l' AWS Appliance Gateway vous invite à vous connecter pour modifier la configuration de votre réseau et d'autres paramètres.

4. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter à la console locale de la passerelle. Pour plus d'informations, voir Connexion à la console locale de File Gateway.

   Une fois connecté, le menu Activation de l'AWS appliance - Configuration apparaît. Vous pouvez sélectionner les options du menu pour effectuer des tâches de configuration de passerelle. Pour plus d'informations, voir Exécution de tâches sur la console locale de la machine virtuelle.

Exécution de tâches sur la console locale de la machine virtuelle

Pour une passerelle de fichiers déployée sur site, vous pouvez effectuer les tâches de maintenance suivantes à l'aide de la console locale de l'hôte de la machine virtuelle. Ces tâches sont communes aux VMware hyperviseurs Microsoft Hyper-V et aux hyperviseurs KVM (Linux Kernel Virtual Machine).

Rubriques

- Connexion à la console locale de File Gateway- Apprenez à vous connecter à la console locale où vous pouvez configurer les paramètres réseau de la passerelle et modifier le mot de passe par défaut.
- Configuration d’un proxy HTTP- Découvrez comment configurer Storage Gateway pour acheminer tout le trafic des AWS terminaux via un serveur proxy.
- Configuration des paramètres réseau de votre passerelle- Découvrez comment configurer votre passerelle pour utiliser le DHCP ou une adresse IP statique.
- Test de la connectivité réseau de la passerelle- Découvrez comment utiliser la console locale de la passerelle pour tester la connectivité réseau.
- Affichage de l’état des ressources système de la passerelle- Découvrez comment vérifier les cœurs de processeur virtuels, la taille du volume racine et la RAM de votre passerelle.
- Configuration d'un serveur NTP (Network Time Protocol) pour votre passerelle- Apprenez à afficher et à modifier les configurations du serveur NTP (Network Time Protocol) et à synchroniser l'heure sur votre passerelle avec l'hôte de votre hyperviseur.

- Exécution des commandes Storage Gateway sur la console locale- Apprenez à exécuter des commandes de console locales pour effectuer des tâches telles que l'enregistrement de tables de routage Support, la connexion à, etc.

Connexion à la console locale de File Gateway

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 de la machine virtuelle, vous utilisez les informations d'identification temporaires pour vous connecter. Ces informations d'identification temporaires vous donnent accès à des menus dans lesquels vous pouvez configurer les paramètres réseau de la passerelle et modifier le mot de passe depuis la console locale. Le nom d'utilisateur initial est `admin` et le mot de passe temporaire est`password`. Vous devez modifier le mot de passe lors de votre première connexion.

Pour modifier le mot de passe temporaire

1. Dans le menu principal Activation de l'AWS appliance - Configuration, entrez le chiffre correspondant pour Gateway Console.
2. Exécutez la commande `passwd`. Pour plus d'informations sur l'exécution de la commande, consultez Exécution des commandes Storage Gateway sur la console locale.

Définition du mot de passe de la console locale depuis la console Storage Gateway

Vous pouvez également gérer le mot de passe de la console locale depuis la console Web Storage Gateway. Toute mise à jour réussie du mot de passe effectuée avec la console Web remplacera le mot de passe utilisé par la console locale de la machine virtuelle de passerelle, y compris le mot de passe temporaire si vous ne vous êtes jamais connecté localement. Si la passerelle n'est actuellement pas accessible via le réseau, le processus de mise à jour du mot de passe échouera.

Pour définir le mot de passe de la console locale sur la console Storage Gateway

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Gateways, 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).

   Votre nouveau mot de passe remplace le mot de passe actuel. Le service Storage Gateway n'enregistre, ne stocke ni n'enregistre le mot de passe, mais le transmet en toute sécurité via un canal crypté à la machine virtuelle, où il est stocké en toute sécurité.

   > **Note**
   >
   > Le mot de passe peut être composé de n'importe quel caractère du clavier et d'une longueur 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 de proxy prise en charge par les passerelles 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. Une fois que vous l'avez fait, Storage Gateway achemine tout le trafic des AWS terminaux via votre serveur proxy. Les communications entre la passerelle et les points de terminaison sont cryptées, même lors de l’utilisation du 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 connexion à la console VMware ESXi locale, consultezAccès à la console locale de Gateway 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 le menu principal Activation de l'appliance AWS - Configuration, entrez le chiffre correspondant pour sélectionner Configurer le proxy HTTP.
3. Dans le menu Configuration du proxy HTTP d'activation de l'appliance AWS , entrez le chiffre correspondant à la tâche que vous souhaitez effectuer :

   - Configurer le proxy HTTP : vous devez fournir un nom d'hôte et un port pour finaliser la configuration.
   - Afficher la configuration actuelle du proxy HTTP : 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.
   - Supprimer une configuration de proxy HTTP : le message `HTTP Proxy Configuration Removed` s'affiche.
4. 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

1. Connectez-vous à la console locale de la passerelle :

   - Pour plus d'informations sur la connexion à la console VMware ESXi locale, consultezAccès à la console locale de Gateway 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 le menu principal Activation de l'AWS appliance - Configuration, entrez le chiffre correspondant pour sélectionner Configuration réseau.

3. Dans le menu Configuration réseau, effectuez l'une des tâches suivantes :

Pour exécuter cette tâche	Procédez comme suit
Collecter des informations sur votre carte réseau	Saisissez le chiffre correspondant pour sélectionner Décrire la carte. La liste des noms d'adaptateurs s'affiche et vous êtes invité à saisir 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 : • Adresse MAC • Adresse IP • Masque réseau • Adresse IP de la passerelle • État activé DHCP Vous utilisez les noms d'adaptateur répertoriés ici lorsque vous configurez une adresse IP statique ou lorsque vous définissez l'adaptateur par défaut de votre passerelle.
Configuration du routage DHCP	Saisissez le chiffre correspondant pour sélectionner Configurer le DHCP. Vous êtes invité à configurer l'interface réseau pour utiliser le protocole DHCP.

Pour exécuter cette tâche	Procédez comme suit
Configurer une adresse IP statique pour la passerelle	Saisissez le chiffre correspondant pour sélectionner Configurer l'IP statique. Vous êtes invité à entrer les informations suivantes pour configurer une adresse IP statique : • Nom de la carte réseau • Adresse IP • Masque réseau • Adresse de la passerelle par défaut • Adresse DNS principale • Adresse DNS secondaire **Important** 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 de plus amples informations, veuillez consulter Arrêt de votre machine virtuelle de passerelle. Si votre passerelle utilise plusieurs interfaces réseau, vous devez configurer toutes les

Pour exécuter cette tâche	Procédez comme suit
	interfaces actives pour qu'elles utilisent le DHCP ou des adresses IP statiques. 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. 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.

Pour exécuter cette tâche	Procédez comme suit
Configurer un nom d’hôte pour votre passerelle	Saisissez le chiffre correspondant pour sélectionner Configurer le nom d’hôte. Vous êtes invité à choisir si la passerelle utilisera un nom d’hôte statique que vous spécifiez ou en acquerra un automatiquement via DCHP ou rDNS. Si vous sélectionnez Static, vous êtes invité à fournir un nom d'hôte statique, tel que `testgateway.example.com`. Entrez y pour appliquer la configuration. **Note** Si vous configurez un nom d'hôte statique pour votre passerelle, assurez-vous que le nom d'hôte fourni se trouve dans le domaine auquel la passerelle est jointe. Vous devez également créer un enregistrement A dans votre système DNS qui pointe l'adresse IP de la passerelle vers son nom d'hôte statique.
Afficher la configuration du nom d'hôte de votre passerelle	Entrez le chiffre correspondant pour sélectionner Afficher la configuration du nom d'hôte. Le nom d'hôte, le mode d'acquisition, le domaine et le domaine Active Directory de votre passerelle sont affichés.

Pour exécuter cette tâche	Procédez comme suit
Réinitialiser la configuration du réseau de votre passerelle sur DHCP	Saisissez le chiffre correspondant pour sélectionner Tout réinitialiser vers le DHCP. Toutes les interfaces réseau sont programmées pour utiliser le protocole DHCP. **⚠ Important** 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 votre machine virtuelle de passerelle.
Définir la carte de routage par défaut de la passerelle	Saisissez le chiffre correspondant pour sélectionner Définir la carte par défaut. Les adaptateurs disponibles pour votre passerelle sont affichés et vous êtes invité à choisir l'un des adaptateurs, par exemple,. **`eth0`**
Modifier la configuration DNS de la passerelle	Entrez le chiffre correspondant pour sélection ner Modifier la configuration DNS. Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent. Vous êtes invité à indiquer la nouvelle adresse IP.

Pour exécuter cette tâche	Procédez comme suit
Afficher la configuration DNS de la passerelle	Saisissez le chiffre correspondant pour sélectionner Afficher la configuration DNS. Les cartes disponibles sur les serveurs DNS principaux et secondaires s'affichent. **Note** Pour certaines versions de l' VMware hyperviseur, vous pouvez modifier la configuration de l'adaptateur dans ce menu.
Consultation des tables de routage	Saisissez le chiffre correspondant pour sélectionner Afficher les routes. La route par défaut de votre passerelle s’affiche .

Test de la connectivité réseau de la passerelle

Vous pouvez utiliser la console locale de la passerelle afin de tester votre connexion réseau. Ce test peut être utile lorsque vous dépannez des problèmes de réseau avec votre passerelle.

Pour tester la connectivité réseau de votre passerelle

1. Connectez-vous à la console locale de la passerelle :
   - Pour plus d'informations sur la connexion à la console VMware ESXi locale, consultezAccès à la console locale de Gateway 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 le menu principal Activation de l'appliance AWS - Configuration, entrez le chiffre correspondant pour 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, 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 pour votre passerelle.

4. Si vous avez sélectionné le type de point de terminaison public, entrez le chiffre correspondant pour sélectionner Région AWS celui que vous souhaitez tester. Pour connaître les points de terminaison pris en charge Régions AWS et la liste des points de terminaison de AWS service que vous pouvez utiliser avec Storage Gateway, consultez la section AWS Storage Gateway Points de terminaison et quotas dans le. Références générales AWS

Au fur et à mesure que le test progresse, chaque point de terminaison affiche [RÉUSSITE] ou [ÉCHEC], indiquant l'état de la connexion comme suit :

Message	Description
[REUSSITE]	Storage Gateway dispose d'une connectivité réseau.
[ECHEC]	Storage Gateway ne dispose pas d'une connectiv ité réseau.

Affichage de l'état des ressources système de la 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 connexion à la VMware ESXi console, consultezAccès à la console locale de Gateway 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 le menu principal Activation de l’appliance AWS - Configuration, entrez le chiffre correspondant pour sélectionner Afficher la vérification des ressources du système.

   Chaque ressource affiche [OK], [AVERTISSEMENT] ou [ÉCHEC], indiquant l’état de la ressource comme suit :

Message	Description
[OK]	La ressource a réussi le contrôle des ressource s système.
[AVERTISSEMENT]	La ressource ne respecte pas les exigences recommandées, mais votre passerelle continuera 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 configura tion 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 connexion à la console VMware ESXi locale, consultezAccès à la console locale de Gateway 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 le menu principal Activation de l'AWS appliance - Configuration, entrez le chiffre correspondant pour sélectionner System Time Management.
3. Dans le menu System Time Management, entrez le chiffre correspondant pour effectuer l'une des tâches suivantes.

Pour exécuter cette tâche	Procédez comme suit
Afficher et synchroniser l'heure de votre ordinateur virtuel avec l'heure du serveur NTP.	Entrez le chiffre correspondant pour sélection ner Afficher et synchroniser l'heure du système. L'heure actuelle de votre ordinateur virtuel s'affiche. Votre passerelle de fichiers détermine le décalage horaire par rapport à la machine virtuelle de votre passerelle, et l'heure de votre serveur NTP vous invite à synchroniser l'heure de la machine virtuelle avec l'heure NTP. 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,

Pour exécuter cette tâche	Procédez comme suit
	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 instantan é et l'heure à laquelle cette opération s'est réellement produite. Pour une passerelle déployée sur VMware ESXi, il suffit de définir l'heure de l'hôte de l'hyperviseur et de synchroniser l'heure de la machine virtuelle avec celle de l'hôte pour éviter toute dérive temporelle. Pour de plus amples informations, veuillez consulter Synchroniser l'heure de la machine virtuelle avec VMware celle de l'hôte. Pour une passerelle déployée sur Microsoft Hyper-V, vérifiez régulièrement l'heure de l'ordinateur virtuel. Pour de plus amples informations, veuillez consulter Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux. Pour une passerelle déployée sur KVM, vous pouvez vérifier et synchroniser l'heure de la machine virtuelle à l'aide de l'interface de ligne de commande `virsh` pour KVM.

Pour exécuter cette tâche	Procédez comme suit
Modifier la configuration du serveur NTP	Entrez le chiffre correspondant pour sélectionner Modifier la configuration NTP. Vous êtes invité à entrer un serveur NTP principal et secondaire.
Afficher la configuration du serveur NTP	Entrez le chiffre correspondant pour sélectionner Afficher la configuration NTP. La configuration de votre serveur NTP s'affiche .

Exécution des commandes Storage Gateway sur la console locale

La console locale de machine virtuelle dans Storage Gateway permet de fournir un environnement sécurisé pour la configuration et le diagnostic des problèmes avec votre passerelle. À l'aide des commandes de la console locale, vous pouvez effectuer des tâches de maintenance telles que l'enregistrement des tables de routage Support, la connexion à, 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 connexion à la console VMware ESXi locale, consultezAccès à la console locale de Gateway 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 le menu principal Activation de l’appliance AWS - Configuration, entrez le chiffre correspondant pour sélectionner Console de passerelle.
3. À partir de l’invite de commande de la console de passerelle, entrez **h**.

   La console affiche le menu COMMANDES DISPONIBLES, qui répertorie les commandes disponibles :

Commande	Fonction
dig	Collectez les résultats de dig pour le dépannage du DNS.
exit	Retournez au menu Configuration.
h	Affichez la liste des commandes disponibles.
ifconfig	Affichez ou configurez les interfaces réseau. **Note** Nous vous recommandons de configurer les paramètres réseau ou IP à l'aide de la console Storage Gateway ou de l'option de menu dédiée de la console locale. Pour obtenir des instructions, voir Configuration des paramètres réseau de votre passerelle Configuration des paramètres .
ip	Afficher/manipuler le routage, les appareils et les tunnels. **Note** Nous vous recommandons de configurer les paramètres réseau ou IP à l'aide de la console Storage Gateway ou de l'option de menu dédiée de la console locale. Pour obtenir des instructions, voir Configuration des paramètres réseau de votre passerelle Configuration des paramètres .

Commande	Fonction
iptables	Outil d'administration pour le filtrage des IPv4 paquets et le NAT.
ncport	Testez la connectivité à un port TCP spécifique sur un réseau.
nping	Collectez les résultats de nping pour le dépannage de réseau.
open-support-channel	Connect to AWS Support. Pour savoir comment activer l'accès au AWS support, voir Vous souhaitez que le AWS support vous aide à résoudre les problèmes de votre passerelle EC2.
passwd	Mettez à jour les jetons d’authentification.
save-iptables	Conservez les tableaux IP.
save-routing-table	Enregistrez l’entrée de table de routage récemment ajoutée.
tcptraceroute	Collectez la sortie traceroute sur le trafic TCP vers une destination.

Commande	Fonction
sslcheck	Renvoie le résultat avec l'émetteur du certificat **Note** Storage Gateway utilise la vérification par l'émetteur du certificat et ne prend pas en charge l'inspection SSL. Si cette commande renvoie un émetteur autre que aws-appliance@amazon.com, il est probable qu'une application effectue une inspection SSL. Dans ce cas, nous recommandons de contourner l'inspection SSL pour l'appliance Storage Gateway.

4. À partir de l'invite de commande de la console de passerelle, entrez la commande correspondante pour la fonction que vous souhaitez utiliser, puis suivez les instructions.

Pour en savoir plus sur une commande, entrez **`man`** + *`command name`* à l'invite de commande.

Exécution de tâches sur la console locale de la passerelle Amazon EC2

Certaines tâches de maintenance nécessitent une connexion à la console locale lors de l'exécution d'une passerelle déployée sur une instance Amazon EC2. Cette section décrit comment se connecter à la console locale et effectuer des tâches de maintenance.

Rubriques

- Connexion à la console locale de votre passerelle Amazon EC2- Apprenez à vous connecter et à vous connecter à la console locale de passerelle de votre instance Amazon EC2 à l'aide d'un client Secure Shell (SSH).
- Routage de votre passerelle déployée sur Amazon EC2 via un proxy HTTP- Découvrez comment configurer un proxy Socket Secure version 5 (SOCKS5) entre AWS et une passerelle déployée sur une instance Amazon EC2.

- Test de la connectivité réseau de la passerelle- Découvrez comment utiliser la console locale de la passerelle pour tester la connectivité réseau entre votre passerelle et les différentes ressources du réseau.
- Affichage de l'état des ressources système de la passerelle- Apprenez à utiliser la console locale de la passerelle pour vérifier les cœurs de processeur virtuels, la taille du volume racine et la RAM de votre passerelle.
- Exécution de commandes Storage Gateway sur la console locale pour une passerelle Amazon EC2- Apprenez à exécuter des commandes de console locales pour effectuer des tâches telles que l'enregistrement de tables de routage Support, la connexion à, etc.
- Configuration des paramètres réseau de votre passerelle Amazon EC2- Apprenez à utiliser la console locale pour afficher et configurer les paramètres réseau tels que le DNS et le nom d'hôte d'une passerelle sur une instance Amazon EC2.

Connexion à la console locale de votre passerelle Amazon EC2

Vous vous connectez à la console locale de la passerelle sur une instance Amazon EC2 à l'aide d'un client Secure Shell (SSH). Pour des informations détaillées, consultez Connect to your 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 plus d'informations sur les paires de clés Amazon EC2, consultez les 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 l'instance Amazon EC2 via SSH et connectez-vous en tant qu'utilisateur administrateur.
2. Une fois connecté, le menu principal Activation de l'AWS appliance - Configuration s'affiche, à partir duquel vous pouvez effectuer diverses tâches.

Pour en savoir plus sur cette tâche	Consultez cette rubrique
Configurer un proxy HTTP pour la passerelle	Routage de votre passerelle déployée sur Amazon EC2 via un proxy HTTP
Configurer les paramètres réseau pour votre passerelle	Configuration des paramètres réseau de votre passerelle Amazon EC2

Pour en savoir plus sur cette tâche	Consultez cette rubrique
Tester la connectivité réseau	Test de la connectivité réseau de la passerelle
Consulter le contrôle d'une ressource système	Affichage de l'état des ressources système de la passerelle.
Exécuter les commandes de console Storage Gateway	Exécution de commandes Storage Gateway sur la console locale pour une passerelle Amazon EC2

Pour arrêter la passerelle, entrez **0**.

Pour quitter la session de configuration, entrez **X**.

Routage de votre passerelle déployée sur Amazon 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. Une fois que vous l'avez fait, Storage Gateway achemine tout le trafic des AWS terminaux via votre serveur proxy. Les communications entre la passerelle et les points de terminaison sont cryptées, même lors de l'utilisation du 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, veuillez consulter Connexion à la console locale de votre passerelle Amazon EC2.
2. Dans le menu principal Activation de l'appliance AWS - Configuration, entrez le chiffre correspondant pour sélectionner Configurer le proxy HTTP.
3. Dans le menu Configuration du proxy HTTP d'activation de l'appliance AWS , entrez le chiffre correspondant à la tâche que vous souhaitez effectuer :

    - Configurer le proxy HTTP : vous devez fournir un nom d'hôte et un port pour finaliser la configuration.

- Afficher la configuration actuelle du proxy HTTP : 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.
- Supprimer une configuration de proxy HTTP : le message `HTTP Proxy Configuration Removed` s'affiche.

Test de la connectivité réseau de la passerelle

Vous pouvez utiliser la console locale de la passerelle afin de tester votre connexion 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 obtenir des instructions, veuillez consulter Connexion à la console locale de votre passerelle Amazon EC2.
2. Dans le menu principal Activation de l'appliance AWS - Configuration, entrez le chiffre correspondant pour 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, 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 pour votre passerelle.
4. Si vous avez sélectionné le type de point de terminaison public, entrez le chiffre correspondant pour sélectionner Région AWS celui que vous souhaitez tester. Pour connaître les points de terminaison pris en charge Régions AWS et la liste des points de terminaison de AWS service que vous pouvez utiliser avec Storage Gateway, consultez la section AWS Storage Gateway Points de terminaison et quotas dans le. Références générales AWS

Au fur et à mesure que le test progresse, chaque point de terminaison affiche [RÉUSSITE] ou [ÉCHEC], indiquant l'état de la connexion comme suit :

Message	Description
[REUSSITE]	Storage Gateway dispose d'une connectivité réseau.

Message	Description
[ECHEC]	Storage Gateway ne dispose pas d’une connectiv ité réseau.

Affichage de l’état des ressources système de la passerelle

Lorsque votre passerelle de fichiers démarre, elle vérifie ses cœurs de processeur virtuels, la taille du volume racine et sa RAM. Il détermine ensuite si les ressources système disponibles sont suffisantes pour que votre passerelle fonctionne correctement. Vous pouvez consulter les résultats de la vérification des ressources système à l'aide de la console locale de la passerelle.

Pour afficher le statut d’un contrôle de ressource du système

1. Connectez-vous à la console locale sur votre passerelle de fichiers Amazon EC2. Pour obtenir des instructions, veuillez consulter Connexion à la console locale de votre passerelle Amazon EC2.
2. Dans le menu principal Activation de l’appliance AWS - Configuration, entrez le chiffre correspondant pour sélectionner Afficher la vérification des ressources du système.

   La console locale de la passerelle affiche [OK], [WARNING] ou [FAIL] pour indiquer l'état de la ressource comme suit :

Message	Description
[OK]	La ressource a réussi le contrôle des ressource s système.
[AVERTISSEMENT]	La ressource ne répond pas aux exigences recommandées, mais votre passerelle peut continuer à fonctionner. La console locale de la passerelle affiche un message qui décrit les résultats de la vérification des ressources.
[ECHEC]	La ressource ne répond pas à la configura tion minimum requise. Il est possible que votre passerelle ne fonctionne pas correctement.

Message	Description
	La console locale de la passerelle affiche un message qui décrit les résultats de la vérificat ion des ressources.

La console locale affiche également le nombre d'erreurs et d'avertissements à côté de l'option de menu de vérification des ressources.

Exécution de commandes Storage Gateway sur la console locale pour une passerelle Amazon EC2

La AWS Storage Gateway console fournit un environnement sécurisé pour configurer et diagnostiquer les problèmes liés à votre passerelle. À l'aide des commandes de la console, vous pouvez effectuer des tâches de maintenance telles que l'enregistrement des tables de routage ou la connexion à Support.

Pour exécuter une commande de configuration ou de diagnostic

1. Connectez-vous à la console locale de la passerelle. Pour obtenir des instructions, veuillez consulter Connexion à la console locale de votre passerelle Amazon EC2.
2. Dans le menu principal Activation de l’appliance AWS - Configuration, entrez le chiffre correspondant pour sélectionner Console de passerelle.
3. À partir de l’invite de commande de la console de passerelle, entrez **h**.

   La console affiche le menu COMMANDES DISPONIBLES, qui répertorie les commandes disponibles :

Commande	Fonction
dig	Collectez les résultats de dig pour le dépannage du DNS.
exit	Retournez au menu Configuration.
h	Affichez la liste des commandes disponibles.

Commande	Fonction
ifconfig	Affichez ou configurez les interfaces réseau. **Note** Nous vous recommandons de configurer les paramètres réseau ou IP à l'aide de la console Storage Gateway ou de l'option de menu dédiée de la console locale. Pour obtenir des instructions, voir Configuration des paramètres réseau de votre passerelle Configuration des paramètres .
ip	Afficher/manipuler le routage, les appareils et les tunnels. **Note** Nous vous recommandons de configurer les paramètres réseau ou IP à l'aide de la console Storage Gateway ou de l'option de menu dédiée de la console locale. Pour obtenir des instructions, voir Configuration des paramètres réseau de votre passerelle Configuration des paramètres .
iptables	Outil d'administration pour le filtrage des IPv4 paquets et le NAT.
ncport	Testez la connectivité à un port TCP spécifique sur un réseau.
nping	Collectez les résultats de nping pour le dépannage de réseau.

Commande	Fonction
open-support-channel	Connect to AWS Support.
save-iptables	Conservez les tableaux IP.
save-routing-table	Enregistrez l'entrée de table de routage récemment ajoutée.
tcptraceroute	Collectez la sortie traceroute sur le trafic TCP vers une destination.

4. À partir de l'invite de commande de la console de passerelle, entrez la commande correspondante pour la fonction que vous souhaitez utiliser, puis suivez les instructions.

Pour en savoir plus sur une commande, entrez **man** + *command name* à l'invite de commande.

Configuration des paramètres réseau de votre passerelle Amazon EC2

Vous pouvez consulter et configurer les paramètres réseau de votre passerelle de fichiers Amazon EC2 à l'aide de la console locale de la passerelle.

Pour configurer les paramètres de votre réseau

1. Connectez-vous à la console locale sur votre passerelle de fichiers Amazon EC2. Pour obtenir des instructions, veuillez consulter Connexion à la console locale de votre passerelle Amazon EC2.
2. Dans le menu principal Activation de l'AWS appliance - Configuration, entrez le chiffre correspondant pour sélectionner Configuration réseau.
3. Dans le menu Activation de l'AWS appliance - Configuration réseau, entrez le chiffre correspondant à la tâche que vous souhaitez effectuer :

   - Modifier la configuration DNS - La console locale de la passerelle affiche les adaptateurs disponibles pour les serveurs DNS principaux et secondaires. La console vous invite ensuite à fournir la nouvelle adresse IP.
   - Afficher la configuration DNS - La console locale de la passerelle affiche les adaptateurs disponibles pour les serveurs DNS principaux et secondaires.

- Configurer le nom d'hôte : la console locale de la passerelle vous invite à choisir si la passerelle utilisera un nom d'hôte statique que vous spécifiez ou si elle va acquérir un nom d'hôte automatiquement via DCHP ou RDNS.

  > **Note**
  >
  > Si vous choisissez de configurer un nom d'hôte statique pour votre passerelle, vous devez créer un enregistrement A dans votre système DNS qui pointe l'adresse IP de la passerelle vers son nom d'hôte statique.

- Afficher la configuration du nom d'hôte : la console locale de la passerelle affiche le nom d'hôte, le mode d'acquisition, le domaine et le domaine Active Directory pour votre passerelle de fichiers Amazon EC2.

Arrêt de votre machine virtuelle de 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. Vous arrêtez les machines virtuelles de passerelle sur site à l'aide de votre interface d'hyperviseur et les instances Amazon EC2 à l'aide de la console Amazon EC2.

> **Important**
>
> Si vous utilisez un stockage éphémère et que vous arrêtez et démarrez votre passerelle Amazon EC2, la passerelle sera hors ligne de manière permanente. Cela se produit parce que le disque de stockage physique est remplacé. Il n'existe aucune solution à ce problème. La seule solution consiste à supprimer la passerelle et à en activer une nouvelle sur une nouvelle instance EC2.

Remplacement de votre passerelle de existante par une nouvelle instance

Vous pouvez remplacer une passerelle de existante par une nouvelle instance à mesure que vos besoins en données et en performances augmentent, ou si vous recevez une AWS notification vous demandant de migrer votre passerelle. Cela peut être nécessaire si vous souhaitez déplacer votre

passerelle vers une meilleure plate-forme hôte ou des instances Amazon EC2 plus récentes, ou pour actualiser le matériel du serveur sous-jacent.

> **Important**
>
> Utilisez ces instructions uniquement pour la migration des dispositifs de passerelle exécutant la version 1.x. Vous ne pouvez pas les utiliser pour migrer des dispositifs de passerelle exécutant des versions inférieures.

> **Note**
>
> La migration ne peut être effectuée qu'entre des passerelles du même type. Par exemple, vous ne pouvez pas migrer des paramètres ou des données d'une passerelle de FSx fichiers vers une passerelle de fichiers S3.

Pour remplacer votre passerelle de passerelle de FSx fichiers par une nouvelle instance dotée d'un disque de cache vide et d'un nouvel ID de passerelle :

1. Arrêtez toutes les applications qui écrivent sur la passerelle de existante. Vérifiez que la `CachePercentDirty` métrique de l'onglet Surveillance est correcte `0` avant de configurer les associations de systèmes de fichiers sur la nouvelle passerelle.
2. Utilisez le AWS Command Line Interface (AWS CLI) pour recueillir et enregistrer les informations de configuration relatives à votre passerelle de existante et aux systèmes de fichiers associés en procédant comme suit :

   a. Enregistrez les informations de configuration de la passerelle de .

   ```
   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 relatives à la passerelle, telles que son nom, ses interfaces réseau, son fuseau horaire configuré et son état (si la passerelle est en cours d'exécution).

   b. Enregistrez les paramètres SMB (Server Message Block) de la passerelle de .

```
aws storagegateway describe-smb-settings --gateway-arn
 "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
```

Cette commande génère un bloc JSON qui contient le nom de domaine du Microsoft Active Directory auquel la passerelle est jointe.

c. Enregistrez les informations de partage de fichiers pour chaque système de fichiers associé à la passerelle de :

Utilisez la commande suivante pour chaque système de fichiers associé.

```
aws storagegateway describe-file-system-associations --file-system-
association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-
association/fsa-987A654B"
```

Cette commande génère un bloc JSON contenant des métadonnées relatives au système de fichiers, telles que son ARN d'emplacement, la destination du journal d'audit, les attributs d'actualisation du cache, les adresses IP configurées et les balises.

3. Créez une nouvelle passerelle de avec les mêmes paramètres et la même configuration que l'ancienne passerelle. Si nécessaire, reportez-vous aux informations que vous avez enregistrées à l'étape 2.
4. Créez de nouvelles associations de systèmes de fichiers pour la nouvelle passerelle avec les mêmes paramètres et configurations que les systèmes de fichiers configurés sur l'ancienne passerelle. Si nécessaire, reportez-vous aux informations que vous avez enregistrées à l'étape 2.
5. Vérifiez que votre nouvelle passerelle fonctionne correctement, puis remappez/découpez vos clients des anciens systèmes de fichiers vers les nouveaux systèmes de fichiers de la manière la mieux adaptée à votre environnement.
6. Vérifiez que votre nouvelle passerelle fonctionne correctement, puis supprimez l'ancienne passerelle de la console Storage Gateway.

> **Important**
>
> Avant de supprimer une passerelle de fichiers , assurez-vous qu'aucune application n'écrit actuellement dans le cache de cette passerelle. Si vous supprimez une passerelle 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'ancienne instance Amazon EC2.

Suppression de votre passerelle et suppression des ressources associées

Si vous n'avez l'intention de continuer à utiliser votre passerelle, pensez à supprimer la passerelle 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 dans la console de AWS Storage Gateway gestion et ses connexions au système de fichiers de de fichiers sont fermées. 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 Référence d'API de AWS Storage Gateway.

Suppression de la 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 une machine virtuelle (VM), une fois que vous avez supprimé la passerelle, la machine virtuelle 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 Kernel-based Virtual Machine) 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.

Pour supprimer une passerelle

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Choisissez Passerelles, puis sélectionnez une ou plusieurs passerelles à supprimer.
3. Pour Actions, choisissez Delete stack (Supprimer la pile). La boîte de dialogue de confirmation s'affiche.

   Warning

   Avant d'exécuter cette étape, assurez-vous qu'aucune application n'est 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.

4. Vérifiez que vous souhaitez bien supprimer les passerelles spécifiées, puis tapez le mot supprimer dans le champ de confirmation et choisissez Supprimer.
5. (Facultatif) Si vous souhaitez fournir des commentaires sur votre passerelle supprimée, complétez la boîte de dialogue de commentaires, puis choisissez Soumettre. Sinon, choisissez Passer.

Important

Vous ne payez plus de frais logiciels après avoir supprimé une passerelle, mais des ressources telles que le bucket Amazon S3 et les instances Amazon EC2 persistent. Vous pouvez supprimer l'instance de passerelle Amazon EC2 une fois la passerelle de fichiers supprimée.

Performances et optimisation

Cette section décrit les conseils et les meilleures pratiques pour optimiser les performances de File Gateway.

Rubriques

- Conseils de performance de base pour File Gateway
- Optimisation des performances de la passerelle
- Optimisation du débit de la passerelle de fichiers S3
- Optimisation de la passerelle de fichiers S3 pour les sauvegardes de bases de données SQL Server

Conseils de performance de base pour File Gateway

Dans cette section, vous trouverez des conseils pour le provisionnement du matériel pour votre machine virtuelle FSx File Gateway. Les configurations d'instance répertoriées dans le tableau sont des exemples et sont fournies à titre 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.

> **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 les passerelles EC2.
> La limite de taille suggérée pour les répertoires individuels des systèmes de fichiers que vous connectez à File Gateway est de 10 000 fichiers par répertoire. Vous pouvez utiliser File Gateway avec des répertoires contenant plus de 10 000 fichiers, mais les performances peuvent être affectées.

Dans les tableaux suivants, les opérations de lecture par accès au cache sont lues à partir des données de fichier servies depuis le cache. Les opérations de lecture manquante du cache sont

des lectures à partir des données de fichiers fournies par le serveur de fichiers Amazon FSx pour Windows.

Le tableau suivant présente un exemple de configuration de passerelle de FSx fichiers.

FSx Performances de la passerelle de fichiers sur les clients Windows

Exemple de configuration	Protocole	Débit d'écriture (taille de fichier 1 Go)	Débit de lecture atteint par le cache	Débit de lecture raté par le cache
Disque racine : 80 Go, SSD io1, 4 000 IOPS Disques de cache : 2 x 2 TiB NVME Performances réseau minimales : 10 Gb/s Processeur : 32 vCPU | Mémoire vive : 244 Go	SMBv3 - 1 fil	162 MiB/sec (1,4 Gbit/s)	403 MiB/sec (3,4 Gbit/s)	288 MiB/sec (2,4 Gbit/s)
	SMBv3 - 8 fils	511 MiB/sec (4,3 Gbit/s)	571 MiB/sec (4,8 Gbit/s)	567 MiB/sec (4,8 Gbit/s)

> **Note**
>
> Vos performances peuvent varier en fonction de la configuration de votre plateforme hôte et de la bande passante réseau. Les performances du débit d'écriture diminuent avec la taille du fichier, le débit le plus élevé possible pour les petits fichiers (moins de 32 Mo) étant de 16 fichiers par seconde.

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

Pour optimiser les performances de la passerelle, vous pouvez ajouter des disques hautes performances tels que des disques SSD (SSDs) et un NVMe contrôleur. Vous pouvez également attacher des disques virtuels directement à la machine virtuelle à partir d'un réseau SAN au lieu d'avoir recours au système NTFS Microsoft Hyper-V. L'amélioration des performances du disque se traduit généralement par un meilleur débit et un plus grand nombre d' input/output opérations par seconde (IOPS). Pour plus d'informations sur l'ajout de disques, consultezConfiguration d'un stockage de cache supplémentaire.

Pour mesurer le débit, utilisez les métriques `ReadBytes` et `WriteBytes` avec la statistique Amazon CloudWatch `Samples`. Par exemple, la statistique `Samples` 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**
>
> CloudWatch les métriques ne sont pas disponibles pour toutes les passerelles. Pour obtenir des informations sur les métriques de passerelle, consultez Surveillance de votre passerelle de .

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. Vérifiez également que vous n'êtes pas en train de surabonner le CPUs serveur hôte.

Lorsque vous ajoutez des éléments supplémentaires CPUs à votre serveur hôte de passerelle, vous augmentez la capacité de traitement de la passerelle. Cela permet à votre passerelle de gérer, en parallèle, à la fois le stockage des données de votre application vers votre stockage local et le téléchargement de ces données pour Windows File Server. Cela permet CPUs également de garantir que votre passerelle dispose de suffisamment de ressources CPU lorsque l'hôte est partagé avec d'autres VMs. La présence d'une quantité suffisante de ressources de processeur permet généralement d'améliorer le débit.

Storage Gateway prend en charge l'utilisation CPUs de 24 sur votre serveur hôte de passerelle. Vous pouvez utiliser 24 CPUs pour améliorer de manière significative les performances de votre passerelle. Nous vous recommandons la configuration de passerelle suivante pour votre serveur hôte de passerelle :

- 24 CPUs.
- 16 Gio de RAM réservée pour les passerelles de fichiers
  - 16 Gio de RAM réservée pour les passerelles avec une taille de cache maximale de 16 Tio
  - 32 Gio de RAM réservée pour les passerelles avec une taille de cache de 16 à 32 Tio
  - 48 Gio de RAM réservée pour les passerelles avec une taille de cache de 32 à 64 Tio
- Disque 1 attaché au contrôleur paravirtuel 1, à utiliser comme cache de passerelle de la façon suivante :
  - SSD utilisant un NVMe contrôleur.
- Carte réseau 1 configurée sur le réseau de machine virtuelle 1 :
  - Utilisez le réseau VM 1 et ajoutez VMXnet3 (10 Gbit/s) à utiliser pour l'ingestion.
- Carte réseau 2 configurée sur le réseau de machine virtuelle 2 :
  - Utilisez le réseau VM 2 et ajoutez un VMXnet3 (10 Gbit/s) à utiliser pour vous connecter AWS.

Soutenir les disques virtuels de la passerelle avec des disques physiques distincts

Lorsque vous provisionnez des disques de passerelle, nous vous recommandons vivement de ne pas provisionner de disques locaux pour le stockage local qui utilisent le même disque de stockage physique sous-jacent. Par exemple, pour VMware ESXi, les ressources de stockage physiques sous-jacentes sont représentées sous la forme d'un magasin de données. Lorsque vous déployez la machine virtuelle de la passerelle, vous choisissez une banque de données sur

laquelle stocker les fichiers de la machine virtuelle. 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 que machine virtuelle 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 les `WriteBytes` métriques `ReadBytes` et de la passerelle pour mesurer le débit total de 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 la machine virtuelle et les disques locaux, s’ils ne sont pas attachés directement.

Ajouter des ressources de processeur à votre environnement d’application

Si votre application peut utiliser des ressources CPU supplémentaires, l'ajout de ressources supplémentaires CPUs peut l'aider à augmenter sa I/O charge.

Certaines opérations sur les fichiers sur la passerelle de FSx fichiers, telles que le changement de nom de dossiers de niveau supérieur ou la modification des autorisations, peuvent entraîner plusieurs opérations sur les fichiers qui entraînent une I/O charge importante sur votre système FSx de fichiers Windows File Server. Si votre système de fichiers ne dispose pas de ressources de performance suffisantes pour votre charge de travail, il est possible qu'il supprime les clichés

instantanés, car il donne la priorité à la disponibilité permanente I/O plutôt qu'à la conservation historique des clichés instantanés.

Dans la FSx console Amazon, consultez la page Surveillance et performances pour voir si votre système de fichiers est sous-approvisionné. Si tel est le cas, vous pouvez passer au stockage SSD, augmenter la capacité de débit ou augmenter le nombre d'IOPS du SSD pour gérer votre charge de travail.

Optimisation du débit de la passerelle de fichiers S3

Les sections suivantes décrivent les meilleures pratiques pour optimiser le débit entre vos clients NFS et SMB, S3 File Gateway et Amazon S3. Les conseils fournis dans chaque section contribuent progressivement à améliorer le débit global. Bien qu'aucune de ces recommandations ne soit requise et qu'elles ne soient pas interdépendantes, elles ont été sélectionnées et ordonnées d'une manière logique qui permet de tester et d'ajuster les Support implémentations de S3 File Gateway. Lorsque vous implémentez et testez ces suggestions, gardez à l'esprit que chaque déploiement de S3 File Gateway est unique et que les résultats peuvent donc varier.

S3 File Gateway fournit une interface de fichiers permettant de stocker et de récupérer des objets Amazon S3 à l'aide des protocoles de fichiers NFS ou SMB standard, avec un mappage 1:1 natif entre le fichier et l'objet. Vous déployez S3 File Gateway en tant que machine virtuelle soit sur site dans votre VMware environnement KVM Microsoft Hyper-V ou Linux, soit dans le AWS cloud en tant qu'instance Amazon EC2. S3 File Gateway n'est pas conçu pour remplacer complètement le NAS d'entreprise. S3 File Gateway émule un système de fichiers, mais il ne s'agit pas d'un système de fichiers. L'utilisation d'Amazon S3 comme stockage dorsal durable entraîne une surcharge supplémentaire pour chaque I/O opération. L'évaluation des performances de S3 File Gateway par rapport à celles d'un NAS ou d'un serveur de fichiers existant ne constitue donc pas une comparaison équivalente.

Déployez votre passerelle au même endroit que vos clients

Nous vous recommandons de déployer votre dispositif virtuel S3 File Gateway dans un emplacement physique avec une latence réseau aussi faible que possible entre celui-ci et vos clients NFS ou SMB. Lorsque vous choisissez un emplacement pour votre passerelle, tenez compte des points suivants :

- La réduction de la latence réseau vers la passerelle peut contribuer à améliorer les performances des clients NFS ou SMB.

- La passerelle de fichiers S3 est conçue pour tolérer une latence réseau plus élevée entre la passerelle et Amazon S3 qu'entre la passerelle et les clients.
- Pour les instances de passerelle de fichiers S3 déployées dans Amazon EC2, nous recommandons de conserver la passerelle et les clients NFS ou SMB dans le même groupe de placement. Pour plus d'informations, consultez la section Groupes de placement pour vos instances Amazon EC2 dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

Réduisez les goulots d'étranglement causés par la lenteur des disques

Nous vous recommandons de surveiller la `IoWaitPercent` CloudWatch métrique afin d'identifier les problèmes de performances pouvant résulter de la lenteur des disques de stockage sur votre passerelle de fichiers S3. Lorsque vous essayez d'optimiser les problèmes de performances liés au disque, tenez compte des points suivants :

- `IoWaitPercent`indique le pourcentage de temps pendant lequel le processeur attend une réponse de la racine ou des disques de cache.
- Lorsqu'il `IoWaitPercent` est supérieur à 5 à 10 %, cela indique généralement un goulot d'étranglement des performances de la passerelle dû à des disques peu performants. Cette métrique doit être aussi proche que possible de 0 %, ce qui signifie que la passerelle n'attend jamais sur le disque, ce qui permet d'optimiser les ressources du processeur.
- Vous pouvez consulter l'`IoWaitPercent`onglet Monitoring de la console Storage Gateway ou configurer des CloudWatch alarmes recommandées pour vous avertir automatiquement si la métrique dépasse un seuil spécifique. Pour plus d'informations, consultez la section Création d' CloudWatch alarmes recommandées pour votre passerelle.
- Nous vous recommandons d'utiliser l' NVMe un ou l'autre SSD pour les disques racine et de cache de votre passerelle afin de minimiser`IoWaitPercent`.

Ajuster l'allocation des ressources des machines virtuelles pour le processeur, la RAM et les disques de cache

Lorsque vous essayez d'optimiser le débit de votre passerelle de fichiers S3, il est important d'allouer suffisamment de ressources à la machine virtuelle de passerelle, notamment le processeur, la RAM et les disques de cache. Les exigences minimales en matière de ressources virtuelles de 4 CPUs, 16 Go de RAM et 150 Go de stockage de cache ne conviennent généralement qu'aux petites charges de

travail. Lorsque vous allouez des ressources virtuelles pour des charges de travail plus importantes, nous recommandons ce qui suit :

- Augmentez le nombre CPUs alloué entre 16 et 48, en fonction de l'utilisation typique du processeur générée par votre passerelle de fichiers S3. Vous pouvez surveiller l'utilisation du processeur à l'aide de la `UserCpuPercent` métrique. Pour plus d'informations, consultez la section Comprendre les métriques de passerelle.
- Augmentez la RAM allouée entre 32 et 64 Go.

> **Note**
>
> S3 File Gateway ne peut pas utiliser plus de 64 Go de RAM.

- Utilisez NVMe un SSD pour les disques racine et le disque de cache, et dimensionnez vos disques de cache en fonction de l'ensemble de données de travail maximal que vous prévoyez d'écrire sur la passerelle. Pour plus d'informations, consultez les meilleures pratiques en matière de dimensionnement du cache de S3 File Gateway sur le YouTube canal officiel Amazon Web Services.
- Ajoutez au moins 4 disques de cache virtuels à la passerelle, plutôt que d'utiliser un seul grand disque. Plusieurs disques virtuels peuvent améliorer les performances même s'ils partagent le même disque physique sous-jacent, mais les améliorations sont généralement plus importantes lorsque les disques virtuels sont situés sur des disques physiques sous-jacents différents.

  Par exemple, si vous souhaitez déployer 12 To de cache, vous pouvez utiliser l'une des configurations suivantes :

  - 4 disques de cache de 3 To
  - 8 disques de cache de 1,5 To
  - 12 disques de cache de 1 To

  Outre les performances, cela permet une gestion plus efficace de la machine virtuelle au fil du temps. À mesure que votre charge de travail évolue, vous pouvez augmenter progressivement le nombre de disques de cache et votre capacité de cache globale, tout en conservant la taille initiale de chaque disque virtuel afin de préserver l'intégrité de la passerelle.

  Pour plus d'informations, voir Déterminer la quantité de stockage sur disque local.

Lorsque vous déployez S3 File Gateway en tant qu'instance Amazon EC2, tenez compte des points suivants :

- Le type d'instance que vous choisissez peut avoir un impact significatif sur les performances de la passerelle. Amazon EC2 offre une grande flexibilité pour ajuster l'allocation des ressources pour votre instance de passerelle de fichiers S3.
- Pour connaître les types d'instances Amazon EC2 recommandés pour la passerelle de fichiers S3, consultez la section Exigences relatives aux types d'instances Amazon EC2.
- Vous pouvez modifier le type d'instance Amazon EC2 qui héberge une passerelle de fichiers S3 active. Cela vous permet d'ajuster facilement la génération de matériel Amazon EC2 et l'allocation des ressources pour trouver le ratio idéal price-to-performance. Pour modifier le type d'instance, suivez la procédure suivante dans la console Amazon EC2 :

  1. Arrêtez l'instance Amazon EC2.
  2. Modifiez le type d'instance Amazon EC2.
  3. Allumez l'instance Amazon EC2.

  > **Note**
  >
  > L'arrêt d'une instance hébergeant une passerelle de fichiers S3 perturbera temporairement l'accès au partage de fichiers. Assurez-vous de planifier une fenêtre de maintenance si nécessaire.

- Le price-to-performance ratio d'une instance Amazon EC2 fait référence à la puissance de calcul que vous obtenez pour le prix que vous payez. Généralement, les instances Amazon EC2 de nouvelle génération offrent le meilleur price-to-performance ratio, avec du matériel plus récent et des performances améliorées à un coût relativement inférieur à celui des anciennes générations. Des facteurs tels que le type d'instance, la région et les modèles d'utilisation ont une incidence sur ce ratio. Il est donc important de sélectionner l'instance adaptée à votre charge de travail spécifique afin d'optimiser la rentabilité.

Régler le niveau de sécurité des PME

Le SMBv3 protocole permet à la fois la signature SMB et le chiffrement SMB, ce qui présente certains compromis en termes de performances et de sécurité. Pour optimiser le débit, vous pouvez ajuster le niveau de sécurité SMB de votre passerelle afin de spécifier quelles fonctionnalités de sécurité sont

appliquées aux connexions client. Pour plus d'informations, voir Définir un niveau de sécurité pour votre passerelle.

Lorsque vous ajustez le niveau de sécurité SMB, tenez compte des points suivants :

- Le niveau de sécurité par défaut pour S3 File Gateway est Appliquer le chiffrement. Ce paramètre applique à la fois le chiffrement et la signature pour les connexions des clients SMB aux partages de fichiers de passerelle, ce qui signifie que tout le trafic entre le client et la passerelle est chiffré. Ce paramètre n'affecte pas le trafic en provenance de la passerelle AWS, qui est toujours chiffré.

  La passerelle limite chaque connexion client chiffrée à un seul vCPU. Par exemple, si vous n'avez qu'un seul client chiffré, ce client sera limité à un seul vCPU, même si 4 vCPU ou plus CPUs sont alloués à la passerelle. De ce fait, le débit des connexions chiffrées entre un seul client et S3 File Gateway est généralement limité entre 40 et 60 Mo/s.
- Si vos exigences en matière de sécurité vous permettent d'adopter une posture plus souple, vous pouvez modifier le niveau de sécurité sur Négocié par le client, ce qui désactivera le chiffrement SMB et appliquera uniquement la signature SMB. Avec ce paramètre, les connexions client à la passerelle peuvent utiliser plusieurs vCPUs, ce qui se traduit généralement par une augmentation des performances de débit.

> **Note**
>
> Après avoir modifié le niveau de sécurité SMB de votre passerelle de fichiers S3, vous devez attendre que le statut du partage de fichiers passe de Updating à Available dans la console Storage Gateway, puis déconnecter et reconnecter vos clients SMB pour que le nouveau paramètre prenne effet.

Utiliser plusieurs threads et clients pour paralléliser les opérations d'écriture

Il est difficile d'atteindre des performances de débit maximales avec une passerelle de fichiers S3 qui n'utilise qu'un seul client NFS ou SMB pour écrire un fichier à la fois, car l'écriture séquentielle à partir d'un seul client est une opération à thread unique. Nous recommandons plutôt d'utiliser plusieurs threads provenant de chaque client NFS ou SMB pour écrire plusieurs fichiers en parallèle, et d'utiliser plusieurs clients NFS ou SMB simultanément sur votre passerelle de fichiers S3 afin d'optimiser le débit de la passerelle.

L'utilisation de plusieurs threads peut améliorer considérablement les performances. Cependant, l'utilisation d'un plus grand nombre de threads nécessite davantage de ressources système, ce qui peut avoir un impact négatif sur les performances si la taille de la passerelle n'est pas adaptée à l'augmentation de la charge. Dans un déploiement classique, vous pouvez vous attendre à obtenir de meilleures performances de débit à mesure que vous ajoutez de nouveaux threads et clients, jusqu'à ce que vous atteigniez les limites matérielles et de bande passante maximales pour votre passerelle. Nous vous recommandons d'essayer différents nombres de threads afin de trouver l'équilibre optimal entre vitesse et utilisation des ressources système pour votre configuration matérielle et réseau spécifique.

Tenez compte des informations suivantes concernant les outils courants qui peuvent vous aider à tester la configuration de votre thread et de votre client :

- Vous pouvez tester les performances d'écriture multithread en utilisant des outils tels que Robocopy pour copier un ensemble de fichiers vers un partage de fichiers sur votre passerelle. Par défaut, Robocopy utilise 8 fils lors de la copie de fichiers, mais vous pouvez spécifier jusqu'à 128 fils.

  Pour utiliser plusieurs threads avec Robocopy, ajoutez le `/MT:n` commutateur à votre commande, où n est le nombre de threads que vous souhaitez utiliser. Par exemple :

  ```
  robocopy C:\source D:\destination /MT:64
  ```

  Cette commande utilisera 64 threads pour l'opération de copie.

  > **Note**
  >
  > Nous ne recommandons pas d'utiliser l'Explorateur Windows pour glisser-déposer des fichiers lors des tests de débit maximal, car cette méthode est limitée à un seul thread et copie les fichiers de manière séquentielle.

  Pour plus d'informations, consultez Robocopy sur le site Web de Microsoft Learn.
- Vous pouvez également effectuer des tests à l'aide d'outils d'analyse comparative du stockage courants tels que DISKSPD ou FIO. Ces outils proposent des options permettant d'ajuster le nombre de threads, la profondeur d'E/S et d'autres paramètres en fonction de vos exigences de charge de travail spécifiques.

  DiskSpd vous permet de contrôler le nombre de threads à l'aide du `-t` paramètre. Par exemple :

```
diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
```

Cet exemple de commande effectue les opérations suivantes :

- Crée un fichier de test de 10 Go () `-c1G`
- Fonctionne pendant 300 secondes (`-d300`)
- Effectue un I/O test aléatoire avec 50 % de lectures, 50 % d'écritures (`-r -w50`)
- Utilise 64 fils (`s-t64`)
- Définit la profondeur de la file d'attente à 32 par thread (`-o32`)
- Utilise une taille de bloc de 1 Mo () `-b1M`
- Désactive la mise en cache matérielle et logicielle () `-h -L`

Pour plus d'informations, voir Utiliser DISKSPD pour tester les performances de stockage des charges de travail sur le site Web de Microsoft Learn.

- FIO utilise le `numjobs` paramètre pour contrôler le nombre de threads parallèles. Par exemple :

```
fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
--size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
group_reporting
```

Cet exemple de commande effectue les opérations suivantes :

- Effectue un I/O test aléatoire (`--rw=randrw`)
- Effectue 70 % de lectures et 30 % d'écritures (`--rwmixread=70`)
- Utilise une taille de bloc de 1 Mo () `--bs=1M`
- Règle la I/O profondeur à 64 (`--iodepth=64`)
- Tests sur un fichier de 10 Go (`--size=10G`)
- Fonctionne pendant 5 minutes (`--runtime=300`)
- Crée 64 tâches parallèles (threads) (`--numjobs=64`)
- Utilise un I/O moteur asynchrone () `--ioengine=libaio`
- Regroupe les résultats pour faciliter l'analyse (`--group_reporting`)

Pour plus d'informations, consultez la page de manuel fio Linux.

-

Désactiver l'actualisation automatique du cache

La fonctionnalité d'actualisation automatique du cache permet à votre passerelle de fichiers S3 d'actualiser automatiquement ses métadonnées, ce qui permet de capturer les modifications apportées par les utilisateurs ou les applications à votre ensemble de fichiers en écrivant directement dans le compartiment Amazon S3, plutôt que par le biais de la passerelle. Pour plus d'informations, consultez Actualisation du cache d'objets du compartiment Amazon S3.

Pour optimiser le débit de la passerelle, nous recommandons de désactiver cette fonctionnalité dans les déploiements où toutes les lectures et écritures dans le compartiment Amazon S3 seront effectuées via votre passerelle de fichiers S3.

Lorsque vous configurez l'actualisation automatique du cache, tenez compte des points suivants :

- Si vous devez utiliser l'actualisation automatique du cache parce que des utilisateurs ou des applications de votre déploiement écrivent parfois directement sur Amazon S3, nous vous recommandons de configurer l'intervalle de temps le plus long possible entre les actualisations, ce qui est toujours pratique pour les besoins de votre entreprise. Un intervalle d'actualisation du cache plus long permet de réduire le nombre d'opérations de métadonnées que la passerelle doit effectuer lors de la navigation dans les répertoires ou de la modification de fichiers.

  Par exemple : définissez l'actualisation automatique du cache sur 24 heures, au lieu de 5 minutes, si cela est acceptable pour votre charge de travail.
- L'intervalle de temps minimum est de 5 minutes. L'intervalle maximal est de 30 jours.
- Si vous choisissez de définir un intervalle d'actualisation du cache très court, nous vous recommandons de tester l'expérience de navigation dans les annuaires pour vos clients NFS et SMB. Le temps nécessaire pour actualiser le cache de la passerelle peut augmenter considérablement en fonction du nombre de fichiers et de sous-répertoires contenus dans votre compartiment Amazon S3.

Augmenter le nombre de threads de téléchargement sur Amazon S3

Par défaut, S3 File Gateway ouvre 8 threads pour le téléchargement de données Amazon S3, ce qui fournit une capacité de téléchargement suffisante pour la plupart des déploiements classiques. Cependant, il est possible qu'une passerelle reçoive des données de clients NFS et SMB à un débit supérieur à celui qu'elle peut charger sur Amazon S3 avec la capacité standard de 8 threads, ce qui peut amener le cache local à atteindre sa limite de stockage.

Dans certaines circonstances, Support cela peut augmenter le nombre de threads de téléchargement Amazon S3 pour votre passerelle de 8 à 40, ce qui permet de charger davantage de données en parallèle. En fonction de la bande passante et d'autres facteurs spécifiques à votre déploiement, cela peut augmenter considérablement les performances de téléchargement et contribuer à réduire la quantité de stockage en cache nécessaire pour prendre en charge votre charge de travail.

Nous vous recommandons d'utiliser cette `CachePercentDirty` CloudWatch métrique pour surveiller la quantité de données stockées sur les disques de cache de la passerelle locale qui n'ont pas encore été chargées vers Amazon S3, et de contacter Support pour déterminer si l'augmentation du nombre de threads de téléchargement peut améliorer le débit de votre passerelle de fichiers S3. Pour plus d'informations, consultez la section Comprendre les métriques de passerelle.

> **Note**
>
> Ce paramètre consomme des ressources supplémentaires du processeur de la passerelle. Nous recommandons de surveiller l'utilisation du processeur de la passerelle et d'augmenter les ressources du processeur allouées si nécessaire.

Augmenter les paramètres de délai d'expiration des PME

Lorsque S3 File Gateway copie des fichiers volumineux vers un partage de fichiers SMB, la connexion du client SMB peut être interrompue après une période prolongée.

Nous vous recommandons d'étendre le délai d'expiration de session SMB pour vos clients SMB à 20 minutes ou plus, en fonction de la taille des fichiers et de la vitesse d'écriture de votre passerelle. La valeur par défaut est de 300 secondes ou 5 minutes. Pour plus d'informations, consultez la section Votre tâche de sauvegarde de passerelle échoue ou des erreurs se produisent lors de l'écriture sur votre passerelle.

Activez le verrouillage opportuniste pour les applications compatibles

Le verrouillage opportuniste, ou « oplocks », est activé par défaut pour chaque nouvelle passerelle de fichiers S3. Lorsqu'il utilise des oplocks avec des applications compatibles, le client regroupe plusieurs petites opérations en opérations plus importantes, ce qui est plus efficace pour le client, la passerelle et le réseau. Nous vous recommandons de conserver le verrouillage opportuniste activé si vous utilisez des applications qui exploitent la mise en cache locale côté client, telles que Microsoft Office, Adobe Suite et bien d'autres, car cela peut améliorer considérablement les performances.

Si vous désactivez le verrouillage opportuniste, les applications qui prennent en charge les oplocks ouvriront généralement les fichiers volumineux (50 Mo ou plus) beaucoup plus lentement. Ce délai est dû au fait que la passerelle envoie des données par parties de 4 Ko, ce qui se traduit par un débit élevé I/O ou faible.

Ajustez la capacité de la passerelle en fonction de la taille de l'ensemble de fichiers de travail

Le paramètre de capacité de la passerelle indique le nombre maximal de fichiers pour lesquels votre passerelle stockera les métadonnées dans son cache local. Par défaut, la capacité de la passerelle est définie sur Petite, ce qui signifie que la passerelle stocke les métadonnées d'un maximum de 5 millions de fichiers. Le paramètre par défaut fonctionne bien pour la plupart des charges de travail, même s'il y a des centaines de millions, voire des milliards d'objets dans Amazon S3, car seul un petit sous-ensemble de fichiers est activement accessible à un moment donné dans un déploiement classique. Ce groupe de fichiers est appelé « ensemble de travail ».

Si votre charge de travail accède régulièrement à un ensemble de fichiers de plus de 5 millions, votre passerelle devra effectuer de fréquentes expulsions du cache, c'est-à-dire de petites opérations d'E/S stockées dans la RAM et conservées sur le disque racine. Cela peut avoir un impact négatif sur les performances de la passerelle, car celle-ci récupère de nouvelles données depuis Amazon S3.

Vous pouvez surveiller la `IndexEvictions` métrique pour déterminer le nombre de fichiers dont les métadonnées ont été supprimées du cache pour faire de la place à de nouvelles entrées. Pour plus d'informations, consultez la section Comprendre les métriques de passerelle.

Nous vous recommandons d'utiliser l'action `UpdateGatewayInformation` API pour augmenter la capacité de la passerelle afin qu'elle corresponde au nombre de fichiers de votre ensemble de travail habituel. Pour de plus amples informations, veuillez consulter UpdateGatewayInformation.

> **Note**
>
> L'augmentation de la capacité de la passerelle nécessite de la RAM et de la capacité du disque racine supplémentaires.
>
> - Les fichiers de petite taille (5 millions de fichiers) nécessitent au moins 16 Go de RAM et 80 Go de disque racine.
> - Le format moyen (10 millions de fichiers) nécessite au moins 32 Go de RAM et 160 Go de disque racine.

- Les fichiers volumineux (20 millions de fichiers) nécessitent 64 Go de RAM et 240 Go de disque racine.

Important

La capacité de la passerelle ne peut pas être diminuée.

Déployez plusieurs passerelles pour des charges de travail plus importantes

Nous vous recommandons de répartir votre charge de travail sur plusieurs passerelles lorsque cela est possible, plutôt que de consolider de nombreux partages de fichiers sur une seule grande passerelle. Par exemple, vous pouvez isoler un partage de fichiers très utilisé sur une passerelle, tout en regroupant les partages de fichiers les moins fréquemment utilisés sur une autre passerelle.

Lorsque vous planifiez un déploiement avec plusieurs passerelles et partages de fichiers, tenez compte des points suivants :

- Le nombre maximum de partages de fichiers sur une passerelle unique est de 50, mais le nombre de partages de fichiers gérés par une passerelle peut avoir un impact sur les performances de la passerelle. Pour plus d'informations, consultez la section Conseils de performance pour les passerelles comportant plusieurs partages de fichiers.
- Les ressources de chaque passerelle de fichiers S3 sont partagées entre tous les partages de fichiers, sans partitionnement.
- Un partage de fichiers unique très utilisé peut avoir un impact sur les performances des autres partages de fichiers sur la passerelle.

Note

Il est déconseillé de créer plusieurs partages de fichiers mappés vers le même emplacement Amazon S3 à partir de plusieurs passerelles, sauf si au moins l'un d'entre eux est en lecture seule.
Les écritures simultanées sur le même fichier à partir de plusieurs passerelles sont considérées comme un scénario à écritures multiples, ce qui peut entraîner des problèmes d'intégrité des données.

Optimisation de la passerelle de fichiers S3 pour les sauvegardes de bases de données SQL Server

Les sauvegardes de base de données constituent un cas d'utilisation courant et recommandé pour S3 File Gateway, qui assure une conservation rentable à court et à long terme en stockant les sauvegardes de base de données dans Amazon S3, avec la possibilité d'effectuer un cycle de vie afin de réduire les coûts des niveaux de stockage selon les besoins. Grâce à cette solution, vous pouvez réduire le besoin d'applications de sauvegarde d'entreprise à l'aide d'outils intégrés tels que SQL Server Management Studio et Oracle RMAN.

Les sections suivantes décrivent les meilleures pratiques pour optimiser le déploiement de votre passerelle de fichiers S3 afin d'optimiser les performances et de prendre en charge de manière rentable des centaines de téraoctets de sauvegardes de bases de données SQL. Les conseils fournis dans chaque section contribuent progressivement à améliorer le débit global. Bien qu'aucune de ces recommandations ne soit requise et qu'elles ne soient pas interdépendantes, elles ont été sélectionnées et ordonnées d'une manière logique qui permet de tester et d'ajuster les Support implémentations de S3 File Gateway. Lorsque vous implémentez et testez ces suggestions, gardez à l'esprit que chaque déploiement de S3 File Gateway est unique et que les résultats peuvent donc varier.

S3 File Gateway fournit une interface de fichiers permettant de stocker et de récupérer des objets Amazon S3 à l'aide des protocoles de fichiers NFS ou SMB standard, avec un mappage 1:1 natif entre le fichier et l'objet. Vous déployez S3 File Gateway en tant que machine virtuelle soit sur site dans votre VMware environnement KVM Microsoft Hyper-V ou Linux, soit dans le AWS cloud en tant qu'instance Amazon EC2. S3 File Gateway n'est pas conçu pour remplacer complètement le NAS d'entreprise. S3 File Gateway émule un système de fichiers, mais il ne s'agit pas d'un système de fichiers. L'utilisation d'Amazon S3 comme stockage dorsal durable entraîne une surcharge supplémentaire pour chaque I/O opération. L'évaluation des performances de S3 File Gateway par rapport à celles d'un NAS ou d'un serveur de fichiers existant ne constitue donc pas une comparaison équivalente.

Déployez votre passerelle au même endroit que vos serveurs SQL

Nous vous recommandons de déployer votre dispositif virtuel S3 File Gateway dans un emplacement physique avec une latence réseau aussi faible que possible entre celui-ci et vos serveurs SQL. Lorsque vous choisissez un emplacement pour votre passerelle, tenez compte des points suivants :

- La réduction de la latence réseau vers la passerelle peut contribuer à améliorer les performances des clients PME, tels que les serveurs SQL.
- La passerelle de fichiers S3 est conçue pour tolérer une latence réseau plus élevée entre la passerelle et Amazon S3 qu'entre la passerelle et les clients.
- Pour les instances de passerelle de fichiers S3 déployées dans Amazon EC2, nous recommandons de conserver la passerelle et les serveurs SQL dans le même groupe de placement. Pour plus d'informations, consultez la section Groupes de placement pour vos instances Amazon EC2 dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

Réduisez les goulots d'étranglement causés par la lenteur des disques

Nous vous recommandons de surveiller la `IoWaitPercent` CloudWatch métrique afin d'identifier les problèmes de performances pouvant résulter de la lenteur des disques de stockage sur votre passerelle de fichiers S3. Lorsque vous essayez d'optimiser les problèmes de performances liés au disque, tenez compte des points suivants :

- `IoWaitPercent`indique le pourcentage de temps pendant lequel le processeur attend une réponse de la racine ou des disques de cache.
- Lorsqu'il `IoWaitPercent` est supérieur à 5 à 10 %, cela indique généralement un goulot d'étranglement des performances de la passerelle dû à des disques peu performants. Cette métrique doit être aussi proche que possible de 0 %, ce qui signifie que la passerelle n'attend jamais sur le disque, ce qui permet d'optimiser les ressources du processeur.
- Vous pouvez consulter l'`IoWaitPercent`onglet Monitoring de la console Storage Gateway ou configurer des CloudWatch alarmes recommandées pour vous avertir automatiquement si la métrique dépasse un seuil spécifique. Pour plus d'informations, consultez la section Création d' CloudWatch alarmes recommandées pour votre passerelle.
- Nous vous recommandons d'utiliser l' NVMe un ou l'autre SSD pour les disques racine et de cache de votre passerelle afin de minimiser`IoWaitPercent`.

Ajuster l'allocation des ressources de la machine virtuelle S3 File Gateway pour le processeur, la RAM et les disques de cache

Lorsque vous essayez d'optimiser le débit de votre passerelle de fichiers S3, il est important d'allouer suffisamment de ressources à la machine virtuelle de passerelle, notamment le processeur, la RAM et les disques de cache. Les exigences minimales en matière de ressources virtuelles de 4 CPUs, 16

Go de RAM et 150 Go de stockage de cache ne conviennent généralement qu'aux petites charges de travail. Lorsque vous allouez des ressources virtuelles pour des charges de travail plus importantes, nous recommandons ce qui suit :

- Augmentez le nombre CPUs alloué entre 16 et 48, en fonction de l'utilisation typique du processeur générée par votre passerelle de fichiers S3. Vous pouvez surveiller l'utilisation du processeur à l'aide de la `UserCpuPercent` métrique. Pour plus d'informations, consultez la section Comprendre les métriques de passerelle.
- Augmentez la RAM allouée entre 32 et 64 Go.

> **Note**
>
> S3 File Gateway ne peut pas utiliser plus de 64 Go de RAM.

- Utilisez NVMe un SSD pour les disques racine et le disque de cache, et dimensionnez vos disques de cache en fonction de l'ensemble de données de travail maximal que vous prévoyez d'écrire sur la passerelle. Pour plus d'informations, consultez les meilleures pratiques en matière de dimensionnement du cache de S3 File Gateway sur le YouTube canal officiel Amazon Web Services.
- Ajoutez au moins 4 disques de cache virtuels à la passerelle, plutôt que d'utiliser un seul grand disque. Plusieurs disques virtuels peuvent améliorer les performances même s'ils partagent le même disque physique sous-jacent, mais les améliorations sont généralement plus importantes lorsque les disques virtuels sont situés sur des disques physiques sous-jacents différents.

  Par exemple, si vous souhaitez déployer 12 To de cache, vous pouvez utiliser l'une des configurations suivantes :

  - 4 disques de cache de 3 To
  - 8 disques de cache de 1,5 To
  - 12 disques de cache de 1 To

  Outre les performances, cela permet une gestion plus efficace de la machine virtuelle au fil du temps. À mesure que votre charge de travail évolue, vous pouvez augmenter progressivement le nombre de disques de cache et votre capacité de cache globale, tout en conservant la taille initiale de chaque disque virtuel afin de préserver l'intégrité de la passerelle.

  Pour plus d'informations, voir Déterminer la quantité de stockage sur disque local.

Lorsque vous déployez S3 File Gateway en tant qu'instance Amazon EC2, tenez compte des points suivants :

- Le type d'instance que vous choisissez peut avoir un impact significatif sur les performances de la passerelle. Amazon EC2 offre une grande flexibilité pour ajuster l'allocation des ressources pour votre instance de passerelle de fichiers S3.
- Pour connaître les types d'instances Amazon EC2 recommandés pour la passerelle de fichiers S3, consultez la section Exigences relatives aux types d'instances Amazon EC2.
- Vous pouvez modifier le type d'instance Amazon EC2 qui héberge une passerelle de fichiers S3 active. Cela vous permet d'ajuster facilement la génération de matériel Amazon EC2 et l'allocation des ressources pour trouver le ratio idéal price-to-performance. Pour modifier le type d'instance, suivez la procédure suivante dans la console Amazon EC2 :

  1. Arrêtez l'instance Amazon EC2.
  2. Modifiez le type d'instance Amazon EC2.
  3. Allumez l'instance Amazon EC2.

  > **Note**
  >
  > L'arrêt d'une instance hébergeant une passerelle de fichiers S3 perturbera temporairement l'accès au partage de fichiers. Assurez-vous de planifier une fenêtre de maintenance si nécessaire.

- Le price-to-performance ratio d'une instance Amazon EC2 fait référence à la puissance de calcul que vous obtenez pour le prix que vous payez. Généralement, les instances Amazon EC2 de nouvelle génération offrent le meilleur price-to-performance ratio, avec du matériel plus récent et des performances améliorées à un coût relativement inférieur à celui des anciennes générations. Des facteurs tels que le type d'instance, la région et les modèles d'utilisation ont une incidence sur ce ratio. Il est donc important de sélectionner l'instance adaptée à votre charge de travail spécifique afin d'optimiser la rentabilité.

Améliorez le débit des clients des PME en ajustant le niveau de sécurité de votre passerelle de fichiers S3

Le SMBv3 protocole permet à la fois la signature SMB et le chiffrement SMB, ce qui présente certains compromis en termes de performances et de sécurité. Pour optimiser le débit, vous pouvez ajuster le niveau de sécurité SMB de votre passerelle afin de spécifier quelles fonctionnalités de sécurité sont

appliquées aux connexions client. Pour plus d'informations, voir Définir un niveau de sécurité pour votre passerelle.

Lorsque vous ajustez le niveau de sécurité SMB, tenez compte des points suivants :

- Le niveau de sécurité par défaut pour S3 File Gateway est Appliquer le chiffrement. Ce paramètre applique à la fois le chiffrement et la signature pour les connexions des clients SMB aux partages de fichiers de passerelle, ce qui signifie que tout le trafic entre le client et la passerelle est chiffré. Ce paramètre n'affecte pas le trafic en provenance de la passerelle AWS, qui est toujours chiffré.

  La passerelle limite chaque connexion client chiffrée à un seul vCPU. Par exemple, si vous n'avez qu'un seul client chiffré, ce client sera limité à un seul vCPU, même si 4 vCPU ou plus CPUs sont alloués à la passerelle. De ce fait, le débit des connexions chiffrées entre un seul client et S3 File Gateway est généralement limité entre 40 et 60 Mo/s.
- Si vos exigences en matière de sécurité vous permettent d'adopter une posture plus souple, vous pouvez modifier le niveau de sécurité sur Négocié par le client, ce qui désactivera le chiffrement SMB et appliquera uniquement la signature SMB. Avec ce paramètre, les connexions client à la passerelle peuvent utiliser plusieurs vCPUs, ce qui se traduit généralement par une augmentation des performances de débit.

> **Note**
>
> Après avoir modifié le niveau de sécurité SMB de votre passerelle de fichiers S3, vous devez attendre que le statut du partage de fichiers passe de Updating à Available dans la console Storage Gateway, puis déconnecter et reconnecter vos clients SMB pour que le nouveau paramètre prenne effet.

Améliorez le débit des clients PME en divisant les sauvegardes SQL en plusieurs fichiers

- Il est difficile d'atteindre des performances de débit maximales avec une passerelle de fichiers S3 qui permet à un seul serveur SQL d'écrire un fichier à la fois, car l'écriture séquentielle à partir d'un seul serveur SQL est une opération à thread unique. Nous vous recommandons plutôt d'utiliser plusieurs threads de chaque serveur SQL pour écrire plusieurs fichiers en parallèle, et d'utiliser plusieurs serveurs SQL simultanément sur votre passerelle de fichiers S3 afin d'optimiser le débit de la passerelle. Avec les sauvegardes SQL, la division des sauvegardes en plusieurs fichiers

permet à chaque fichier d'utiliser un thread distinct, qui écrira plusieurs fichiers simultanément sur le partage de fichiers S3 File Gateway. Plus vous avez de threads, plus vous pouvez atteindre un débit élevé, dans les limites de la passerelle.

- SQL Server prend en charge l'écriture simultanée dans plusieurs fichiers au cours d'une seule opération de sauvegarde. Par exemple, vous pouvez spécifier plusieurs destinations de fichiers à l'aide des commandes T-SQL ou de SQL Server Management Studio (SSMS). Chaque fichier utilise un thread distinct pour envoyer les données du serveur SQL au partage de fichiers de la passerelle. Cette approche permet d'améliorer le I/O débit, ce qui peut améliorer considérablement la vitesse et l'efficacité des sauvegardes.

Lorsque vous configurez vos sauvegardes SQL Server, tenez compte des points suivants :

- En divisant les sauvegardes en plusieurs fichiers, les administrateurs de SQL Server peuvent optimiser les temps de sauvegarde et gérer plus efficacement les sauvegardes de bases de données volumineuses.
- Le nombre de fichiers utilisés dépend de la configuration de stockage du serveur et des exigences en matière de performances. Pour les bases de données volumineuses, nous recommandons de diviser les sauvegardes en plusieurs fichiers plus petits de 10 Go à 20 Go chacun.
- Il n'existe aucune limite stricte quant au nombre de fichiers dans lesquels SQL Server peut écrire pendant une sauvegarde, mais des considérations pratiques telles que l'architecture de stockage et la bande passante réseau devraient guider ce choix.

Pour en savoir plus, consultez :

- Sauvegardez SQL Server 43 à 67 % plus rapidement en écrivant dans plusieurs fichiers
- Stockez facilement vos sauvegardes SQL Server dans Amazon S3 à l'aide de File Gateway

Empêchez les échecs de copie de fichiers volumineux en augmentant les paramètres de délai d'expiration SMB

Lorsque S3 File Gateway copie des fichiers de sauvegarde SQL volumineux vers un partage de fichiers SMB, la connexion du client SMB peut être interrompue après une période prolongée. Nous vous recommandons d'étendre le délai d'expiration de session SMB pour vos clients SMB SQL Server à 20 minutes ou plus, en fonction de la taille des fichiers et de la vitesse d'écriture de votre passerelle. La valeur par défaut est de 300 secondes ou 5 minutes. Pour plus d'informations,

consultez la section Votre tâche de sauvegarde de passerelle échoue ou des erreurs se produisent lors de l'écriture sur votre passerelle.

Augmenter le nombre de threads de téléchargement sur Amazon S3

Par défaut, S3 File Gateway ouvre 8 threads pour le téléchargement de données Amazon S3, ce qui fournit une capacité de téléchargement suffisante pour la plupart des déploiements classiques. Cependant, il est possible qu'une passerelle reçoive des données en provenance de serveurs SQL à un débit supérieur à celui qu'elle peut télécharger sur Amazon S3 avec la capacité standard de 8 threads, ce qui peut amener le cache local à atteindre sa limite de stockage.

Dans certaines circonstances, Support cela peut augmenter le nombre de threads de téléchargement Amazon S3 pour votre passerelle de 8 à 40, ce qui permet de charger davantage de données en parallèle. En fonction de la bande passante et d'autres facteurs spécifiques à votre déploiement, cela peut augmenter considérablement les performances de téléchargement et contribuer à réduire la quantité de stockage en cache nécessaire pour prendre en charge votre charge de travail.

Nous vous recommandons d'utiliser cette `CachePercentDirty` CloudWatch métrique pour surveiller la quantité de données stockées sur les disques de cache de la passerelle locale qui n'ont pas encore été chargées vers Amazon S3, et de contacter Support pour déterminer si l'augmentation du nombre de threads de téléchargement peut améliorer le débit de votre passerelle de fichiers S3. Pour plus d'informations, consultez la section Comprendre les métriques de passerelle.

> **Note**
>
> Ce paramètre consomme des ressources supplémentaires du processeur de la passerelle. Nous recommandons de surveiller l'utilisation du processeur de la passerelle et d'augmenter les ressources du processeur allouées si nécessaire.

Désactiver l'actualisation automatique du cache

La fonctionnalité d'actualisation automatique du cache permet à votre passerelle de fichiers S3 d'actualiser automatiquement ses métadonnées, ce qui permet de capturer les modifications apportées par les utilisateurs ou les applications à votre ensemble de fichiers en écrivant directement dans le compartiment Amazon S3, plutôt que par le biais de la passerelle. Pour plus d'informations, consultez Actualisation du cache d'objets du compartiment Amazon S3.

Pour optimiser le débit de la passerelle, nous recommandons de désactiver cette fonctionnalité dans les déploiements où toutes les lectures et écritures dans le compartiment Amazon S3 seront effectuées via votre passerelle de fichiers S3.

Lorsque vous configurez l'actualisation automatique du cache, tenez compte des points suivants :

- Si vous devez utiliser l'actualisation automatique du cache parce que des utilisateurs ou des applications de votre déploiement écrivent parfois directement sur Amazon S3, nous vous recommandons de configurer l'intervalle de temps le plus long possible entre les actualisations, ce qui est toujours pratique pour les besoins de votre entreprise. Un intervalle d'actualisation du cache plus long permet de réduire le nombre d'opérations de métadonnées que la passerelle doit effectuer lors de la navigation dans les répertoires ou de la modification de fichiers.

  Par exemple : définissez l'actualisation automatique du cache sur 24 heures, au lieu de 5 minutes, si cela est acceptable pour votre charge de travail.
- L'intervalle de temps minimum est de 5 minutes. L'intervalle maximal est de 30 jours.
- Si vous choisissez de définir un intervalle d'actualisation du cache très court, nous vous recommandons de tester l'expérience de navigation dans les annuaires pour vos serveurs SQL. Le temps nécessaire pour actualiser le cache de la passerelle peut augmenter considérablement en fonction du nombre de fichiers et de sous-répertoires contenus dans votre compartiment Amazon S3.

Déployez plusieurs passerelles pour prendre en charge la charge de travail

Storage Gateway peut prendre en charge les sauvegardes SQL pour les environnements de grande taille comprenant des centaines de bases de données SQL, plusieurs serveurs SQL et des centaines de téraoctets de données de sauvegarde en répartissant la charge de travail sur plusieurs passerelles.

Lorsque vous planifiez un déploiement avec plusieurs passerelles et serveurs SQL, tenez compte des points suivants :

- Une passerelle unique peut généralement télécharger jusqu'à 20 To par jour, avec des ressources matérielles et une bande passante suffisantes. Vous pouvez augmenter cette limite jusqu'à 40 To par jour en augmentant le nombre de threads de téléchargement Amazon S3.
- Nous vous recommandons d'effectuer un proof-of-concept test pour mesurer les performances et prendre en compte toutes les variables de votre déploiement. Après avoir déterminé le débit

maximal de votre charge de travail de sauvegarde SQL, vous pouvez adapter le nombre de passerelles en fonction de vos besoins.

- Nous vous recommandons de concevoir votre solution en tenant compte de la croissance, car le nombre et la taille des bases de données peuvent augmenter au fil du temps. Pour continuer à évoluer et à prendre en charge une charge de travail croissante, vous pouvez déployer des passerelles supplémentaires selon vos besoins.

Ressources supplémentaires pour les charges de travail de sauvegarde des bases de données

- Stockez les sauvegardes SQL Server dans Amazon S3 à l'aide de AWS Storage Gateway
- Stockez facilement vos sauvegardes SQL Server dans Amazon S3 à l'aide de File Gateway
- Utilisation AWS Storage Gateway pour stocker des sauvegardes de bases de données Oracle dans Amazon S3
- Sauvegarde de bases de données Oracle sur Amazon S3 à grande échelle
- Intégrez une base de données SAP ASE à Amazon S3 à l'aide de AWS Storage Gateway
- Comment One AWS Hero l'utilise AWS Storage Gateway pour la sauvegarde dans le cloud
- Meilleures pratiques en matière de dimensionnement du cache de S3 File Gateway

Sécurité dans AWS Storage Gateway

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Storage Gateway, consultez AWS Services in Scope by Compliance Program AWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utilisez Storage Gateway. Les rubriques suivantes vous montrent comment configurer Storage Gateway pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Storage Gateway.

Protection des données dans AWS Storage Gateway

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans AWS Storage Gateway. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée d'AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou Gestion des identités et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Storage Gateway ou autre Services AWS à l'aide de la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement des données en utilisant AWS KMS

Amazon FSx File Gateway prend en charge le chiffrement SMB conformément à la dernière spécification SMB v3.1.1, y compris les normes AES 128 CCM et AES 128 GCM. Les clients compatibles se connecteront automatiquement à l'aide du chiffrement. En outre, FSx File Gateway utilise le chiffrement SMB lorsqu'il communique avec FSx Windows File Server dans AWS. Vous

devez configurer un Direct Connect lien vers AWS et définir des politiques appropriées pour autoriser le trafic SMB et le trafic de gestion à AWS passer par.

Chiffrer un système de fichiers

Pour plus d'informations, consultez la section Chiffrement des données sur Amazon FSx dans le guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.

Lorsque vous utilisez AWS KMS le chiffrement de vos données, gardez à l'esprit les points suivants :

- Vos données sont chiffrées lorsqu'elles sont au repos dans le cloud. C'est-à-dire que les données sont cryptées dans Amazon FSx.
- Les utilisateurs IAM doivent disposer des autorisations requises pour appeler les opérations AWS KMS d'API. Pour plus d'informations, consultez Utilisation des politiques IAM avec AWS KMS dans le Guide du développeur AWS Key Management Service .

> **Important**
>
> Lorsque vous utilisez une AWS KMS clé pour le chiffrement côté serveur, vous devez choisir une clé symétrique. Storage Gateway ne prend pas en charge les clés asymétriques. Pour en savoir plus, consultez Utilisation des clés symétriques et asymétriques dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations AWS KMS, voir Qu'est-ce que c'est AWS Key Management Service ?

Gestion des identités et des accès pour AWS Storage Gateway

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources AWS SGW. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion de l'accès à l'aide de politiques
- Comment AWS Storage Gateway fonctionne avec IAM

- Exemples de politiques basées sur l'identité pour Storage Gateway AWS
- Résolution des problèmes AWS d'identité et d'accès à Storage Gateway
- Utilisation de balises pour contrôler l'accès à votre passerelle et à vos ressources

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction de votre rôle :

- Utilisateur du service : demandez des autorisations à votre administrateur si vous ne pouvez pas accéder aux fonctionnalités (voir Résolution des problèmes AWS d'identité et d'accès à Storage Gateway)
- Administrateur du service : déterminez l'accès des utilisateurs et soumettez les demandes d'autorisation (voir Comment AWS Storage Gateway fonctionne avec IAM)
- Administrateur IAM : rédigez des politiques pour gérer l'accès (voir Exemples de politiques basées sur l'identité pour Storage Gateway AWS)

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez Connexion à votre Compte AWS dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez Signature AWS Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources.

Il est vivement déconseillé d’utiliser l’utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d’identification de l’utilisateur racine, consultez Tâches qui requièrent les informations d’identification de l’utilisateur racine dans le Guide de l’utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d’identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d’utiliser AWS IAM Identity Center. Pour plus d’informations, consultez Qu’est-ce que IAM Identity Center ? dans le Guide de l’utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité qui dispose d’autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d’utiliser ces informations d’identification temporaires au lieu des utilisateurs IAM avec des informations d’identification à long terme. Pour plus d'informations, voir Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires dans le guide de l'utilisateur IAM.

Les groupes IAM spécifient une collection d’utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d’utilisateurs. Pour plus d’informations, consultez Cas d’utilisation pour les utilisateurs IAM dans le Guide de l’utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité dotée d’autorisations spécifiques qui fournit des informations d’identification temporaires. Vous pouvez assumer un rôle en passant d'un rôle d'utilisateur à un rôle IAM (console) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d’informations, consultez Méthodes pour endosser un rôle dans le Guide de l’utilisateur IAM.

Les rôles IAM sont utiles pour l’accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d’informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l’utilisateur IAM.

Gestion de l’accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d’informations les documents de politique JSON, consultez Vue d’ensemble des politiques JSON dans le Guide de l’utilisateur IAM.

À l’aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d’aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l’opération.

Politiques basées sur l’identité

Les stratégies basées sur l’identité sont des documents de stratégie d’autorisations JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Définition d’autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l’utilisateur IAM.

Les politiques basées sur l’identité peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l’utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Vous devez spécifier un principal dans une politique basée sur les ressources.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) — Spécifiez les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez Politiques de contrôle de service dans le Guide de l'utilisateur AWS Organizations .
- Politiques de contrôle des ressources (RCPs) : définissez le maximum d'autorisations disponibles pour les ressources de vos comptes. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Storage Gateway fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS SGW, découvrez quelles fonctionnalités IAM peuvent être utilisées avec SGW. AWS

Fonctionnalités IAM que vous pouvez utiliser avec AWS Storage Gateway

Fonctionnalité IAM	AWS Assistance SGW
Politiques basées sur l’identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Transmission des sessions d’accès (FAS)	Oui
Rôles de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS SGW et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour SGW AWS

Prend en charge les politiques basées sur l’identité : oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Définition d’autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour SGW AWS

Pour consulter des exemples de politiques basées sur l'identité AWS SGW, consultez. Exemples de politiques basées sur l'identité pour Storage Gateway AWS

Politiques basées sur les ressources au sein de SGW AWS

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour AWS SGW

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions AWS SGW, reportez-vous à la section Actions définies par AWS Storage Gateway dans le Service Authorization Reference.

Les actions politiques dans AWS SGW utilisent le préfixe suivant avant l'action :

```
sgw
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

Pour consulter des exemples de politiques basées sur l'identité AWS SGW, consultez. Exemples de politiques basées sur l'identité pour Storage Gateway AWS

Ressources politiques pour AWS SGW

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources AWS SGW et leurs caractéristiques ARNs, consultez la section Resources Defined by AWS Storage Gateway dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez la section Actions définies par AWS Storage Gateway.

Pour consulter des exemples de politiques basées sur l'identité AWS SGW, consultez. Exemples de politiques basées sur l'identité pour Storage Gateway AWS

Clés de conditions de politique pour AWS SGW

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition AWS SGW, reportez-vous à la section Clés de condition pour AWS Storage Gateway dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Storage Gateway.

Pour consulter des exemples de politiques basées sur l'identité AWS SGW, consultez. Exemples de politiques basées sur l'identité pour Storage Gateway AWS

ACLs en AWS SGW

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec SGW AWS

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs nommés balise. Vous pouvez associer des balises aux entités et aux AWS

ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AWS SGW

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM et Services AWS compatibles avec IAM dans le Guide de l'utilisateur IAM.

Sessions d'accès transmises pour AWS SGW

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour AWS SGW

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut interrompre les fonctionnalités de AWS SGW. Modifiez les rôles de service uniquement lorsque AWS SGW fournit des instructions à cet effet.

Rôles liés aux services pour SGW AWS

Prend en charge les rôles liés à un service : oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Storage Gateway AWS

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources AWS SGW. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS SGW, y compris le ARNs format de chaque type de ressource, consultez la section Actions, ressources et clés de condition pour AWS Storage Gateway dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la AWS console SGW
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AWS SGW dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles.

Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la AWS console SGW

Pour accéder à la console AWS Storage Gateway, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources AWS SGW de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console AWS SGW, associez également la AWS SGW *ConsoleAccess* ou la politique *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

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

```
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Résolution des problèmes AWS d'identité et d'accès à Storage Gateway

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS SGW et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS SGW
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources AWS SGW

Je ne suis pas autorisé à effectuer une action dans AWS SGW

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `sgw:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `sgw:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à AWS SGW.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS SGW. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

> **Important**
>
> Storage Gateway peut assumer les rôles de service existants qui sont transmis à l'aide de l'action de `iam:PassRole` stratégie, mais il ne prend pas en charge les politiques IAM qui utilisent la clé de `iam:PassedToService` contexte pour limiter l'action à des services spécifiques.
> Pour plus d'informations, consultez les rubriques suivantes dans le Gestion des identités et des accès AWS Guide de l'utilisateur :
>
> - IAM : transmettre un rôle IAM à un service spécifique AWS
> - Octroi à un utilisateur de l'autorisation de transmettre un rôle à un AWS service
> - Clés disponibles pour IAM

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes ressources AWS SGW

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si AWS SGW prend en charge ces fonctionnalités, consultezComment AWS Storage Gateway fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de balises pour contrôler l'accès à votre passerelle et à vos ressources

Pour contrôler l'accès aux ressources et aux actions de la passerelle, vous pouvez utiliser des politiques Gestion des identités et des accès AWS (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`.

JSON

```
{
    "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:us-east-1:111122223333:*/*"
        }
    ]
}
```

Contrôle de l'accès en fonction des balises dans une demande IAM

Pour contrôler ce qu'un utilisateur peut faire sur une ressource de passerelle, vous pouvez utiliser les conditions d'une politique IAM basée sur des balises. Par exemple, vous pouvez rédiger une politique qui autorise ou refuse à un utilisateur la possibilité d'effectuer des opérations d'API spécifiques en fonction de la balise qu'il a fournie lors de la création de 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 **`Department`** et **`Finance`**. 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.

JSON

```
{
   "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"
            }
         }
      }
   ]
}
```

Validation de conformité pour AWS Storage Gateway

Des auditeurs tiers évaluent la sécurité et la conformité de AWS Storage Gateway dans le cadre de plusieurs programmes de AWS conformité. Il s'agit notamment du SOC, du PCI, de l'ISO, du FedRAMP, de l'HIPAA, du MTCS, du C5, du K-ISMS, de l'ENS High, de l'OSPAR et du HITRUST CSF.

Pour une liste des AWS services concernés par des programmes de conformité spécifiques, voir AWS Services concernés par programme de conformitéAWS . Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lorsque vous utilisez Storage Gateway est déterminée par la sensibilité de vos données, des objectifs de conformité de votre entreprise, ainsi que de la législation et de la réglementation en vigueur. AWS fournit les ressources suivantes pour faciliter le respect de la conformité :

- Guides de démarrage rapide sur la sécurité et la conformité Guides sur la sécurité et la conformité — Ces guides de déploiement abordent les considérations architecturales et fournissent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA — Ce livre blanc décrit comment les entreprises peuvent créer des applications conformes à la loi HIPAA. AWS
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- Évaluation des ressources à l'aide des règles énoncées dans le guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub CSPM— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans AWS Storage Gateway

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité.

Un Région AWS est un emplacement physique dans le monde entier où les centres de données sont regroupés. Chaque groupe de centres de données logiques est appelé zone de disponibilité (AZ). Chacun Région AWS comprend au moins trois personnes isolées et physiquement séparées AZs au sein d'une zone géographique. Contrairement aux autres fournisseurs de cloud, qui définissent souvent une région comme un centre de données unique, la conception multi-AZ de chacun d'entre

eux Région AWS offre des avantages distincts. Chaque AZ dispose d'une alimentation, d'un refroidissement et d'une sécurité physique indépendants et est connecté via des ultra-low-latency réseaux redondants. Si votre déploiement nécessite de mettre l'accent sur la haute disponibilité, vous pouvez configurer les services et les ressources de manière à ce qu'ils soient multiples AZs afin d'obtenir une meilleure tolérance aux pannes.

Régions AWS répondent aux plus hauts niveaux de sécurité de l'infrastructure, de conformité et de protection des données. Tout le trafic entre les deux AZs est crypté. Les performances du réseau sont suffisantes pour réaliser une réplication synchrone entre AZs. AZs simplifiez le partitionnement des services et des ressources pour une haute disponibilité. Si votre déploiement est partitionné AZs, vos ressources sont mieux isolées et protégées contre les problèmes tels que les pannes de courant, les éclairs, les tornades, les tremblements de terre, etc. AZs sont physiquement séparés par une distance significative de toute autre AZ, bien que tous soient situés à moins de 100 km (60 miles) l'un de l'autre.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS globale, Storage Gateway prend en charge VMware vSphere High Availability (VMware HA) pour protéger les charges de travail de stockage contre les pannes matérielles, d'hyperviseurs ou de réseau. Pour plus d'informations, consultez la section Utilisation de VMware vSphere High Availability avec Storage Gateway Utilisation de Gateway.

Sécurité de l'infrastructure dans AWS Storage Gateway

En tant que service géré, AWS Storage Gateway est protégé par les procédures de sécurité du réseau AWS mondial décrites dans Security Pillar - AWS Well-Architected Framework.

Vous utilisez des appels d'API AWS publiés pour accéder à Storage Gateway via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2. 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.

> **Note**
>
> Vous devez traiter l'appliance AWS Storage Gateway comme une machine virtuelle gérée et ne pas tenter d'accéder à son installation ou de la modifier de quelque manière que ce soit. Toute tentative d'installation d'un logiciel de numérisation ou de mise à jour de progiciels à l'aide de méthodes autres que le mécanisme normal de mise à jour de la passerelle peut entraîner un dysfonctionnement de la passerelle et avoir un impact sur notre capacité à prendre en charge ou à réparer la passerelle.
> AWS examine, analyse et CVEs corrige régulièrement. Nous intégrons des correctifs à ces problèmes dans Storage Gateway dans le cadre de notre cycle normal de publication des logiciels. Ces correctifs sont généralement appliqués dans le cadre du processus normal de mise à jour de la passerelle pendant les fenêtres de maintenance planifiées. Pour plus d'informations sur les mises à jour de passerelle, voir Gestion des mises à jour de passerelle à l'aide de la AWS Storage Gateway console.

AWS Bonnes pratiques en matière de sécurité

AWS fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Ces bonnes pratiques doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations. Pour plus d’informations, consultez les Bonnes pratiques de sécuritéAWS.

Connexion et surveillance AWS Storage Gateway

Storage Gateway est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Storage Gateway. CloudTrail capture tous les appels d'API pour Storage Gateway sous forme d'événements. Les appels capturés incluent les appels de la console Storage Gateway et les appels de code adressés aux opérations d’API Storage Gateway. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour Storage Gateway. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Storage Gateway, l'adresse IP à partir de

laquelle la demande a été effectuée, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur Storage Gateway dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Storage Gateway, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris ceux relatifs à Storage Gateway, créez un historique. Un suivi permet CloudTrail de transférer des fichiers journaux vers un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal d'activité consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Simple Storage Service (Amazon S3) de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les actions Storage Gateway sont consignées et documentées dans la rubrique Actions. Par exemple, les appels aux `ActivateGateway` `ListGateways`, et `ShutdownGateway` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou Gestion des identités et des accès AWS (IAM).

- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail .

Comprendre les entrées des fichiers journaux de Storage Gateway

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'action.

```
{ "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
               "type": "IAMUser",
               "principalId": "AIDAII5AUEPBH2M7JTNVC",
               "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": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
```

```
                                                    },
                                                    "responseElements": {
                                                                          "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                                    },
                                                    "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                                    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                                    "eventType": "AwsApiCall",
                                                    "apiVersion": "20130630",
                                                    "recipientAccountId": "444455556666"
            }]
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l' ListGatewaysaction.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "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 ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
```

```
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
            }]
}
```

Résolution des problèmes liés au déploiement de Storage Gateway

Vous trouverez ci-dessous des informations sur les meilleures pratiques et les problèmes de résolution des problèmes liés aux passerelles, aux plateformes hôtes, aux systèmes de fichiers, à la haute disponibilité, à la restauration des données et aux instantanés. Les informations de dépannage des passerelles sur site concernent les passerelles déployées sur des plateformes de virtualisation prises en charge. Les informations de résolution des problèmes de haute disponibilité concernent les passerelles exécutées sur la plate-forme VMware vSphere High Availability (HA).

Rubriques

- Résolution des problèmes : problèmes liés à la connectivité hors connexion- Découvrez comment diagnostiquer les problèmes susceptibles de faire apparaître votre passerelle hors ligne dans la console Storage Gateway.
- Résolution des problèmes : problèmes liés à Active Directory- Découvrez ce qu'il convient de faire si vous recevez des messages d'erreur tels que `NETWORK_ERRORTIMEOUT`, ou `ACCESS_DENIED` lorsque vous essayez de joindre votre passerelle de fichiers à un domaine Microsoft Active Directory.
- Résolution des problèmes : problèmes d'activation de la passerelle- Découvrez ce qu'il convient de faire si vous recevez un message d'erreur interne lorsque vous tentez d'activer votre Storage Gateway.
- Résolution des problèmes liés à la passerelle sur site- Découvrez les problèmes courants que vous pouvez rencontrer lors de l'utilisation de vos passerelles locales et comment autoriser la connexion Support à votre passerelle pour faciliter le dépannage.
- Résolution des problèmes : problèmes d'installation de Microsoft Hyper-V- Découvrez les problèmes courants que vous pouvez rencontrer lors du déploiement de Storage Gateway sur la plateforme Microsoft Hyper-V.
- Résolution des problèmes : problèmes liés à la passerelle Amazon EC2- Trouvez des informations sur les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec des passerelles déployées sur Amazon EC2.
- Résolution des problèmes : problèmes liés à l'appliance matérielle- Découvrez comment résoudre les problèmes que vous pourriez rencontrer avec l'appliance matérielle AWS Storage Gateway.

- Résolution des problèmes : problèmes liés à la passerelle de fichiers- Trouvez des informations qui peuvent vous aider à comprendre la cause des erreurs et des notifications de santé qui apparaissent dans les CloudWatch journaux de votre passerelle de fichiers.
- Résolution des problèmes : problèmes de haute disponibilité- Découvrez ce qu'il convient de faire si vous rencontrez des problèmes avec les passerelles déployées dans un environnement VMware HA.

Résolution des problèmes : passerelle hors ligne dans la console Storage Gateway

Utilisez les informations de dépannage suivantes pour déterminer ce qu'il convient de faire si la AWS Storage Gateway console indique que votre passerelle est hors ligne.

Il se peut que votre passerelle apparaisse comme étant hors ligne pour une ou plusieurs des raisons suivantes :

- La passerelle ne peut pas atteindre les points de terminaison du service Storage Gateway.
- La passerelle s'est arrêtée de façon inattendue.
- Un disque de cache associé à la passerelle a été déconnecté ou modifié, ou est en panne.

Pour remettre votre passerelle en ligne, identifiez et résolvez le problème à l'origine de sa mise hors ligne.

Vérifiez le pare-feu ou le proxy associé

Si vous avez configuré votre passerelle pour utiliser un proxy, ou si vous l'avez placée derrière un pare-feu, passez en revue les règles d'accès du proxy ou du pare-feu. Le proxy ou le pare-feu doit autoriser le trafic à destination et en provenance des ports réseau et des points de terminaison de service requis par Storage Gateway. Pour plus d'informations, voir Exigences relatives au au réseau et au pare-feu Exigences relatives au au .

Vérifiez s'il existe une inspection SSL ou approfondie des paquets en cours du trafic de votre passerelle

Si une inspection SSL ou approfondie des paquets est actuellement effectuée sur le trafic réseau entre votre passerelle et AWS, il se peut que votre passerelle ne soit pas en mesure de communiquer

avec les points de terminaison de service requis. Pour remettre votre passerelle en ligne, vous devez désactiver l'inspection.

Vérifiez la métrique de IOWait pourcentage après un redémarrage ou une mise à jour logicielle

Après un redémarrage ou une mise à jour logicielle, vérifiez si la `IOWaitPercent` métrique de votre passerelle de fichiers est égale ou supérieure à 10. Cela peut ralentir la réponse de votre passerelle pendant qu'elle reconstruit le cache d'index en RAM. Pour plus d'informations, voir problèmes : Utilisation CloudWatch des métriques.

Vérifiez l'absence d'une panne de courant ou d'une défaillance matérielle sur l'hôte de l'hyperviseur

Une panne de courant ou une panne matérielle sur l'hyperviseur hôte de votre passerelle peut provoquer l'arrêt inattendu de votre passerelle et l'empêcher de l'atteindre. Une fois que vous aurez rétabli l'alimentation et la connectivité réseau, votre passerelle sera de nouveau accessible.

Une fois que votre passerelle sera de nouveau en ligne, assurez-vous de prendre des mesures pour récupérer vos données. Pour plus d'informations, consultez Meilleures pratiques : récupération de vos données .

Vérifiez les problèmes liés à un disque de cache associé

Votre passerelle peut se déconnecter si au moins un des disques de cache associés à votre passerelle a été supprimé, modifié ou redimensionné, ou s'il est endommagé.

Si un disque de cache fonctionnel a été retiré de l'hôte de l'hyperviseur :

1. Arrêtez la passerelle.
2. Ajoutez de nouveau le disque.

> **Note**
>
> Assurez-vous d'ajouter le disque au même nœud de disque.

3. Redémarrez la passerelle.

Si un disque de cache est endommagé, a été remplacé ou a été redimensionné :

- Suivez la procédure de méthode 2 décrite dans Remplacer votre passerelle de fichiers S3 existante par une nouvelle instance pour configurer une nouvelle passerelle et retélécharger les informations du disque cache depuis le AWS cloud.

Résolution des problèmes : problèmes de connexion à la passerelle vers Active Directory

Utilisez les informations de dépannage suivantes pour déterminer la marche à suivre si vous recevez des messages d'erreur tels que `NETWORK_ERRORTIMEOUT`, ou `ACCESS_DENIED` lorsque vous essayez de joindre votre passerelle de fichiers à un domaine Microsoft Active Directory.

Pour résoudre ces erreurs, effectuez les vérifications et les configurations suivantes.

Vérifiez que la passerelle peut atteindre le contrôleur de domaine en exécutant un test nping

Pour exécuter un test nping :

1. Connectez-vous à la console locale de la passerelle à l'aide de votre logiciel de gestion d'hyperviseur (VMware, Hyper-V ou KVM) pour les passerelles sur site, ou à l'aide de SSH pour les passerelles Amazon EC2.
2. Entrez le chiffre correspondant pour sélectionner Gateway Console, puis entrez h pour répertorier toutes les commandes disponibles. Pour tester la connectivité entre la machine virtuelle Storage Gateway et le domaine, exécutez la commande suivante :

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > `corp.domain.com`Remplacez-le par le nom DNS de votre domaine Active Directory et remplacez-le `389` par le port LDAP de votre environnement.
   > Vérifiez que vous avez ouvert les ports requis dans votre pare-feu.

Voici un exemple de test nping réussi où la passerelle a pu atteindre le contrôleur de domaine :

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>

Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

Voici un exemple de test Nping où il n'y a aucune connectivité ou réponse depuis la `corp.domain.com` destination :

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Vérifiez les options DHCP définies pour le VPC de votre instance de passerelle Amazon EC2

Si la passerelle de fichiers est exécutée sur une instance Amazon EC2, vous devez vous assurer qu'un ensemble d'options DHCP est correctement configuré et attaché à l'Amazon Virtual Private Cloud (VPC) qui contient l'instance de passerelle. Pour plus d'informations, consultez les ensembles d'options DHCP dans Amazon VPC.

Vérifiez que la passerelle peut résoudre le domaine en exécutant une requête DIG

Si le domaine ne peut pas être résolu par la passerelle, celle-ci ne peut pas rejoindre le domaine.

Pour exécuter une requête DIG :

1. Connectez-vous à la console locale de la passerelle à l'aide de votre logiciel de gestion d'hyperviseur (VMware, Hyper-V ou KVM) pour les passerelles sur site, ou à l'aide de SSH pour les passerelles Amazon EC2.
2. Entrez le chiffre correspondant pour sélectionner Gateway Console, puis entrez h pour répertorier toutes les commandes disponibles. Pour vérifier si la passerelle peut résoudre le domaine, exécutez la commande suivante :

   ```
   dig -d corp.domain.com
   ```

   > **Note**
   >
   > `corp.domain.com`Remplacez-le par le nom DNS de votre domaine Active Directory.

Voici un exemple de réponse réussie :

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

Vérifiez les paramètres et les rôles du contrôleur de domaine

Vérifiez que le contrôleur de domaine n'est pas configuré en lecture seule et qu'il dispose de suffisamment de rôles pour que les ordinateurs puissent se joindre. Pour tester cela, essayez de joindre d'autres serveurs du même sous-réseau VPC que la machine virtuelle passerelle vers le domaine.

Vérifiez que la passerelle est connectée au contrôleur de domaine le plus proche

La meilleure pratique consiste à associer votre passerelle à un contrôleur de domaine géographiquement proche de l'appliance de passerelle. Si l'appliance de passerelle ne peut pas communiquer avec le contrôleur de domaine dans les 20 secondes en raison de la latence du réseau, le processus d'adhésion au domaine peut expirer. Par exemple, le processus peut expirer si l'appliance de passerelle se trouve dans l'est des États-Unis (Virginie du Nord) Région AWS et que le contrôleur de domaine se trouve dans la région Asie-Pacifique (Singapour Région AWS).

> **Note**
>
> Pour augmenter le délai d'expiration par défaut de 20 secondes, vous pouvez exécuter la commande join-domain dans le AWS Command Line Interface (AWS CLI) et inclure l'`--timeout-in-seconds`option permettant d'augmenter le délai. Vous pouvez également utiliser l'appel JoinDomain d'API et inclure le `TimeoutInSeconds` paramètre pour augmenter le temps. La valeur maximale du délai d'attente est de 3 600 secondes.
> Si vous recevez des erreurs lors de l'exécution de AWS CLI commandes, assurez-vous que vous utilisez la AWS CLI version la plus récente.

Vérifiez qu'Active Directory crée de nouveaux objets informatiques dans l'unité organisationnelle (UO) par défaut

Assurez-vous que Microsoft Active Directory ne possède aucun objet de stratégie de groupe qui crée de nouveaux objets informatiques à un emplacement autre que l'unité d'organisation par défaut. Avant de pouvoir joindre votre passerelle au domaine Active Directory, un nouvel objet informatique doit exister dans l'unité d'organisation par défaut. Certains environnements Active Directory sont personnalisés de manière à ce qu'ils soient différents OUs pour les objets nouvellement créés. Pour garantir qu'un nouvel objet informatique pour la machine virtuelle de passerelle existe dans l'unité

d'organisation par défaut, essayez de créer l'objet ordinateur manuellement sur votre contrôleur de domaine avant de rejoindre la passerelle vers le domaine. Vous pouvez également exécuter la commande join-domain à l'aide du. AWS CLI Spécifiez ensuite l'option pour`--organizational-unit`.

> **Note**
>
> Le processus de création de l'objet informatique est appelé pré-préparation.

Consultez les journaux des événements de votre contrôleur de domaine

Si vous ne parvenez pas à rejoindre la passerelle vers le domaine après avoir essayé toutes les autres vérifications et configurations décrites dans les sections précédentes, nous vous recommandons de consulter les journaux des événements de votre contrôleur de domaine. Vérifiez l'absence d'erreurs dans l'afficheur d'événements du contrôleur de domaine. Vérifiez que les requêtes de passerelle ont atteint le contrôleur de domaine.

Résolution des problèmes : erreur interne lors de l'activation de la passerelle

Les demandes d'activation de Storage Gateway empruntent deux chemins réseau. Les demandes d'activation entrantes envoyées par un client se connectent à la machine virtuelle (VM) de la passerelle ou à l'instance Amazon Elastic Compute Cloud (Amazon EC2) via le port 80. Si la passerelle reçoit correctement la demande d'activation, elle communique avec les points de terminaison Storage Gateway pour recevoir une clé d'activation. Si la passerelle ne parvient pas à atteindre les points de terminaison Storage Gateway, elle répond au client par un message d'erreur interne.

Utilisez les informations de dépannage suivantes pour déterminer ce qu'il convient de faire si vous recevez un message d'erreur interne lorsque vous tentez d'activer votre AWS Storage Gateway.

> **Note**
>
> - Assurez-vous de déployer de nouvelles passerelles à l'aide du dernier fichier image de machine virtuelle ou de la dernière version d'Amazon Machine Image (AMI). Vous recevrez

un message d'erreur interne si vous tentez d'activer une passerelle qui utilise une AMI obsolète.

- Assurez-vous de sélectionner le type de passerelle que vous souhaitez déployer correctement avant de télécharger l'AMI. Les fichiers .ova et chaque type AMIs de passerelle sont différents et ne sont pas interchangeables.

Résoudre les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison public

Pour résoudre les erreurs d'activation lors de l'activation de votre passerelle à l'aide d'un point de terminaison public, effectuez les vérifications et configurations suivantes.

Vérifiez les ports requis

Pour les passerelles déployées sur site, vérifiez que les ports sont ouverts sur votre pare-feu local. Pour les passerelles déployées sur une instance Amazon EC2, vérifiez que les ports sont ouverts sur le groupe de sécurité de l'instance. Pour vérifier que les ports sont ouverts, exécutez une commande telnet sur le point de terminaison public à partir d'un serveur. Ce serveur doit se trouver dans le même sous-réseau que la passerelle. Par exemple, les commandes telnet suivantes testent la connexion au port 443 :

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Pour vérifier que la passerelle elle-même peut atteindre le point de terminaison, accédez à la console de machine virtuelle locale de la passerelle (pour les passerelles déployées sur site). Vous pouvez également accéder par SSH à l'instance de la passerelle (pour les passerelles déployées sur Amazon EC2). Exécutez ensuite un test de connectivité réseau. Confirmez le retour du test`[PASSED]`. Pour plus d'informations, voir votre passerelle Test de la connectivité réseau de .

> **Note**
>
> Le nom d'utilisateur de connexion par défaut pour la console de passerelle est`admin`, et le mot de passe par défaut est`password`.

Assurez-vous que la sécurité du pare-feu ne modifie pas les paquets envoyés depuis la passerelle vers les points de terminaison publics

Les inspections SSL, les inspections approfondies des paquets ou d'autres formes de sécurité par pare-feu peuvent interférer avec les paquets envoyés depuis la passerelle. La prise de contact SSL échoue si le certificat SSL est modifié par rapport aux attentes du point de terminaison d'activation. Pour vérifier qu'aucune inspection SSL n'est en cours, exécutez une commande OpenSSL sur le point de terminaison d'activation principal `anon-cp.storagegateway.region.amazonaws.com` () sur le port 443. Vous devez exécuter cette commande depuis une machine située dans le même sous-réseau que la passerelle :

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> *region*Remplacez-le par votre Région AWS.

Si aucune inspection SSL n'est en cours, la commande renvoie une réponse similaire à la suivante :

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
```

```
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Si une inspection SSL est en cours, la réponse indique une chaîne de certificats modifiée, similaire à ce qui suit :

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

Le point de terminaison d'activation accepte les poignées de main SSL uniquement s'il reconnaît le certificat SSL. Cela signifie que le trafic sortant de la passerelle vers les points de terminaison doit être exempté des inspections effectuées par les pare-feux de votre réseau. Ces inspections peuvent être une inspection SSL ou une inspection approfondie des paquets.

Vérifier la synchronisation de l'heure de la passerelle

Des décalages temporels excessifs peuvent provoquer des erreurs de connexion SSL. Pour les passerelles locales, vous pouvez utiliser la console de machine virtuelle locale de la passerelle pour vérifier la synchronisation de l'heure de votre passerelle. Le décalage temporel ne doit pas dépasser

60 secondes. Pour plus d'informations, voir Synchronisation de l'heure de votre machine virtuelle de passerelle

L'option System Time Management n'est pas disponible sur les passerelles hébergées sur des instances Amazon EC2. Pour vous assurer que les passerelles Amazon EC2 peuvent correctement synchroniser l'heure, vérifiez que l'instance Amazon EC2 peut se connecter à la liste de pools de serveurs NTP suivante via les ports UDP et TCP 123 :

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Résolvez les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison Amazon VPC

Pour résoudre les erreurs d'activation lors de l'activation de votre passerelle à l'aide d'un point de terminaison Amazon Virtual Private Cloud (Amazon VPC), effectuez les vérifications et configurations suivantes.

Vérifiez les ports requis

Assurez-vous que les ports requis au sein de votre pare-feu local (pour les passerelles déployées sur site) ou de votre groupe de sécurité (pour les passerelles déployées dans Amazon EC2) sont ouverts. Les ports requis pour connecter une passerelle à un point de terminaison VPC Storage Gateway sont différents de ceux requis pour connecter une passerelle à des points de terminaison publics. Les ports suivants sont requis pour la connexion à un point de terminaison VPC Storage Gateway :

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

Pour plus d'informations, consultez Création d'un point de terminaison VPC pour Storage Gateway Création d'un point de terminaison VPC pour Storage Gateway Création .

Vérifiez également le groupe de sécurité attaché à votre point de terminaison VPC Storage Gateway. Le groupe de sécurité par défaut attaché au point de terminaison peut ne pas autoriser les ports requis. Créez un nouveau groupe de sécurité qui autorise le trafic provenant de la plage d'adresses IP de votre passerelle sur les ports requis. Attachez ensuite ce groupe de sécurité au point de terminaison du VPC.

> **Note**
>
> Utilisez la console Amazon VPC pour vérifier le groupe de sécurité attaché au point de terminaison VPC. Affichez votre point de terminaison VPC Storage Gateway depuis la console, puis choisissez l'onglet Security Groups.

Pour vérifier que les ports requis sont ouverts, vous pouvez exécuter des commandes telnet sur le point de terminaison VPC Storage Gateway. Vous devez exécuter ces commandes depuis un serveur situé dans le même sous-réseau que la passerelle. Vous pouvez exécuter les tests sur le premier nom DNS qui ne spécifie pas de zone de disponibilité. Par exemple, les commandes telnet suivantes testent les connexions de port requises à l'aide du nom DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com :

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Assurez-vous que la sécurité du pare-feu ne modifie pas les paquets envoyés depuis la passerelle vers votre point de terminaison Amazon VPC (Storage Gateway).

Les inspections SSL, les inspections approfondies des paquets ou d'autres formes de sécurité par pare-feu peuvent interférer avec les paquets envoyés depuis la passerelle. La prise de contact SSL échoue si le certificat SSL est modifié par rapport aux attentes du point de terminaison d'activation. Pour vérifier qu'aucune inspection SSL n'est en cours, exécutez une commande OpenSSL sur votre point de terminaison VPC Storage Gateway. Vous devez exécuter cette commande depuis une

machine située dans le même sous-réseau que la passerelle. Exécutez la commande pour chaque port requis :

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Si aucune inspection SSL n'est en cours, la commande renvoie une réponse similaire à la suivante :

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
```

```
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Si une inspection SSL est en cours, la réponse indique une chaîne de certificats modifiée, similaire à ce qui suit :

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

Le point de terminaison d'activation accepte les poignées de main SSL uniquement s'il reconnaît le certificat SSL. Cela signifie que le trafic sortant de la passerelle vers votre point de terminaison VPC via les ports requis est exempté des inspections effectuées par les pare-feux de votre réseau. Ces inspections peuvent être des inspections SSL ou des inspections approfondies des paquets.

Vérifier la synchronisation de l'heure de la passerelle

Des décalages temporels excessifs peuvent provoquer des erreurs de connexion SSL. Pour les passerelles locales, vous pouvez utiliser la console de machine virtuelle locale de la passerelle pour vérifier la synchronisation de l'heure de votre passerelle. Le décalage temporel ne doit pas dépasser

60 secondes. Pour plus d'informations, voir Synchronisation de l'heure de votre machine virtuelle de passerelle

L'option System Time Management n'est pas disponible sur les passerelles hébergées sur des instances Amazon EC2. Pour vous assurer que les passerelles Amazon EC2 peuvent correctement synchroniser l'heure, vérifiez que l'instance Amazon EC2 peut se connecter à la liste de pools de serveurs NTP suivante via les ports UDP et TCP 123 :

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

Vérifiez la présence d'un proxy HTTP et confirmez les paramètres du groupe de sécurité associés

Avant l'activation, vérifiez si un proxy HTTP sur Amazon EC2 est configuré sur la machine virtuelle de passerelle locale en tant que proxy Squid sur le port 3128. Dans ce cas, confirmez les points suivants :

- Le groupe de sécurité attaché au proxy HTTP sur Amazon EC2 doit disposer d'une règle d'entrée. Cette règle entrante doit autoriser le trafic proxy Squid sur le port 3128 à partir de l'adresse IP de la machine virtuelle de passerelle.
- Le groupe de sécurité attaché au point de terminaison Amazon EC2 VPC doit disposer de règles entrantes. Ces règles entrantes doivent autoriser le trafic sur les ports 1026-1028, 1031, 2222 et 443 à partir de l'adresse IP du proxy HTTP sur Amazon EC2.

Résolvez les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison public et qu'il existe un point de terminaison VPC Storage Gateway dans le même VPC

Pour résoudre les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison public lorsqu'il existe un point de terminaison Amazon Virtual Private Cloud (Amazon VPC) dans le même VPC, effectuez les vérifications et configurations suivantes.

Vérifiez que le paramètre Activer le nom DNS privé n'est pas activé sur votre point de terminaison VPC Storage Gateway

Si l'option Activer le nom DNS privé est activée, vous ne pouvez activer aucune passerelle entre ce VPC et le point de terminaison public.

Pour désactiver l'option de nom DNS privé :

1. Ouvrez la console VPC Amazon.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez votre point de terminaison VPC Storage Gateway.
4. Choisissez Actions.
5. Choisissez Gérer les noms DNS privés.
6. Pour Activer le nom DNS privé, désactivez Activer pour ce point de terminaison.
7. Choisissez Modifier les noms DNS privés pour enregistrer le paramètre.

Résolution des problèmes liés à la passerelle sur site

Vous trouverez ci-dessous des informations sur les problèmes courants que vous pouvez rencontrer lors de l'utilisation de vos passerelles locales et sur la manière d'autoriser la connexion Support à votre passerelle pour faciliter le dépannage.

Le tableau suivant répertorie les problèmes types que vous pourriez rencontrer avec les passerelles sur site.

Problème	Action à exécuter
Vous ne pouvez pas trouver l’adresse IP de votre passerelle.	Utilisez le client de l’hyperviseur pour vous connecter à votre hôte afin de recherche l’adresse IP de la passerelle. • En VMware ESXi effet, l'adresse IP de la machine virtuelle se trouve dans le client vSphere sous l'onglet Résumé. • Pour Microsoft Hyper-V, vous pouvez trouver l’adresse IP de la machine virtuelle en vous connectant à la console locale.

Problème	Action à exécuter
	Si vous avez toujours du mal à trouver l’adresse IP de la passerelle : • Vérifiez que la machine virtuelle est activé. Une adresse IP est attribuée à votre passerelle uniquement lorsque la machine virtuelle est activé. • Attendez que le démarrage de la machine virtuelle soit terminé. Si vous venez d’allumer la machine virtuelle, la passerelle peut mettre quelques minutes pour finaliser sa séquence de démarrage.
Vous rencontrez des problèmes de réseau ou de pare-feu.	• 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 AWS pour ces points de terminaison de service. Pour plus d’informations sur les exigences de réseau et de pare-feu, consultez Exigences pour le réseau et le pare-feu.

Problème	Action à exécuter
L’activation de votre passerelle échoue lorsque vous cliquez sur le bouton Passer à l’activation dans la console de gestion Storage Gateway.	• Vérifiez que la machine virtuelle de la passerelle est accessible en faisant un ping de la machine virtuelle à partir du client. • Vérifiez que votre machine virtuelle dispose d’une connectiv ité 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 la passerelle. • 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 la machine virtuelle de la passerelle est correcte. Pour plus d'informations sur la synchronisation de l'heure des hôtes de l'hyperviseur VMs, 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 de l’assistant Configurer et activer la passerelle. • Vérifiez que votre machine virtuelle dispose d'au moins 16 Go de RAM. L'allocation de passerelle échoue s'il y a moins de 16 Go de RAM. Pour de plus amples informations, veuillez consulter Exigences relatives à la configuration de File Gateway.

Problème	Action à exécuter
Vous avez besoin d’améliorer la bande passante entre votre passerelle et AWS.	Vous pouvez améliorer la bande passante de votre passerelle AWS en configurant votre connexion Internet AWS sur un adaptateur réseau (NIC) distinct de celui qui connecte vos applications et la machine virtuelle de la passerelle. Cette approche est utile si vous disposez d'une connexion à bande passante élevée AWS et que vous souhaitez éviter les problèmes de bande passante, en particulier lors de la restauration d'un instantané. Pour une charge de travail à haut débit, vous pouvez utiliser Direct Connect afin d’établir une connexion réseau dédiée entre votre passerelle sur site et AWS. Pour mesurer la bande passante de la connexion entre votre passerelle et AWS, utilisez les `CloudBytesUploaded` métriques `CloudBytesDownloaded` et de la passerelle. Pour en savoir plus sur ce sujet, consultez Performances et optimisation. L’amélioration de votre connexion Internet permet d’éviter le remplissage de votre tampon de chargement.

Problème	Action à exécuter

Le débit vers ou depuis votre passerelle tombe à zéro.	• Dans l'onglet Gateway de la console Storage Gateway, vérifiez que les adresses IP de votre machine virtuelle de passerelle sont les mêmes que celles que vous voyez dans le logiciel client de votre hyperviseur (c'est-à-dire le client VMware vSphere ou Microsoft Hyper-V Manager). Si elles ne correspondent pas, redémarrez votre passerelle à partir de la console Storage Gateway, comme illustré dans Arrêt de votre machine virtuelle de passerelle. Suite au redémarrage, les adresses dans la liste des Adresses IP de l'onglet Passerelle de la console Storage Gateway doivent correspondre aux adresses IP de votre passerelle, que vous définissez à partir du client de l'hyperviseur.
	  • En VMware ESXi effet, l'adresse IP de la machine virtuelle se trouve dans le client vSphere sous l'onglet Résumé.
	  • Pour Microsoft Hyper-V, vous pouvez trouver l'adresse IP de la machine virtuelle en vous connectant à la console locale.
	• Vérifiez la connectivité de votre passerelle AWS comme décrit dansTest de la connectivité réseau de la passerelle.
	• Vérifiez la configuration de l'adaptateur réseau de votre passerell e dans le client de gestion de l'hyperviseur et assurez-vous que toutes les interfaces que vous souhaitez utiliser pour la passerelle sont activées.
	• Vérifiez la configuration de l'adaptateur réseau de votre passerell e dans la console locale de la passerelle. Pour obtenir des instructions, veuillez consulter Configuration des paramètres réseau de votre passerelle.
	
	Vous pouvez consulter le débit à destination et en provenance de votre passerelle depuis la CloudWatch console Amazon. Pour plus d'informations sur la mesure du débit à destination et en provenance de votre passerelle vers AWS, consultezPerformances et optimisation.

Problème	Action à exécuter
Vous rencontrez des problèmes d'importation (déploiement) de Storage Gateway sur Microsoft Hyper-V.	Consultez Résolution des problèmes : installation de Microsoft Hyper-V, qui traite des problèmes les plus courants de déploiement d'une passerelle sur Microsoft Hyper-V.
Vous recevez un message qui indique que les données qui ont été écrites sur le volume dans votre passerelle ne sont pas stockées en toute sécurité dans AWS.	Vous recevez ce message si la machine virtuelle de la passerelle a été créé à partir d'un clone ou d'un instantané d'une autre machine virtuelle de passerelle. Si ce n'est pas le cas, contactez Support.

Activer l' Support accès pour résoudre les problèmes liés à votre passerelle hébergée sur site

Storage Gateway fournit une console locale que vous pouvez utiliser pour effectuer plusieurs tâches de maintenance, notamment l'autorisation Support d'accéder à votre passerelle pour vous aider à résoudre les problèmes liés à la passerelle. Par défaut, Support l'accès à votre passerelle est désactivé. Vous activez cet accès via la console locale de l'hôte. Pour donner Support accès à votre passerelle, vous devez d'abord vous connecter à la console locale de l'hôte, accéder à la console de Storage Gateway, puis vous connecter au serveur de support.

Pour activer l' Support accès à votre passerelle

1. Connectez-vous à la console locale de l'hôte.
   - VMware ESXi — pour plus d'informations, voirAccès à la console locale de Gateway avec VMware ESXi.
   - Microsoft Hyper-V – pour plus d'informations, consultez Accéder à la console locale de passerelle avec Microsoft Hyper-V.
2. À l'invite, entrez le chiffre correspondant pour sélectionner Console Gateway.
3. Entrez **h** pour ouvrir la liste des commandes disponibles.

4. Effectuez l’une des actions suivantes :

   - Si votre passerelle utilise un point de terminaison public, dans la fenêtre COMMANDES DISPONIBLES, entrez **`open-support-channel`** pour vous connecter au support client 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.
   - Si votre passerelle utilise un point de terminaison de VPC, dans la fenêtre AVAILABLE COMMANDS (COMMANDES DISPONIBLES), entrez **`open-support-channel`**. Si votre passerelle n’est pas activée, indiquez le point de terminaison de VPC ou l’adresse IP pour vous connecter au support client 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 Protocol/User Datagram Protocol (TCP/UDP (contrôle de transmission). Au lieu de cela, la passerelle permet une connexion Secure Shell (SSH) (TCP 22) aux serveurs Storage Gateway et fournit le canal de support pour la connexion.

5. Une fois le canal d'assistance établi, fournissez votre numéro de service d'assistance Support afin de Support pouvoir vous aider à résoudre les problèmes.
6. Une fois la session de support terminée, entrez **`q`** pour y mettre fin. Ne fermez pas la session avant que le support Amazon Web Services vous informe 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.

Résolution des problèmes : installation de Microsoft Hyper-V

Le tableau suivant répertorie les problèmes classiques que vous pouvez rencontrer lors du déploiement de Storage Gateway sur la plateforme Microsoft Hyper-V.

Problème	Action à exécuter
Vous essayez d'importer une passerelle et vous recevez le message d'erreur suivant : « Une erreur de serveur s'est produite lors de la tentative d'importation de la machine virtuelle. L'importation a échoué. Impossible de trouver les fichiers d'importation de machines virtuelles à l'emplacement [...]. Vous ne pouvez importer une machine virtuelle que si vous avez utilisé Hyper-V pour la créer et l'exporter. »	Cette erreur se produit dans les conditions suivantes : • 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 une machine virtuelle doit êtreAWS-Storage-Gateway . Par exemple : `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • Si vous avez déjà déployé une passerelle, mais n'avez pas sélectionné l'option Copier la machine virtuelle et que vous avez activé l'option Dupliquer tous les fichiers dans la boîte de dialogue Importer une machine virtuelle, la machine virtuelle 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. Si vous prévoyez de créer plusieurs passerelles à partir d'un seul emplacement de fichiers source décompressés, vous devez sélectionner Copier la machine virtuelle et cocher la case Dupliquer tous les fichiers dans la boîte de dialogue Importer une machine virtuelle.
Vous essayez d'importer une passerelle et vous recevez le message d'erreur suivant : « Une erreur de serveur s'est produite lors de la tentative d'importation de la machine virtuelle. L'importation a échoué.	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 la machine virtuelle, cette erreur se produit. Pour résoudre ce problème, spécifiez de nouveaux emplacements sous Serveur dans le panneau situé sur le côté gauche de la boîte de dialogue des paramètres Hyper-V.

Problème	Action à exécuter
La tâche d'importation n'a pas réussi à copier le fichier depuis [...] : le fichier existe. (0x80070050) »	
Vous essayez d'importer une passerelle et vous recevez le message d'erreur suivant : « Une erreur de serveur s'est produite lors de la tentative d'importation de la machine virtuelle. L'importation a échoué. L’importation a échoué car la machine virtuelle doit avoir un nouvel identificateur. Sélectionnez un nouvel identificateur et réessayez l’importation. »	Lorsque vous importez la passerelle, assurez-vous de sélectionner Copier la machine virtuelle et de cocher la case Dupliquer tous les fichiers dans la boîte de dialogue Importer une machine virtuelle afin de créer un nouvel identifiant unique pour la machine virtuelle.

Problème	Action à exécuter
Vous essayez de démarrer une machine virtuelle de passerelle et vous recevez le message d'erreur suivant : « Une erreur s'est produite lors de la tentative de démarrage des machines virtuelles sélectionnées. Le paramètre du processeu r de partition enfant est incompatible avec la partition parent. 'AWS-Storage-Gateway' n'a pas pu être initialisé. (ID de machine virtuelle [...]) »	Cette erreur est probablement due à un écart entre le processeur requis CPUs pour la passerelle et le processeur disponible CPUs sur l'hôte. Veillez à ce que le nombre de CPU de la machine virtuelle soit pris en charge par l’hyperviseur sous-jacent. Pour plus d’informations sur les exigences relatives à Storage Gateway, consultez Exigences relatives à la configuration de File Gateway.

Problème	Action à exécuter
Vous essayez de démarrer une machine virtuelle de passerelle et vous recevez le message d'erreur suivant : « Une erreur s'est produite lors de la tentative de démarrage des machines virtuelles sélectionnées. 'AWS-Storage-Gateway' n'a pas pu être initialisé. (ID de machine virtuelle [...]) Impossible de créer la partition : les ressources système sont insuffisantes pour exécuter le service demandé. (0x800705AA) »	Cette erreur est probablement provoquée par un écart de RAM entre la RAM obligatoire pour la passerelle et la RAM disponible sur l'hôte. Pour plus d'informations sur les exigences relatives à Storage Gateway, consultez Exigences relatives à la configuration de File Gateway.
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.	L'horloge de la machine virtuelle 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 la machine virtuelle à l'aide de l'option de synchronisation de l'heure de la console de passerelle. Pour de plus amples informations, veuillez consulter Configuration d'un serveur NTP (Network Time Protocol) pour votre passerelle.
Vous devez placer les fichiers décompressés Storage Gateway de Microsoft Hyper-V sur le système de fichiers hôte.	Accédez à l'hôte comme vous le feriez avec un serveur Microsoft Windows standard. Par exemple, si l'hôte de l'hyperviseur est nommé `hyperv-server` , vous pouvez utiliser le chemin UNC suivant `\\hyperv-server\c$` , ce qui implique que le nom `hyperv-server` peut être résolu ou est défini dans votre fichier d'hôtes local.

Problème	Action à exécuter
Vous êtes invité à saisir les informations d'identification lors de la connexion à l'hyperviseur.	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.
Vous remarquerez peut-être de mauvaises performances réseau si vous activez la file d'attente des machines virtuelles (VMQ) pour un hôte Hyper-V utilisant un adaptateur réseau Broadcom.	Pour plus d'informations sur une solution de contournement, consultez la documentation Microsoft, voir Mauvaises performances réseau sur les machines virtuelles sur un hôte Windows Server 2012 Hyper-V si VMQ est activé.

Résolution des problèmes : 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 Déployer un hôte Amazon EC2 par défaut pour File Gateway FSx.

Rubriques

- L'activation de votre passerelle ne se produit pas au bout de quelques instants
- Vous ne trouvez pas votre instance de passerelle EC2 dans la liste des instances
- Vous souhaitez vous connecter à votre instance de passerelle à l'aide de l'Amazon EC2 Serial Console
- Vous souhaitez aider Support à résoudre les problèmes liés à votre passerelle Amazon EC2

L'activation de votre passerelle ne se produit pas au bout de quelques instants

Vérifiez les points suivants dans la console Amazon EC2 :

- Le port 80 est ouvert dans le groupe de sécurité que vous avez associé à l'instance. Pour plus d'informations sur l'ajout d'une règle de groupe de sécurité, consultez la section Ajout d'une règle de groupe de sécurité dans le guide de l'utilisateur Amazon EC2.
- L'instance de passerelle est marquée comme étant en cours d'exécution. Dans la console Amazon EC2, la valeur État de 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 ce faire, ouvrez la console Storage Gateway , choisissez Déployer 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 souhaitez vous connecter à votre instance de passerelle à l'aide de l'Amazon EC2 Serial Console

Vous pouvez utiliser l'Amazon EC2 Serial Console pour résoudre des problèmes de démarrage, de configuration réseau et autres. Pour obtenir des instructions et des conseils de dépannage, consultez Amazon EC2 Serial Console dans le Guide de l'utilisateur Amazon Elastic Compute Cloud.

Vous souhaitez aider Support à résoudre les problèmes liés à votre passerelle Amazon EC2

Storage Gateway fournit une console locale que vous pouvez utiliser pour effectuer plusieurs tâches de maintenance, notamment l'autorisation Support d'accéder à votre passerelle pour vous aider à résoudre les problèmes liés à la passerelle. Par défaut, Support l'accès à votre passerelle est désactivé. Vous activez cet accès via la console locale Amazon EC2. Vous vous connectez à la console locale Amazon EC2 via Secure Shell (SSH). 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 autoriser la Support connexion à votre passerelle, vous devez d'abord vous connecter à la console locale de l'instance Amazon EC2, accéder à la console de Storage Gateway, puis fournir l'accès.

Pour activer l' Support accès à une passerelle déployée sur une instance Amazon EC2

1. Connectez-vous à la console locale pour votre instance Amazon EC2. Pour obtenir des instructions, consultez Connexion à votre instance dans le Manuel 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**
   >
   > *PRIVATE-KEY*Il s'agit du `.pem` fichier contenant le certificat privé de la paire de clés EC2 que vous avez utilisée pour lancer l'instance Amazon EC2. Pour plus d'informations, consultez Récupération de la clé publique pour votre paire de clés dans le Guide de l'utilisateur Amazon EC2.

*INSTANCE-PUBLIC-DNS-NAME*Il s'agit du nom DNS (Domain Name System) public de votre instance Amazon EC2 sur laquelle votre passerelle s'exécute. Pour obtenir ce nom DNS public, sélectionnez l'instance Amazon EC2 dans la console EC2, puis cliquez sur l'onglet Description.

2. À l'invite, entrez **`6 - Command Prompt`** pour ouvrir la console Support 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 la fenêtre COMMANDES DISPONIBLES, entrez **`open-support-channel`** pour vous connecter au support client 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.
   - Si votre passerelle utilise un point de terminaison de VPC, dans la fenêtre AVAILABLE COMMANDS (COMMANDES DISPONIBLES), entrez **`open-support-channel`**. Si votre passerelle n'est pas activée, indiquez le point de terminaison de VPC ou l'adresse IP pour vous connecter au support client 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 Protocol/User Datagram Protocol (TCP/UDP (contrôle de transmission). Au lieu de cela, la passerelle permet une connexion Secure Shell (SSH) (TCP 22) aux serveurs Storage Gateway et fournit le canal de support pour la connexion.

5. Une fois le canal d'assistance établi, fournissez votre numéro de service d'assistance Support afin de Support pouvoir vous aider à résoudre les problèmes.
6. Une fois la session de support terminée, entrez **`q`** pour y mettre fin. Ne fermez pas la session avant que le support Amazon Web Services vous informe 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 connecter à l'instance Storage Gateway.

Résolution des problèmes : problèmes liés à l'appliance matérielle

> **Note**
>
> Avis de fin de disponibilité : à compter du 12 mai 2025, l'appliance AWS Storage Gateway matérielle ne sera plus proposée. Les clients actuels possédant l'appliance AWS Storage Gateway matérielle peuvent continuer à utiliser et à bénéficier d'une assistance jusqu'en mai 2028. Vous pouvez également utiliser le AWS Storage Gateway service pour donner à vos applications sur site et dans le cloud un accès pratiquement illimité à un espace de stockage dans le cloud.

Les rubriques suivantes traitent des problèmes que vous pouvez rencontrer avec l'appliance matérielle AWS Storage Gateway, ainsi que des suggestions pour les résoudre.

Rubriques

- Impossible de déterminer l’adresse IP du service
- Comment effectuer une réinitialisation d’usine ?
- Comment réaliser un redémarrage à distance ?
- Où obtenir le support technique pour Dell iDRAC ?
- Impossible de trouver le numéro de série de l’appliance matérielle
- Où obtenir le support des appliances matérielles ?

Impossible de 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 rétablir les paramètres d'usine de votre appliance, contactez l'équipe de AWS Storage Gateway Hardware Appliance pour obtenir de l'aide, comme décrit dans la section Support ci-dessous.

Comment réaliser un redémarrage à distance ?

Si vous devez redémarrer votre appliance à distance, vous pouvez le faire à l'aide de l'interface de gestion Dell iDRAC. Pour plus d'informations, voir i DRAC9 Virtual Power Cycle : mise sous tension à distance des PowerEdge serveurs Dell EMC sur le InfoHub site Web de Dell Technologies.

Où obtenir le support technique pour Dell iDRAC ?

Le PowerEdge serveur Dell 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 plus d'informations sur les informations d'identification iDRAC, voir Dell PowerEdge - Quelles sont les informations d'identification de connexion par défaut pour iDRAC ? .
- Assurez-vous que le microprogramme est conçu up-to-date pour empêcher les failles de sécurité.
- 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.

Impossible de trouver le numéro de série de l'appliance matérielle

Vous pouvez trouver le numéro de série de votre dispositif matériel AWS Storage Gateway à l'aide de la console Storage Gateway.

Pour trouver le numéro de série de l'appliance matérielle :

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Le menu de navigation sur la gauche de la page, choisissez Matériel.
3. Sélectionnez votre appliance matérielle dans la liste.
4. Localisez le champ Numéro de série dans l'onglet Détails de votre appareil.

Où obtenir le support des appliances matérielles ?

Pour contacter AWS le support technique pour votre appliance matérielle, consultez Support.

L' Support équipe peut vous demander d'activer le canal d'assistance pour résoudre à distance vos problèmes de passerelle. 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 d'assistance pour AWS

1. Ouvrez la console matérielle.
2. Choisissez Open Support Channel en bas de la page principale de la console matérielle, puis appuyez sur`Enter`.

   Le numéro de port attribué devrait apparaître dans les 30 secondes s'il n'y a aucun problème de connectivité réseau ou de pare-feu. Par exemple :

   État : Ouvert sur le port 19599
3. Notez le numéro de port et indiquez-le à Support.

Résolution des problèmes : problèmes liés à la passerelle de fichiers

Vous pouvez configurer votre passerelle de fichiers pour écrire des entrées de journal dans un groupe de CloudWatch journaux Amazon. Dans ce cas, vous recevez des notifications concernant l'état de santé de la passerelle et toute erreur rencontrée par la passerelle. Vous trouverez des informations sur ces notifications d'erreur et de santé dans CloudWatch les journaux.

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 : FileMissing
- Erreur : FsxFileSystemAuthenticationFailure
- Erreur : FsxFileSystemConnectionFailure
- Erreur : FsxFileSystemFull
- Erreur : GatewayClockOutOfSync
- Erreur : InvalidFileState
- Erreur : ObjectMissing
- Erreur : DroppedNotifications
- Notification : HardReboot

- Notification : Reboot
- Résolution des problèmes : problèmes liés au domaine Active Directory
- Résolution des problèmes : utilisation de CloudWatch métriques

Erreur : FileMissing

L'`FileMissing`erreur est similaire à l'`ObjectMissing`erreur et les étapes pour la résoudre sont identiques. Vous pouvez obtenir un `FileMissing` message d'erreur lorsqu'un rédacteur autre que la passerelle de fichiers spécifiée supprime le fichier spécifié sur Amazon FSx. Tout téléchargement ultérieur vers Amazon FSx ou toute extraction de l'objet FSx depuis Amazon échoue.

Pour résoudre une FileMissing erreur

1. Enregistrez la dernière copie du fichier dans le système de fichiers local de votre client SMB (vous aurez 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.
3. Copiez la dernière version du fichier que vous avez enregistré à l'étape 1 Amazon à FSx l'aide de votre client SMB. Faites-le via votre passerelle de fichiers.

Erreur : FsxFileSystemAuthenticationFailure

Vous pouvez obtenir un `FsxFileSystemAuthenticationFailure` message d'erreur lorsque les informations d'identification fournies lors de l'attachement du système de fichiers ont expiré ou lorsque ses privilèges ont été révoqués.

Pour résoudre une FsxFileSystemAuthenticationFailure erreur

1. Assurez-vous que les informations d'identification fournies au moment de joindre le système de FSx fichiers Amazon sont toujours valides.
2. Assurez-vous que l'utilisateur dispose de toutes les autorisations nécessaires, comme décrit dans Joindre un système de fichiers Amazon FSx pour Windows File Server.

Erreur : FsxFileSystemConnectionFailure

Vous pouvez obtenir un `FsxFileSystemConnectionFailure` message d'erreur lorsque le FSx serveur Amazon est inaccessible depuis la machine passerelle.

Pour résoudre une FsxFileSystemConnectionFailure erreur

1. Assurez-vous que toutes les règles de pare-feu et de VPC autorisent la connexion entre la machine passerelle et le serveur Amazon FSx .
2. Assurez-vous que le FSx serveur Amazon fonctionne.

Erreur : FsxFileSystemFull

Un `FsxFileSystemFull` message d'erreur peut s'afficher lorsqu'il n'y a pas assez d'espace disque disponible dans le système de FSx fichiers Amazon.

Pour résoudre une FsxFileSystemFull erreur

- Augmentez l'espace de stockage pour le système de FSx fichiers Amazon.

Erreur : GatewayClockOutOfSync

Une `GatewayClockOutOfSync` erreur peut se produire lorsque la passerelle détecte une différence de 5 minutes ou plus entre l'heure du système local et l'heure indiquée par les serveurs AWS Storage Gateway. Les problèmes de synchronisation des horloges peuvent avoir un impact négatif sur la connectivité entre la passerelle et AWS. Si l'horloge de la passerelle n'est pas synchronisée, des erreurs d'E/S peuvent se produire pour les connexions NFS et SMB, et les utilisateurs SMB peuvent rencontrer des erreurs d'authentification.

Pour résoudre une GatewayClockOutOfSync erreur

- Vérifiez la configuration réseau entre la passerelle et le serveur NTP. Pour plus d'informations sur la synchronisation de l'heure de la machine virtuelle de passerelle et la mise à jour de la configuration du serveur NTP, voir NTP (Network Time Protocol) pour votre passerelle.

Erreur : InvalidFileState

Vous pouvez obtenir une `InvalidFileState` erreur lorsqu'un rédacteur autre que la passerelle spécifiée modifie le fichier spécifié dans le partage de fichiers spécifié. Par conséquent, l'état du fichier sur la passerelle ne correspond pas à son état sur Amazon FSx. Tout téléchargement ou extraction ultérieur du fichier auprès d'Amazon FSx peut échouer.

Pour résoudre une InvalidFileState erreur

1. Enregistrez la dernière copie du fichier dans le système de fichiers local de votre client SMB (vous devez copier ce fichier à l'étape 4). Si la version du fichier sur Amazon FSx est la plus récente, téléchargez-la. Vous pouvez le faire en accédant directement au FSx partage Amazon via n'importe quel client SMB.
2. Supprimez le fichier FSx directement dans Amazon.
3. Supprimez le fichier de la passerelle à l'aide de votre client SMB.
4. À l'aide de votre client SMB, copiez la dernière version du fichier que vous avez enregistré à l'étape 1, via votre passerelle de fichiers, sur Amazon FSx.

Erreur : ObjectMissing

Vous pouvez obtenir un `ObjectMissing` message d'erreur lorsqu'un rédacteur autre que la passerelle de fichiers spécifiée supprime le fichier spécifié sur Amazon FSx. Tout téléchargement ultérieur vers Amazon FSx ou toute extraction de l'objet FSx depuis Amazon échoue.

Pour résoudre une ObjectMissing erreur

1. Enregistrez la dernière copie du fichier dans le système de fichiers local de votre client SMB (vous aurez 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.
3. Copiez la dernière version du fichier que vous avez enregistré à l'étape 1 Amazon à FSx l'aide de votre client SMB. Faites-le via votre passerelle de fichiers.

Erreur : DroppedNotifications

Une `DroppedNotifications` erreur peut s'afficher à la place des autres types d'entrées de CloudWatch journal attendus lorsque l'espace de stockage disponible sur le disque racine de votre passerelle est inférieur à 1 Go ou si plus de 100 notifications de santé sont générées dans un intervalle d'une minute. Dans ces circonstances, la passerelle cesse de générer des notifications de CloudWatch journal détaillées par mesure de précaution.

Pour résoudre une DroppedNotifications erreur

1. Vérifiez la `Root Disk Usage` métrique dans l'onglet Monitoring correspondant à votre passerelle dans la console Storage Gateway afin de déterminer si l'espace disque racine disponible est insuffisant.
2. Augmentez la taille du disque de stockage racine de la passerelle si l'espace disponible est inférieur à 1 Go. Consultez la documentation de l'hyperviseur de votre machine virtuelle pour obtenir des instructions.

   Pour augmenter la taille du disque racine pour les passerelles Amazon EC2, consultez la section Demander des modifications à vos volumes EBS dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

   > **Note**
   >
   > Il n'est pas possible d'augmenter la taille du disque racine de l'appliance matérielle AWS Storage Gateway.

3. Redémarrez la passerelle.

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 VMware passerelles, une réinitialisation par vSphere High Availability Application Monitoring peut provoquer cet événement.

Lorsque votre passerelle s'exécute dans un tel environnement, vérifiez la présence de la `HealthCheckFailure` notification et consultez le journal VMware des événements de la machine virtuelle.

Notification : Reboot

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 la machine virtuelle 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.

Résolution des problèmes : problèmes liés au domaine Active Directory

FSx File Gateway ne génère pas de messages de journal spécifiques pour les problèmes de domaine Active Directory. Si vous ne parvenez pas à joindre votre passerelle à votre domaine Active Directory, procédez comme suit :

- Vérifiez que la passerelle n'essaie pas d'utiliser un contrôleur de domaine en lecture seule (RODC) pour rejoindre le domaine.
- Vérifiez que la passerelle est configurée pour utiliser les serveurs DNS appropriés.

  Par exemple, si vous essayez de joindre une instance de passerelle Amazon EC2 à un Active Directory AWS géré, vérifiez que l'option DHCP définie pour votre VPC EC2 spécifie les serveurs DNS Active Directory gérés. AWS

  Les serveurs DNS que vous configurez via le jeu d'options DHCP du VPC sont fournis à toutes les instances EC2 du VPC. Si vous souhaitez spécifier un serveur DNS pour une passerelle individuelle, vous pouvez le faire à l'aide de la console locale EC2 de cette passerelle.

  Pour les passerelles locales, vous devez spécifier un serveur DNS à l'aide de la console locale de la machine virtuelle.
- Vérifiez la connectivité réseau de la passerelle en exécutant les commandes suivantes à partir de l'invite de commande de la console locale de la passerelle. Remplacez les variables surlignées par le nom de domaine et les adresses IP réels de votre déploiement.

  ```
  dig -d ExampleDomainName
  ncport -d ExampleDomainControllerIPAddress -p 445
  ncport -d ExampleDomainControllerIPAddress -p 389
  ```
- Vérifiez que votre compte de service Active Directory dispose des autorisations requises. Pour plus d'informations, voir Exigences relatives aux autorisations relatives aux aux comptes de service Active Directory.
- Vérifiez que la passerelle rejoint la bonne unité organisationnelle (UO).

L'adhésion à un domaine crée un compte d'ordinateur Active Directory dans le conteneur d'ordinateurs par défaut (qui n'est pas une unité d'organisation), en utilisant l'ID de passerelle de la passerelle comme nom de compte (par exemple, SGW-1234ADE). Il n'est pas possible de personnaliser le nom de ce compte.

Si votre environnement Active Directory dispose d'une unité d'organisation désignée pour les nouveaux objets informatiques, vous devez spécifier cette unité d'organisation lorsque vous rejoignez le domaine.

Si vous rencontrez des erreurs de refus d'accès lorsque vous tentez de rejoindre l'unité d'organisation désignée, contactez votre administrateur de domaine Active Directory. L'administrateur devra peut-être pré-configurer le compte informatique de la passerelle avant que celle-ci puisse rejoindre le domaine. Pour plus d'informations, consultez Comment puis-je résoudre les problèmes liés à la connexion de ma passerelle de fichiers Storage Gateway à un domaine pour l'authentification Microsoft Active Directory ? .

- Vérifiez que le nom d'hôte de votre passerelle peut être résolu dans le DNS en exécutant la commande suivante à partir de l'invite de commande de la console locale de la passerelle. Remplacez la variable surlignée par le nom d'hôte réel de votre passerelle.

```
dig -d ExampleHostName -r A
```

  Si vous avez configuré un nom d'hôte personnalisé pour votre passerelle, vous devez ajouter manuellement un enregistrement DNS A qui pointe vers son adresse IP.

- Vérifiez que la latence du réseau entre la passerelle et le contrôleur de domaine est raisonnablement faible. La requête pour rejoindre un domaine peut expirer si la passerelle ne reçoit pas de réponse du contrôleur de domaine dans les 20 secondes.

  Si vous rejoignez la passerelle vers le domaine à l'aide de la commande JoinDomainCLI, vous pouvez ajouter l'`--timeout-in-seconds`indicateur pour augmenter le délai d'attente à un maximum de 3 600 secondes.

- Vérifiez que l'utilisateur Active Directory que vous utilisez pour rejoindre la passerelle vers le domaine possède les privilèges requis pour ce faire.

Résolution des problèmes : utilisation de CloudWatch métriques

Vous trouverez ci-dessous des informations sur les mesures à prendre pour résoudre les problèmes liés à l'utilisation CloudWatch des métriques Amazon avec Storage Gateway.

Rubriques

- Votre passerelle réagit lentement lorsque vous parcourez les annuaires
- Votre passerelle ne répond pas
- Vous ne voyez aucun fichier dans votre système de FSx fichiers Amazon
- Les anciens instantanés ne s'affichent pas dans votre système de FSx fichiers Amazon
- Votre passerelle est lente à transférer des données vers Amazon FSx
- La tâche de sauvegarde de votre passerelle échoue ou des erreurs se produisent lors de l'écriture sur votre passerelle

Votre passerelle réagit lentement lorsque vous parcourez les annuaires

Si votre passerelle de fichiers réagit lentement lorsque vous exécutez la ls commande ou parcourez les répertoires, vérifiez les `IndexEviction` CloudWatch métriques `IndexFetch` et :

- Si la `IndexFetch` métrique est supérieure à 0 lorsque vous exécutez une `ls` commande ou parcourez des répertoires, votre passerelle de fichiers démarrait sans informations sur le contenu du répertoire concerné et devait accéder au serveur de fichiers FSx pour Windows. Les opérations ultérieures pour répertorier le contenu de ce répertoire devraient s'exécuter plus rapidement.
- Si la `IndexEviction` 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 dans le répertoire le moins récemment consulté pour répertorier un nouveau répertoire. Si cela se produit fréquemment et que cela a un impact sur les performances, contactez Support.

  Discutez Support du contenu du système de FSx fichiers Amazon associé et des 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 I/O demande de disque est en suspens. 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 bloquée par un disque racine lent alors qu'elle reconstruit le cache d'index en RAM. Vous pouvez résoudre ce problème en utilisant un disque physique plus rapide pour le disque racine.
- Si la `MemUsedBytes` métrique est égale ou presque identique à la `MemTotalBytes` métrique, cela signifie que votre passerelle de fichiers n'a plus 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 de la 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 de la RAM à votre passerelle de fichiers.

Vous ne voyez aucun fichier dans votre système de FSx fichiers Amazon

Si vous remarquez que les fichiers de la passerelle ne sont pas reflétés dans le système de FSx fichiers Amazon, vérifiez la `FilesFailingUpload` métrique. Si l'indicateur indique que le téléchargement de certains fichiers échoue, consultez vos notifications de santé. Lorsque le téléchargement des fichiers échoue, la passerelle génère une notification de santé contenant plus de détails sur le problème.

Les anciens instantanés ne s'affichent pas dans votre système de FSx fichiers Amazon

Certaines opérations sur les fichiers sur la passerelle de FSx fichiers, telles que le changement de nom de dossiers de niveau supérieur ou la modification des autorisations, peuvent entraîner plusieurs opérations sur les fichiers qui entraînent une I/O charge importante sur votre système FSx de fichiers Windows File Server. Si votre système de fichiers ne dispose pas de ressources de performance suffisantes pour votre charge de travail, il est possible qu'il supprime les clichés instantanés, car il donne la priorité à la disponibilité permanente I/O plutôt qu'à la conservation historique des clichés instantanés.

Dans la FSx console Amazon, consultez la page Surveillance et performances pour voir si votre système de fichiers est sous-approvisionné. Si tel est le cas, vous pouvez passer au stockage SSD,

augmenter la capacité de débit ou augmenter le nombre d'IOPS du SSD pour gérer votre charge de travail.

Votre passerelle est lente à transférer des données vers Amazon FSx

Si votre passerelle de fichiers met du temps à transférer des données vers Amazon FSx pour Windows File Server, procédez comme suit :

- Si la `CachePercentDirty` métrique est supérieure ou égale à 80, votre passerelle de fichiers écrit les données sur le disque plus rapidement qu'elle ne peut les charger sur le serveur de fichiers Amazon FSx pour Windows. Envisagez d'augmenter la bande passante pour le téléchargement depuis votre passerelle de fichiers, d'ajouter un ou plusieurs disques de cache, de ralentir les écritures du client ou d'augmenter la capacité de débit du serveur de fichiers Amazon FSx pour Windows associé.
- Si la `CachePercentDirty` métrique est faible, `IoWaitPercent` vérifiez-la. Si `IoWaitPercent` cette valeur est supérieure à 10, votre passerelle de fichiers est peut-être ralentie par la vitesse du disque 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.

La tâche de sauvegarde de votre passerelle échoue ou des erreurs se produisent lors de l'écriture sur votre passerelle

Si votre tâche de sauvegarde de File Gateway échoue ou si des erreurs se produisent lors de l'écriture sur votre passerelle de fichiers, procédez comme suit :

- Si la `CachePercentDirty` métrique est supérieure ou égale 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 rapidité avec laquelle votre passerelle de fichiers se télécharge vers pour Windows File Server, consultez la `CloudBytesUploaded` métrique. Comparez cette métrique à la `WriteBytes` métrique, qui indique la rapidité avec laquelle le client écrit des fichiers sur votre passerelle de fichiers. Si le client SMB écrit sur votre passerelle de fichiers plus rapidement qu'il ne peut le télécharger pour Windows File Server, ajoutez des disques de cache supplémentaires pour couvrir au minimum la taille de la tâche de sauvegarde. Vous pouvez également augmenter la bande passante de chargement.

- Si une copie de fichier volumineuse, telle qu'une tâche de sauvegarde, échoue mais que la `CachePercentDirty` métrique est inférieure à 80 %, votre passerelle de fichiers atteint peut-être un délai d'expiration de session côté client. Pour les PME, vous pouvez augmenter ce délai à l'aide de la PowerShell commande. `Set-SmbClientConfiguration -SessionTimeout 300` L'exécution de cette commande définit le délai d'expiration à 300 secondes.

Notifications d’intégrité relatives à la haute disponibilité

Lorsque vous exécutez votre passerelle sur la plate-forme VMware vSphere High Availability (HA), vous pouvez recevoir des notifications de santé. Pour plus d’informations sur les notifications relatives à l’état, consultez Résolution des problèmes : problèmes de haute disponibilité.

Résolution des problèmes : problèmes de haute disponibilité

Vous trouverez ci-dessous des informations sur les actions à entreprendre si vous rencontrez des problèmes de disponibilité.

Rubriques

- Notifications d’intégrité
- Métriques

Notifications d’intégrité

Lorsque vous exécutez votre passerelle sur VMware vSphere HA, toutes les passerelles envoient les notifications de santé suivantes au groupe de journaux Amazon CloudWatch que vous avez configuré. Ces notifications vont dans un flux de journaux appelé `AvailabilityMonitor`.

Rubriques

- Notification : Reboot
- Notification : HardReboot
- Notification : HealthCheckFailure
- Notification : AvailabilityMonitorTest

Notification : Reboot

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 la machine virtuelle 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 VMware passerelles, une réinitialisation par vSphere High Availability Application Monitoring peut provoquer cet événement.

Action à exécuter

Lorsque votre passerelle s'exécute dans un tel environnement, vérifiez la présence de la `HealthCheckFailure` notification et consultez le journal VMware des événements de la machine virtuelle.

Notification : HealthCheckFailure

Pour une passerelle sur VMware vSphere HA, vous pouvez recevoir une `HealthCheckFailure` notification lorsqu'un contrôle de santé échoue et qu'un redémarrage de 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 VMware passerelles.

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'une assistance supplémentaire, contactez Support.

Notification : AvailabilityMonitorTest

Pour une passerelle sur VMware vSphere HA, vous pouvez recevoir une `AvailabilityMonitorTest` notification lorsque vous testez le système de surveillance de la disponibilité et des applications 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 le groupe de CloudWatch journaux que vous avez configuré pour plus de détails sur les événements.

Bonnes pratiques pour File Gateway

Cette section contient les rubriques suivantes, qui fournissent des informations sur les meilleures pratiques relatives à l'utilisation des passerelles, des partages de fichiers, des compartiments et des données. Nous vous recommandons de vous familiariser avec les informations décrites dans cette section et d'essayer de suivre ces directives afin d'éviter tout problème avec votre AWS Storage Gateway. Pour obtenir des conseils supplémentaires sur le diagnostic et la résolution des problèmes courants que vous pourriez rencontrer lors de votre déploiement, consultezRésolution des problèmes liés au déploiement de Storage Gateway.

Rubriques

- Bonnes pratiques : récupération de vos données
- Restauration à partir de sauvegardes ou de snapshots directement sur Amazon FSx
- Nettoyez les ressources inutiles

Bonnes pratiques : récupération de vos données

Bien que cela soit rare, votre passerelle peut rencontrer une défaillance irrécupérable. Une panne peut se produire sur la machine virtuelle (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'une machine virtuelle de passerelle à partir d'un instantané créé par votre hyperviseur ou de votre Amazon Machine Image (AMI) d'Amazon EC2. Si la machine virtuelle de la passerelle fonctionne mal, activez une nouvelle passerelle et récupérez vos données pour cette passerelle à l'aide des instructions ci-après.

Récupération après l'arrêt inattendu d'une machine virtuelle

Si votre machine virtuelle 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 obtenir des informations sur le test de la connectivité réseau, consultez Test de la connectivité réseau de la passerelle.

Récupération des données d'un disque de cache défaillant

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.

Récupération de vos données à partir d'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 File Gateway, vous mappez un nouveau système de fichiers de de fichiers au pour Windows File Server qui contient les données que vous souhaitez récupérer.

1. Créez et activez une nouvelle passerelle de fichiers sur un hôte Amazon EC2. Pour de plus amples informations, veuillez consulter Déployer un hôte Amazon EC2 par défaut pour File Gateway FSx.
2. Créez un nouveau système de de fichiers sur la passerelle EC2 que vous avez créée. Pour plus d'informations, voir Créer un système de fichiers FSx pour Windows File Server.

3. Montez votre système de fichiers de de fichiers sur votre client et mappez-le au pour Windows File Server qui contient les données que vous souhaitez récupérer. Pour plus d'informations, voir Monter et utiliser votre partage de fichiers.

Restauration à partir de sauvegardes ou de snapshots directement sur Amazon FSx

Dans certains cas, vous devrez peut-être restaurer les données directement sur votre système de FSx fichiers Amazon, à l'aide d'une sauvegarde ou d'un instantané datant d'une date antérieure. Dans ces cas, il existe un risque de créer un scénario de double écriture entre l'application de sauvegarde et la passerelle de FSx fichiers, ce qui peut entraîner le blocage ou la disparité des fichiers. Pour éviter tout problème lors de la restauration de votre système de FSx fichiers Amazon à partir de sauvegardes ou de snapshots, suivez la procédure suivante.

> **Note**
>
> Les données mises en cache actuellement stockées sur votre passerelle de FSx fichiers ne seront plus valides une fois que vous aurez restauré votre système de FSx fichiers Amazon à partir d'une sauvegarde ou d'un instantané à l'aide de cette procédure.

Pour éviter les problèmes lors de la restauration de votre système de FSx fichiers Amazon à partir de sauvegardes ou de snapshots

1. Détachez le système de FSx fichiers Amazon de la passerelle de FSx fichiers à l'aide de la console Storage Gateway.
2. Restaurez la sauvegarde ou l'instantané directement sur votre système de FSx fichiers Amazon.
3. Rattachez le système de FSx fichiers Amazon à la passerelle de FSx fichiers à l'aide de la console Storage Gateway.

Nettoyez les ressources inutiles

Il est recommandé de nettoyer les ressources de Storage Gateway afin d'éviter des frais imprévus ou inutiles. Par exemple, si vous avez créé une passerelle à titre d'exercice de démonstration ou de test, envisagez de la supprimer ainsi que son dispositif virtuel de votre déploiement. Pour nettoyer les ressources, procédez comme suit.

Pour nettoyer les ressources dont vous n’avez pas besoin

1. Si vous n'avez plus l'intention de continuer à utiliser une passerelle, supprimez-la. Pour de plus amples informations, veuillez consulter Suppression de votre passerelle et suppression des ressources associées.
2. Supprimez la machine virtuelle Storage Gateway de votre hôte sur site. Si vous avez créé votre passerelle sur une instance Amazon EC2, mettez fin à l’instance.

Ressources supplémentaires sur Storage Gateway

Cette section contient les rubriques suivantes, qui fournissent des informations et des ressources supplémentaires relatives à la configuration et à l'utilisation AWS Storage Gateway :

Rubriques

- Configuration de l'hôte- Découvrez comment déployer et configurer un hôte de machine virtuelle pour votre passerelle.
- Utilisation de Storage Gateway avec VMware HA- Découvrez comment configurer Storage Gateway pour qu'il fonctionne avec les fonctionnalités de haute disponibilité de VMware vSphere.
- Obtenir la clé d'activation- Découvrez où trouver la clé d'activation que vous devez fournir lorsque vous déployez une nouvelle passerelle.
- En utilisant Direct Connect- Découvrez comment créer une connexion réseau dédiée entre votre passerelle sur site et le AWS cloud.
- Autorisations Active Directory- Découvrez les autorisations dont votre compte de service doit disposer pour pouvoir rejoindre votre passerelle vers votre domaine Active Directory.
- Obtenir l'adresse IP de votre appliance de passerelle- Découvrez où se trouve l'adresse IP de l'hôte de la machine virtuelle de la passerelle, que vous devez fournir lorsque vous déployez une nouvelle passerelle.
- Comprendre les ressources et les ressources IDs- Découvrez comment AWS identifier les ressources et les sous-ressources créées par Storage Gateway.
- Balisage de vos ressources - Apprenez à utiliser les balises de métadonnées pour classer vos ressources et en faciliter la gestion.
- Composants open source- Découvrez les outils et licences tiers utilisés pour fournir les fonctionnalités de Storage Gateway.
- Quotas- Découvrez les limites et les quotas de File Gateway, y compris les limites minimales et maximales pour les partages de fichiers et les disques de cache locaux.

Déploiement et configuration de l'hôte de la machine virtuelle de passerelle

Les rubriques suivantes fournissent des informations sur la configuration de la plate-forme hôte de machine virtuelle pour votre passerelle.

Rubriques

- Déployer un hôte Amazon EC2 par défaut pour File Gateway FSx
- Déployez un hôte Amazon EC2 personnalisé pour File Gateway FSx
- Modifier les options de métadonnées de l'instance Amazon EC2
- Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux
- Synchroniser l'heure de la machine virtuelle avec VMware celle de l'hôte
- Configuration des adaptateurs réseau pour votre passerelle
- Utilisation de VMware vSphere High Availability avec Storage Gateway

Déployer un hôte Amazon EC2 par défaut pour File Gateway FSx

Cette rubrique décrit les étapes à suivre pour déployer un hôte Amazon EC2 en utilisant les spécifications par défaut.

Vous pouvez déployer et activer une (Amazon FSx File Gateway) sur une instance Amazon Elastic Compute Cloud (Amazon EC2). L'Amazon Machine Image (AMI) AWS Storage Gateway est disponible en tant qu'AMI de la communauté.

> **Note**
>
> La communauté Storage Gateway AMIs est publiée et entièrement prise en charge par AWS. Vous pouvez voir que l'éditeur est AWS un fournisseur vérifié.

1. Pour configurer l'instance Amazon EC2, choisissez Amazon EC2 comme plate-forme hôte dans la section Options de plate-forme du flux de travail. Pour obtenir des instructions sur la configuration de l'instance Amazon EC2, consultez Gateway. FSx
2. Sélectionnez Launch instance pour ouvrir le modèle AWS Storage Gateway AMI dans la console Amazon EC2 et personnaliser des paramètres supplémentaires tels que les types d'instances, les paramètres réseau et Configurer le stockage.
3. Vous pouvez éventuellement sélectionner Utiliser les paramètres par défaut dans la console Storage Gateway pour déployer une instance Amazon EC2 avec la configuration par défaut.

   L'instance Amazon EC2 créée par Utilise la paramètres par défaut possède les spécifications par défaut suivantes :

- Type d’instance : m5.xlarge
- Paramètres réseau
  - Pour VPC, choisissez le VPC dans lequel vous souhaitez faire fonctionner votre instance EC2.
  - Pour Sous-réseau, spécifiez le sous-réseau dans lequel votre instance EC2 doit être lancée.

    > **Note**
    >
    > Les sous-réseaux VPC apparaîtront dans le menu déroulant uniquement si le paramètre d'attribution automatique des adresses IP publiques est activé depuis la console de gestion VPC.

  - Attribuer automatiquement une adresse IP publique : Activé
  - Un groupe de sécurité EC2 est créé et associé à l'instance EC2. Le groupe de sécurité comporte les règles de port entrant suivantes :

    > **Note**
    >
    > Le port 80 doit être ouvert lors de l’activation de la passerelle. Le port est fermé immédiatement après l’activation. Par la suite, votre instance EC2 n’est accessible que via les autres ports du VPC sélectionné.
    > Les partages de fichiers sur votre passerelle ne sont accessibles qu'à partir des hôtes du même VPC que la passerelle. Si les partages de fichiers doivent être accessibles depuis des hôtes extérieurs au VPC, vous devez mettre à jour les règles de groupe de sécurité appropriées.
    > Vous pouvez modifier les groupes de sécurité à tout moment en accédant à la page des détails de l’instance Amazon EC2, en sélectionnant Sécurité, accédant aux Détails du groupe de sécurité et en choisissant l’ID du groupe de sécurité.

Port	Protocole	Protocole du système de fichiers				
80	TCP	Accès HTTP pour l’activation				
137	UDP	NetBIOS				
138	UDP	NetBIOS				
139	TCP, UDP	SMB				
389	TCP	LDAP				
445	TCP	SMB				

- Configurer le stockage

Paramètres par défaut	Volume racine de l’AMI	Cache du volume 2				
Nom du périphérique		’/dev/sdb’				
Size	80 Gio	165 Gio				
Type de volume	gp3	gp3				

Paramètres par défaut	Volume racine de l'AMI	Cache du volume 2
IOPS	3000	3000
Supprimer à la résiliation	Oui	Oui
Encrypted	Non	Non
Débit	125	125

Déployez un hôte Amazon EC2 personnalisé pour File Gateway FSx

Vous pouvez déployer et activer une (Amazon FSx File Gateway) sur une instance Amazon Elastic Compute Cloud (Amazon EC2). L'Amazon Machine Image (AMI) AWS Storage Gateway est disponible en tant qu'AMI de la communauté.

> **Note**
>
> La communauté Storage Gateway AMIs est publiée et entièrement prise en charge par AWS. Vous pouvez voir que l'éditeur est AWS un fournisseur vérifié.
> La Gateway AMIs utilise la convention de dénomination suivante. Le numéro de version ajouté au nom de l'AMI change à chaque publication de version.
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

Pour déployer une instance Amazon EC2 afin d'héberger votre Amazon File Gateway FSx

1. Commencez à configurer une nouvelle passerelle à l'aide de la console Storage Gateway. Pour obtenir des instructions, consultez Configurer une passerelle de FSx fichiers Amazon. Lorsque vous accédez à la section Options de plate-forme, choisissez Amazon EC2 comme plate-forme hôte, puis suivez les étapes ci-dessous pour lancer l'instance Amazon EC2 qui hébergera votre passerelle de fichiers.
2. Choisissez Launch instance pour ouvrir le modèle d' AWS Storage Gateway AMI dans la console Amazon EC2, où vous pouvez configurer des paramètres supplémentaires.

Utilisez Quicklaunch pour lancer l'instance Amazon EC2 avec les paramètres par défaut. Pour plus d'informations sur les spécifications par défaut d'Amazon EC2 Quicklaunch, consultez les spécifications de configuration de Quicklaunch pour Amazon EC2 .

3. Dans le champ Nom, entrez un nom descriptif pour l'instance Amazon EC2. Une fois l'instance déployée, vous pouvez rechercher ce nom pour trouver votre instance sur les pages de liste de la console Amazon EC2.
4. Dans la section Type d'instance, dans Type d'instance, vous pouvez sélectionner la configuration matérielle de votre instance. La configuration matérielle doit répondre à certaines exigences minimales pour prendre en charge votre passerelle. Nous vous recommandons de commencer avec le type d'instance m5.xlarge qui répond aux exigences matérielles minimales pour que votre passerelle fonctionne correctement. Pour de plus amples informations, veuillez consulter Exigences relatives aux types d'instances Amazon EC2.

   Vous pouvez redimensionner votre instance après le lancement si nécessaire. Pour plus d'informations, consultez la section Redimensionnement de votre instance dans le guide de l'utilisateur Amazon EC2.

   > **Note**
   >
   > Certains types d'instances, notamment i3 EC2, utilisent des NVMe disques SSD. Cela peut entraîner des problèmes lorsque vous démarrez ou arrêtez File Gateway ; par exemple, vous pouvez perdre des données du cache. Surveillez la CloudWatch métrique `CachePercentDirty` Amazon et ne démarrez ou arrêtez votre système que lorsque ce paramètre est défini`0`. Pour en savoir plus sur la surveillance des métriques de votre passerelle, consultez la section Mesures et dimensions de Storage Gateway dans la CloudWatch documentation.
5. Dans la section Paire de clés (connexion), pour Nom de la paire de clés - obligatoire, sélectionnez la paire de clés que vous souhaitez utiliser pour vous connecter en toute sécurité à votre instance. Vous pouvez créer une nouvelle paire de clés si nécessaire. Pour obtenir plus d'informations, consultez la section Créer une paire de clés dans le Guide de l'utilisateur d'Amazon Elastic Compute Cloud pour les instances Linux.
6. Dans la section Paramètres réseau, passez en revue les paramètres préconfigurés et choisissez Modifier pour modifier les champs suivants :

a. Pour VPC - obligatoire, choisissez le VPC sur lequel vous souhaitez lancer votre instance Amazon EC2. Pour plus d'informations, consultez Fonctionnement d'Amazon VPC in the Guide de l'utilisateur Amazon Virtual Private Cloud.

b. (Facultatif) Pour Sous-réseau, choisissez le sous-réseau sur lequel vous souhaitez lancer votre instance Amazon EC2.

c. Pour Auto-assign Public IP (Attribuer automatiquement l'adresse IP publique), choisissez Enable (Activer).

7. Dans la sous-section Pare-feu (groupes de sécurité), vérifiez les paramètres préconfigurés. Vous pouvez modifier le nom et la description par défaut du nouveau groupe de sécurité à créer pour votre instance Amazon EC2 si vous le souhaitez, ou choisir d'appliquer les règles de pare-feu d'un groupe de sécurité existant à la place.

8. Dans la sous-section Règles des groupes de sécurité pour le trafic entrant, ajoutez des règles de pare-feu pour ouvrir les ports que les clients utiliseront pour se connecter à votre instance. Pour plus d'informations sur les ports requis pour (Amazon FSx File Gateway), consultez la section aux ports. Pour plus d'informations sur l'ajout de règles de pare-feu, consultez Règles des groupes de sécurité dans le Guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Linux.

> **Note**
>
> Amazon FSx File Gateway nécessite que le port TCP 80 soit ouvert pour le trafic entrant et un accès HTTP unique lors de l'activation de la passerelle. Après activation, vous pouvez fermer ce port.
> En outre, vous devez ouvrir le port TCP 445 pour l'accès SMB, le port UDP 137 pour l'accès NetBIOS, le port UDP 138 pour l'accès NetBIOS et le port TCP 389 pour l'accès LDAP.

9. Dans la sous-section Configuration réseau avancée, passez en revue les paramètres préconfigurés et apportez les modifications si nécessaire.

10. Dans la section Configurer le stockage, choisissez Ajouter un nouveau volume pour ajouter du stockage à votre instance de passerelle.

> **Important**
>
> Vous devez ajouter au moins un volume Amazon EBS d'une capacité d'au moins 150 GiB pour le stockage en cache en plus du volume racine préconfiguré. Pour des

performances accrues, nous recommandons d'allouer plusieurs volumes EBS pour le stockage en cache, d'au moins 150 Gio chacun.

11. Dans la sous-section Détails avancés, vérifiez les paramètres préconfigurés et apportez les modifications si nécessaire.
12. Choisissez Lancez l'instance pour lancer votre nouvelle instance de passerelle Amazon EC2 avec les paramètres configurés.
13. Pour vérifier que votre nouvelle instance a été lancée avec succès, accédez à la page Instances de la console Amazon EC2 et recherchez votre nouvelle instance par son nom. Assurez-vous que l'État de l'instance affiche En cours d'exécution avec une coche verte et que le Contrôle de statut est terminé et qu'une coche verte apparaît.
14. Sélectionnez votre instance sur la page de détails. Copiez l'adresse IP publique depuis la section Résumé de l'instance, puis revenez à la page Configurer la passerelle dans la console Storage Gateway pour reprendre la configuration de votre (Amazon FSx File Gateway).

Vous pouvez déterminer l'ID AMI à utiliser pour lancer une passerelle de fichiers à l'aide de la console Storage Gateway ou en interrogeant le magasin de AWS Systems Manager paramètres.

Pour déterminer l'ID AMI, effectuez l'une des opérations suivantes :

- Commencez à configurer une nouvelle passerelle à l'aide de la console Storage Gateway. Pour obtenir des instructions, consultez Configurer une passerelle de FSx fichiers Amazon. Lorsque vous accédez à la section Options de plate-forme, choisissez Amazon EC2 comme plate-forme hôte, puis choisissez Launch instance pour ouvrir le modèle d' AWS Storage Gateway AMI dans la console Amazon EC2.

  Vous êtes redirigé vers la page AMI de la communauté EC2, où vous pouvez voir l'ID de l'AMI de votre AWS région dans l'URL.
- Interrogez Systems Manager Parameter Store. Vous pouvez utiliser l'API AWS CLI ou Storage Gateway pour interroger le paramètre public de Systems Manager sous l'espace de noms `/aws/service/storagegateway/ami/FILE_FSX_SMB/latest`. Par exemple, l'utilisation de la commande CLI suivante renvoie l'ID de l'AMI actuelle dans celui Région AWS que vous spécifiez.

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  FILE_FSX_SMB/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": 18,
         "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_FSX_SMB/latest",
         "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
        "Value": "ami-033d1edba5606cffb"
    }
}
```

Modifier les options de métadonnées de l'instance Amazon EC2

Le service de métadonnées d'instance (IMDS) est un composant sur instance qui fournit un accès sécurisé aux métadonnées des instances Amazon EC2. Une instance peut être configurée pour accepter les demandes de métadonnées entrantes qui utilisent IMDS version 1 (IMDSv1) ou pour exiger que toutes les demandes de métadonnées utilisent IMDS version 2 ()IMDSv2. IMDSv2 utilise des requêtes orientées session et atténue plusieurs types de vulnérabilités susceptibles d'être utilisées pour tenter d'accéder à l'IMDS. Pour plus d'informations sur IMDSv2 le fonctionnement de la version 2 du service de métadonnées d'instance, consultez le guide de l'utilisateur d'Amazon Elastic Compute Cloud.

Nous vous recommandons d'avoir besoin d'IMDSv2 pour toutes les instances Amazon EC2 hébergeant Storage Gateway. IMDSv2 est obligatoire par défaut sur toutes les instances de passerelle récemment lancées. Si vous avez des instances existantes qui sont toujours configurées pour accepter les demandes de IMDSv1 métadonnées, consultez la section Exiger l'utilisation de IMDSv2 dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud pour obtenir des instructions sur la modification des options de métadonnées de votre instance afin d'exiger l'utilisation de IMDSv2. L'application de cette modification ne nécessite pas de redémarrage de l'instance.

Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux

Pour une passerelle déployée sur VMware ESXi, il suffit de définir l'heure de l'hôte de l'hyperviseur et de synchroniser l'heure de la machine virtuelle avec celle de l'hôte pour éviter toute dérive temporelle. Pour de plus amples informations, veuillez consulter Synchroniser l'heure de la machine virtuelle

avec VMware celle de l'hôte. Pour une passerelle déployée sur Microsoft Hyper-V ou Linux KVM, nous vous recommandons de vérifier régulièrement l'heure de la machine virtuelle en suivant la procédure décrite ci-dessous.

Pour afficher et synchroniser l'heure d'une machine virtuelle de passerelle hyperviseur avec un serveur NTP (Network Time Protocol)

1. Connectez-vous à la console locale de la passerelle :

   - 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 les machines virtuelles basées sur le noyau Linux (KVM), consultez. Accès à la console locale de la passerelle avec Linux KVM
2. Sur l'écran du menu principal de configuration de Storage Gateway, entrez le chiffre correspondant pour sélectionner System Time Management.
3. Sur l'écran du menu Gestion du temps du système, entrez le chiffre correspondant pour sélectionner Afficher et synchroniser l'heure du système.

   La console locale de la passerelle affiche l'heure actuelle du système et la compare à l'heure indiquée par le serveur NTP, puis indique l'écart exact entre les deux heures en secondes.
4. Si l'écart de temps est supérieur à 60 secondes, entrez **y** pour synchroniser l'heure du système avec l'heure NTP. Sinon, entrez **n**.

   La synchronisation de l'heure peut prendre quelques instants.

Synchroniser l'heure de la machine virtuelle avec VMware 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, cliquez avec le bouton droit sur le nom de votre machine virtuelle de passerelle dans le panneau situé sur le côté gauche de la fenêtre de l'application pour ouvrir le menu contextuel de la machine virtuelle, puis choisissez Modifier les paramètres.

      La boîte de dialogue Propriétés de la machine virtuelle s’ouvre.

   b. Choisissez l'onglet Options, puis sélectionnez VMware Outils dans la liste des options.

   c. Cochez l'option Synchroniser l'heure du client avec l'hôte dans la section Avancé sur le côté droit de la boîte de dialogue Propriétés de la machine virtuelle, puis cliquez sur 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 hôte vSphere dans le panneau 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. Sous Date et heure, définissez la date et l'heure de votre hôte vSphere.

   d. Configurez l’hôte afin de synchroniser son heure automatiquement sur un serveur NTP.

      i. Choisissez Options dans la boîte de dialogue de configuration temporelle, puis dans la boîte de dialogue Options du démon NTP (ntpad), choisissez Paramètres NTP dans le panneau 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 l'utiliser `pool.ntp.org` comme nom de domaine.

iv. Dans la boîte de dialogue des options du démon NTP (ntpad), choisissez Général dans le panneau de gauche.

v. Sous Commandes de service, choisissez Démarrer pour démarrer 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.

Configuration des adaptateurs réseau pour votre passerelle

Storage Gateway utilise un seul adaptateur réseau VMXNET3 (10 GbE) par défaut, mais vous pouvez configurer votre passerelle pour qu'elle utilise plusieurs adaptateurs réseau afin que plusieurs adresses IP puissent y accéder. Cela peut être utile dans les cas suivants :

- Maximisation du débit : vous souhaiterez peut-être optimiser le débit vers une passerelle lorsque les adaptateurs réseau constituent un goulot d'étranglement.
- Séparation de l'application : vous devrez peut-être distinguer la façon dont vos applications écrivent sur les volumes d'une passerelle. Par exemple, vous pouvez choisir d'avoir une application de stockage critique qui utilise exclusivement une carte donnée définie pour votre passerelle.
- Contraintes réseau : votre environnement applicatif peut exiger que vous conserviez vos partages de fichiers et les initiateurs qui s'y connectent sur un réseau isolé. Ce réseau est différent du réseau par lequel la passerelle communique avec AWS.

Dans un cas d'utilisation typique de plusieurs adaptateurs, un adaptateur est configuré comme route par laquelle la passerelle communique AWS (c'est-à-dire comme passerelle par défaut). À l'exception de cet adaptateur, les initiateurs doivent se trouver dans le même sous-réseau que l'adaptateur qui contient les partages de fichiers auxquels ils se connectent. Sinon, la communication avec les cibles prévues risque de ne pas être possible. Si une cible est configurée sur le même adaptateur que celui

utilisé pour la communication AWS, le trafic de partage de fichiers pour cette cible et le AWS trafic passent par le même adaptateur.

Dans certains cas, vous pouvez configurer un adaptateur pour qu'il se connecte à la console Storage Gateway, puis ajouter un second adaptateur. Dans ce cas, Storage Gateway configure automatiquement la table de routage pour utiliser le second adaptateur comme route préférée. Pour obtenir des instructions sur la configuration de plusieurs adaptateurs, consultez les rubriques suivantes :

Rubriques

- Configuration de votre passerelle pour plusieurs NICs sur un VMware ESXi hôte
- Configuration de votre passerelle pour plusieurs NICs dans Microsoft Hyper-V Host

Configuration de votre passerelle pour plusieurs NICs sur un VMware ESXi hôte

La procédure suivante suppose qu'un adaptateur réseau est déjà défini sur votre machine virtuelle de passerelle et décrit comment ajouter un adaptateur VMware ESXi.

Pour configurer votre passerelle afin d'utiliser un adaptateur réseau supplémentaire dans l' VMware ESXi hôte

1. Arrêtez la passerelle.
2. Dans le client VMware vSphere, sélectionnez votre machine virtuelle de 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 la machine virtuelle, 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 l'adaptateur VMXNET3 réseau avec Storage Gateway. Pour plus d'informations sur les types d'adaptateurs susceptibles d'apparaître dans la

liste des adaptateurs, consultez la section Types d'adaptateurs réseau dans la ESXi documentation de 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. La fenêtre Adresses IP de la machine virtuelle 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.

7. Dans la console Storage Gateway, activez la passerelle.
8. Dans le volet Navigation de la console Storage Gateway, sélectionnez Passerelles, puis 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 locales communes aux VMware hôtes Hyper-V et KVM, voir Exécution de tâches sur la console locale de la machine virtuelle

Configuration de votre passerelle pour plusieurs NICs dans Microsoft Hyper-V Host

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. Dans la console Storage Gateway, désactivez la passerelle.
2. Dans le gestionnaire Microsoft Hyper-V, sélectionnez votre machine virtuelle de passerelle dans le panneau Machines virtuelles.
3. Si la machine virtuelle de passerelle n'est pas déjà désactivée, cliquez avec le bouton droit sur le nom de la machine virtuelle pour ouvrir le menu contextuel, puis choisissez Désactiver.
4. Cliquez avec le bouton droit sur le nom de la machine virtuelle de passerelle pour ouvrir le menu contextuel, puis sélectionnez Paramètres.

5. Dans la boîte de dialogue Paramètres, sous Matériel, choisissez Ajouter du matériel.
6. Dans le panneau Ajouter du matériel sur le côté droit de la boîte de dialogue Paramètres, choisissez Adaptateur réseau, puis choisissez Ajouter pour ajouter un périphérique.
7. Configurez la carte réseau, puis choisissez Appliquer pour appliquer les paramètres.
8. Dans la boîte de dialogue Paramètres, sous Matériel, vérifiez que le nouvel adaptateur réseau a été ajouté à la liste du matériel, puis cliquez sur OK.
9. Activez la passerelle à l'aide de la console Storage Gateway.
10. Dans le panneau de navigation de la console Storage Gateway, choisissez Gateways, puis sélectionnez la passerelle à laquelle vous avez ajouté l'adaptateur. Vérifiez qu'une deuxième adresse IP est répertoriée dans l'onglet Détails.

Pour plus d'informations sur les tâches de console locales communes aux VMware hôtes Hyper-V et KVM, voir Exécution de tâches sur la console locale de la machine virtuelle

Utilisation de VMware vSphere High Availability avec Storage Gateway

Storage Gateway assure une haute disponibilité VMware grâce à un ensemble de contrôles de santé au niveau des applications intégrés à VMware vSphere High Availability (HA). VMware 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 VMware environnement sur site ou dans un VMware cloud AWS se rétablit automatiquement après la plupart des interruptions de service. Cette récupération s'effectue généralement en moins de 60 secondes, sans perte de données.

> **Note**
>
> Nous vous recommandons de procéder comme suit si vous déployez Storage Gateway dans un cluster VMware HA :
>
> - Déployez le package téléchargeable VMware ESX .ova qui contient la machine virtuelle Storage Gateway sur un seul hôte d'un cluster.
> - Lors du déploiement du package .ova, sélectionnez un magasin de données qui n'est pas local sur 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.

- Dans le cas du clustering, si vous déployez le package .ova sur le cluster, sélectionnez un hôte lorsque vous y êtes invité. Vous pouvez aussi déployer directement sur l'hôte d'un cluster.

Les rubriques suivantes décrivent comment déployer Storage Gateway dans un cluster VMware HA :

Rubriques

- Configuration de votre cluster vSphere HA VMware
- Configurez votre type de passerelle
- Déployer la passerelle
- (Facultatif) Ajoutez des options de remplacement pour les autres utilisateurs VMs de votre cluster
- Activer votre passerelle
- Testez votre configuration VMware de haute disponibilité

Configuration de votre cluster vSphere HA VMware

Tout d'abord, si vous n'avez pas encore créé de VMware cluster, créez-en un. Pour plus d'informations sur la création d'un VMware cluster, consultez la section Créer un cluster vSphere HA dans la VMware documentation.

Configurez ensuite votre VMware cluster pour qu'il fonctionne avec Storage Gateway.

Pour configurer votre VMware cluster

1. Sur la page 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 valeurs suivantes pour chaque option :

   - Réponse en cas de défaillance de l'hôte : redémarrage VMs
   - Réponse en cas d'isolation de l'hôte : arrêt et redémarrage VMs
   - Datastore with PDL (Magasin de données avec PDL) : Disabled (Désactivé)
   - Datastore with APD (Magasin de données avec APD) : Disabled (Désactivé)

- VM Monitoring (Surveillance des MV) : VM and Application Monitoring (Surveillance des machines virtuelles et des applications)

2. Affinez la sensibilité du cluster en ajustant les valeurs suivantes :

   - Intervalle d'échec : après cet intervalle, la machine virtuelle est redémarrée si aucune pulsation de machine virtuelle n'est reçue.
   - Temps de disponibilité minimum : le cluster attend le temps indiqué après le démarrage d'une machine virtuelle pour commencer à surveiller les pulsations des outils de la machine virtuelle.
   - Nombre maximum de réinitialisations par machine virtuelle : le cluster redémarre la machine virtuelle ce nombre de fois au maximum dans la fenêtre temporelle pour le maximum de réinitialisations.
   - Fenêtre temporelle pour le maximum de réinitialisations : fenêtre de temps pendant laquelle compter le nombre 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** heur

Si d'autres sont VMs en cours d'exécution sur le cluster, vous souhaiterez peut-être 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) Ajoutez des options de remplacement pour les autres utilisateurs VMs de votre cluster.

Configurez votre type de passerelle

Utilisez la procédure suivante pour configurer la passerelle

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 — Création et activation d'un Amazon FSx File Gateway

Déployer la passerelle

Dans votre cluster configuré, déployez l'image .ova sur l'un des hôtes du cluster. Pour obtenir des instructions, consultez la section Déployer un modèle OVF ou OVA dans la documentation en ligne de VMware vSphere.

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) Ajoutez des options de remplacement pour les autres utilisateurs VMs de votre cluster

Si d'autres applications sont VMs en cours d'exécution sur votre cluster, vous souhaiterez peut-être définir les valeurs du cluster spécifiquement pour chaque machine virtuelle. Pour obtenir des instructions, consultez la section Personnaliser une machine virtuelle individuelle dans la documentation en ligne de VMware vSphere.

Pour ajouter des options de remplacement pour les autres membres VMs de votre cluster

1. Sur la page Résumé de VMware vSphere, choisissez votre cluster pour ouvrir la page du cluster, puis choisissez 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.

   Définissez les valeurs suivantes pour chaque option sous vSphere HA - VM Monitoring :

   - Surveillance des machines virtuelles : remplacement activé - Surveillance des machines virtuelles et des applications
   - Sensibilité de surveillance des machines virtuelles : dérogation activée - Surveillance des machines virtuelles et des applications
   - Surveillance des machines virtuelles : personnalisée
   - Intervalle de défaillance : **30** secondes
   - Temps de disponibilité minimum : secondes **120**

- Maximum per-VM resets (Nombre maximum de réinitialisations par machine virtuelle) : **5**
- Période maximale de réinitialisation : en quelques heures **1**

Activer votre passerelle

Une fois le fichier .ova déployé dans votre VMware environnement, activez votre passerelle à l'aide de la console Storage Gateway. Pour obtenir des instructions, et activer votre Amazon FSx File Gateway.

Testez votre configuration VMware de haute disponibilité

Après avoir activé votre passerelle, testez votre configuration.

Pour tester votre configuration VMware HA

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Gateways, puis choisissez la passerelle que vous souhaitez tester pour VMware HA.
3. Pour Actions, choisissez Verify VMware HA.
4. Dans la zone Vérifier la configuration de VMware haute disponibilité qui apparaît, cliquez sur OK.

   > **Note**
   >
   > Le test de votre configuration VMware HA redémarre la machine virtuelle de votre passerelle et interrompt la connectivité à votre passerelle. Le test peut prendre quelques minutes.

   Si le test réussit, le statut Verified (Vérifié) apparaît dans l'onglet Détails de la passerelle sur la console.
5. Choisissez Exit (Quitter).

Vous pouvez trouver des informations sur les événements VMware HA dans les groupes de CloudWatch journaux Amazon. Pour de plus amples informations, veuillez consulter Obtenir les journaux d'état de File Gateway avec des CloudWatch groupes de journaux.

Obtention d’une clé d’activation pour votre passerelle

Pour recevoir une clé d’activation pour votre passerelle, envoyez une demande Web à la machine virtuelle (VM) de passerelle. La machine virtuelle renvoie une redirection contenant la clé d’activation, qui est transmise comme l’un des paramètres de l’action d’API `ActivateGateway` afin de spécifier la configuration de votre passerelle. Pour plus d'informations, consultez ActivateGatewayle manuel Storage Gateway API Reference.

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

La demande que vous envoyez à la machine virtuelle de passerelle inclut la 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`*. Le résultat de cette requête renvoie à la fois la région d’activation et la clé.

L’URL inclut également `vpcEndpoint`, l’ID de point de terminaison de VPC pour les passerelles qui se connectent à l’aide du type de point de terminaison de VPC.

> **Note**
>
> L'appliance matérielle AWS Storage Gateway, les modèles d'image de machine virtuelle et les Amazon Machine Images (AMI) Amazon EC2 sont préconfigurés avec les services HTTP nécessaires pour recevoir et répondre aux requêtes Web décrites sur cette page. Il n’est ni obligatoire ni recommandé d’installer des services supplémentaires sur votre passerelle.

Rubriques

- Linux (curl)
- Linux (bash/zsh)
- Microsoft Windows PowerShell
- Utilisation de votre console locale

Linux (curl)

Les exemples suivants vous montrent comment obtenir une clé d'activation à l'aide de Linux (curl).

> **Note**
>
> Remplacez les variables mis en évidence par des valeurs réelles pour votre passerelle. Les valeurs possibles sont les suivantes :
>
> - *gateway_ip_address*- L' IPv4 adresse de votre passerelle, par exemple `172.31.29.201`
> - *gateway_type*- Le type de passerelle que vous souhaitez activer, tel que `STOREDCACHED`,`VTL`,`FILE_S3`, ou`FILE_FSX_SMB`.
> - *region_code*- La région dans laquelle vous souhaitez activer votre passerelle. Voir les Points de terminaison régionaux dans le Guide de référence général AWS . Si ce paramètre n'est pas spécifié, ou si la valeur fournie est mal orthographiée ou ne correspond pas à une région valide, la commande utilisera par défaut la `us-east-1` région.
> - *vpc_endpoint*- Le nom du point de terminaison VPC de votre passerelle, par exemple. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Pour obtenir la clé d'activation d'un point de terminaison public :

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Pour obtenir la clé d'activation d'un point de terminaison de VPC :

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

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 "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); 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 récupérer 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,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Utilisation de votre console locale

Les comment utiliser votre console locale pour générer et afficher une clé d'activation.

Pour obtenir une clé d’activation pour votre passerelle à l’aide de votre console locale

1. Connectez-vous à votre console locale en tant qu'administrateur.
2. Après vous être connecté et avoir vu le menu principal Activation de l’appliance AWS - Configuration, sélectionnez `0` pour choisir Obtenir la clé d’activation.
3. Sélectionnez Storage Gateway pour l’option de la famille de passerelle.
4. Lorsque vous y êtes invité, entrez l' Région AWS endroit où vous souhaitez activer votre passerelle.
5. Saisissez 1 pour Public ou 2 pour Point de terminaison VPC en tant que type de réseau.
6. Saisissez 1 Standard ou 2 FIPS (Federal Information Processing Standard) en tant que type de point de terminaison.

Utilisation Direct Connect avec Storage Gateway

Direct Connect relie votre réseau interne au cloud Amazon Web Services. Direct Connect Grâce à Storage Gateway, vous pouvez créer une connexion répondant aux besoins de charge de travail à haut débit, en fournissant une connexion réseau dédiée entre votre passerelle sur site et. AWS

Storage Gateway utilise des points de terminaison publics. Une fois la Direct Connect connexion établie, vous pouvez créer une interface virtuelle publique pour permettre au trafic d'être acheminé vers les 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 que l' Direct Connect emplacement, ou dans une autre AWS région.

L'illustration suivante montre un exemple de Direct Connect fonctionnement avec Storage Gateway. architecture réseau montrant Storage Gateway connecté au cloud à l'aide d' AWS une connexion directe.

La procédure suivante suppose que vous avez créé une passerelle opérationnelle.

À utiliser Direct Connect avec Storage Gateway

1. Créez et établissez une 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 Mise en route avec Direct Connect dans le Guide de l'utilisateur Direct Connect .
2. Connectez votre appliance Storage Gateway sur site au Direct Connect routeur.
3. Créez une interface virtuelle publique et configurez votre routeur sur site en conséquence. Pour plus d'informations, consultez Création d'une interface virtuelle dans le Guide de l'utilisateur Direct Connect .

Pour plus de détails Direct Connect, voir Qu'est-ce que c'est Direct Connect ? dans le guide de Direct Connect l'utilisateur.

Exigences relatives aux autorisations relatives aux comptes de service Active Directory

Si vous envisagez d'utiliser Microsoft Active Directory pour fournir un accès authentifié aux systèmes de sur votre système de fichiers AWS Storage Gateway, vous devez vous assurer que vous disposez d'un compte de service Active Directory et que le compte de service dispose des autorisations déléguées pour associer des ordinateurs à votre domaine. Un compte de service est un compte utilisateur Active Directory auquel l'autorisation d'effectuer certaines tâches a été déléguée. Vous fournissez le nom d'utilisateur et le mot de passe de ce compte lorsque vous connectez un Storage Gateway à votre domaine Active Directory.

Les autorisations suivantes doivent être déléguées au compte de service Active Directory dans l'unité d'organisation à laquelle vous rejoignez votre passerelle :

- Possibilité de créer et de supprimer des objets informatiques
- Possibilité de réinitialiser les mots de passe
- Possibilité de modifier les autorisations
- Possibilité d'empêcher les comptes de lire et d'écrire des données
- Aptitude validée à lire et à écrire les restrictions du compte
- Capacité validée d'écrire dans le nom du principal de service
- Capacité validée d'écrire sur le nom d'hôte DNS

Il s'agit de l'ensemble minimal d'autorisations requises pour joindre des objets informatiques à votre Active Directory. Pour plus d'informations, consultez la rubrique de documentation de Microsoft Windows Server Erreur : l'accès est refusé lorsque des utilisateurs non administrateurs auxquels le contrôle a été délégué tentent de joindre des ordinateurs à un contrôleur de domaine.

Obtenir l'adresse IP de votre appliance de 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 l'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 :

- VMware hôte : Accès à la console locale de Gateway 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, veuillez consulter .

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 ensuite à la console Storage Gateway et tapez l'adresse IP dans la console.

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 ensuite à la console Storage Gateway et tapez l'adresse IP Elastic dans la console.

Comprendre les ressources et les ressources de Storage Gateway IDs

Dans Storage Gateway, la ressource principale est une passerelle, mais les autres types de ressources sont le partage de fichiers. Les partages de fichiers sont appelés sous-ressources et n'existent que s'ils sont associés à une passerelle.

Ces ressources et sous-ressources sont associées à des noms de ressources Amazon uniques (ARNs), comme indiqué dans ce tableau.

Type de ressource	Format ARN
ARN de passerelle	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*

Type de ressource	Format ARN
ARN de partage de fichiers	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

Travailler avec Resource IDs

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.

Les ID de ressources 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 `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.

> **Important**
>
> IDs pour les volumes Storage Gateway et les instantanés Amazon EBS créés à partir de volumes Gateway 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 partir d'avril 2016, vous pourrez les utiliser plus longtemps IDs afin de tester vos systèmes avec le nouveau format. Pour plus d'informations, consultez Longer EC2 and EBS Resource. IDs
> 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/vol-1122AABBCCDDEEFFG`.
> Un ID d'instantané avec le format d'ID plus long ressemble à ceci :`snap-78e226633445566ee`.
> Pour plus d'informations, consultez Announcement : Heads-up — Longer Storage Gateway volume and snapshot à IDs paraître en 2016.

Balisage des ressources 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 File Gateway, vous pouvez utiliser des balises pour 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 d'étiquette 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 par AWS .
- Les caractères valides pour la propriété de clé sont les lettres UTF-8, les chiffres, les espaces et caractères spéciaux + - = . _ : / et @.

Utilisation des tags

Vous pouvez utiliser des balises avec la console Storage Gateway, l'API Storage Gateway ou l'interface de ligne de commande (CLI) de 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 à la https://console.aws.amazon.com/storagegateway/maison.
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 à la https://console.aws.amazon.com/storagegateway/maison.
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 en forme de crayon à côté de l'étiquette que vous souhaitez modifier, puis modifiez-la.
5. Lorsque vous avez fini de modifier la balise, choisissez Enregistrer.

Pour supprimer une balise

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
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.

Utilisation de composants open source pour AWS Storage Gateway

Cette section décrit les outils et licences tiers dont nous dépendons pour fournir des AWS Storage Gateway fonctionnalités.

Rubriques

- Composants open source pour Storage Gateway
- Composants open source pour Amazon FSx File Gateway

Composants open source pour Storage Gateway

Plusieurs outils et licences tiers sont utilisés pour fournir des fonctionnalités pour Volume Gateway, Tape Gateway et Amazon S3 File Gateway.

Utilisez les liens suivants pour télécharger le code source de certains composants logiciels libres inclus dans le AWS Storage Gateway logiciel :

- Pour les appliances Storage Gateway déployées sur VMware ESXi : sources.tar
- Pour les appliances Storage Gateway déployées sur Microsoft Hyper-V : sources_hyperv.tar
- Pour les appliances Storage Gateway déployées sur une machine virtuelle basée sur le noyau Linux (KVM) : sources_KVM.tar

Ce produit comprend un logiciel développé par OpenSSL Project à utiliser dans la boîte à outils OpenSSL (http://www.openssl.org/). Pour connaître les licences pertinentes pour tous les outils tiers dépendants, consultez Licences tierces.

Composants open source pour Amazon FSx File Gateway

Plusieurs outils et licences tiers sont utilisés pour fournir les fonctionnalités d'Amazon FSx File Gateway (FSx File Gateway).

Utilisez les liens suivants pour télécharger le code source de certains composants logiciels open source inclus dans FSx le logiciel File Gateway :

- Pour la version 2021-07-07 d'Amazon FSx File Gateway : -open-source.tgz sgw-file-fsx-smb
- Pour la version 2021-04-06 d'Amazon FSx File Gateway : -20210406-open-source.tgz sgw-file-fsx-smb

Ce produit comprend un logiciel développé par OpenSSL Project à utiliser dans la boîte à outils OpenSSL (http://www.openssl.org/). Pour connaître les licences pertinentes pour tous les outils tiers dépendants, consultez les liens suivants :

- Pour la version 2021-07-07 d'Amazon FSx File Gateway : licence tierce.
- Pour la version 2021-04-06 d'Amazon FSx File Gateway : licence tierce.

Limites et quotas pour (Amazon FSx File Gateway)

Quotas pour les systèmes FSx de fichiers Amazon

Le tableau suivant répertorie les limites minimales et maximales ainsi que les quotas pour les systèmes de FSx fichiers Amazon.

Ressource	Limite par système de FSx fichiers Amazon
Nombre maximum de tags	50 étiquettes
Durée de conservation maximale pour les sauvegardes automatisées	90 jours

Ressource	Limite par système de FSx fichiers Amazon
Nombre maximum de demandes de copie de sauvegarde en cours vers une seule région de destination par compte.	5 demandes
Capacité de stockage minimale pour les systèmes de fichiers SSD	32 GiO
Capacité de stockage minimale pour les systèmes de fichiers HDD	2 000 GiB
Capacité de stockage maximale pour les systèmes de fichiers SSD et HDD	64 Tio
Capacité de débit minimale	8 MBps
Capacité de débit maximale	2 048 MBps
Nombre maximum de partages de FSx fichiers Amazon	100 000

Tailles des disques locaux recommandées pour votre passerelle

Le tableau suivant recommande les tailles de stockage sur disque local pour chaque AWS Storage Gateway élément de votre déploiement.

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

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

Lorsque vous ajoutez du cache à une passerelle de fichiers FSx existante, il est important de créer de nouveaux disques sur votre hôte virtuel (hyperviseur ou instance Amazon EC2). Ne modifiez pas la taille des disques existants s'ils ont déjà été alloués en tant que cache.

Référence d’API pour Storage Gateway

Outre l'utilisation de la console, vous pouvez utiliser l' AWS Storage Gateway API pour configurer et gérer vos passerelles par programmation. Cette section décrit les AWS Storage Gateway opérations, la signature des demandes d'authentification et le traitement des erreurs. Pour obtenir des informations sur les régions et les points de terminaison disponibles pour Storage Gateway, consultez Points de terminaison et quotas AWS Storage Gateway dans le document Références générales AWS.

> **Note**
>
> Vous pouvez également l'utiliser AWS SDKs lorsque vous développez des applications avec Storage Gateway. AWS SDKs Pour Java, .NET et PHP, ils encapsulent l'API Storage Gateway sous-jacente, simplifiant ainsi vos tâches de programmation. Pour obtenir des informations sur le téléchargement des bibliothèques de kits SDK, consultez Exemples de bibliothèques de codes.

Rubriques

- AWS Storage Gateway En-têtes de demande obligatoires
- Signature des requêtes
- Réponses d’erreur
- Actions de l'API Storage Gateway

AWS Storage Gateway En-têtes de demande obligatoires

Cette section décrit les en-têtes obligatoires que vous devez envoyer avec chaque requête POST à AWS Storage Gateway. Vous incluez les en-têtes HTTP pour identifier les informations clés relatives à la demande, y compris l’opération que vous souhaitez appeler, la date de la demande et les informations correspondant à votre autorisation en tant qu’expéditeur de la demande. Les en-têtes ne sont pas sensibles à la casse et leur ordre n’est pas important.

L'exemple suivant montre les en-têtes utilisés dans l'ActivateGatewayopération.

```
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
```

Les en-têtes suivants doivent être inclus dans vos requêtes POST à AWS Storage Gateway. Les en-têtes présentés ci-dessous qui commencent par « x-amz » sont AWS des en-têtes spécifiques. Tous les autres en-têtes répertoriés sont des en-têtes courants utilisés dans les transactions HTTP.

En-tête	Description
`Authorization`	L'en-tête d'autorisation contient plusieurs informations sur la demande qui permettent de AWS Storage Gateway déterminer si la demande est une action valide pour le demandeur. Le format de cet en-tête est le suivant (sauts de ligne ajoutés pour faciliter la lecture) : `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` Dans la syntaxe précédente, vous spécifiez l'année YourAccessKey, le mois et le jour (yyyymmdd), la région et le. CalculatedSignature Le format de l'en-tête d'autorisation est dicté par les exigences du processus de signature AWS V4. Les détails de la signature sont détaillés dans la rubrique Signature des requêtes.
`Content-Type`	À utiliser `application/x-amz-json-1.1` comme type de contenu pour toutes les demandes adressées à AWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`

En-tête	Description
`Host`	Utilisez l'en-tête de l'hôte pour spécifier le AWS Storage Gateway point de terminaison auquel vous envoyez votre demande. Par exemple, `storagegateway.us-east-2.amazonaws.com` correspond au point de terminaison de la région USA Est (Ohio). Pour plus d'informations sur les points de terminaison disponibles pour AWS Storage Gateway, consultez la section AWS Storage Gateway Points de terminaison et quotas dans le. Références générales AWS `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	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`.) Lorsqu'un `x-amz-date` en-tête est présent, il AWS Storage Gateway ignore tout `Date` en-tête lors de l'authentification de la demande. Le `x-amz-date` format doit être ISO8601 Basic au format YYYYMMDD'T'HHMMSS'Z'. Si l'`x-amz-date` en-tête `Date` et sont utilisés à la fois, le format de l'en-tête Date ne doit pas nécessairement l'être ISO8601. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	Cet en-tête spécifie la version de l'API et l'opération que vous demandez. Les valeurs d'en-tête cibles sont formées en concaténant la version de l'API avec le nom de l'API et ont le format suivant. `x-amz-target: StorageGateway_ APIversion .operationName` La valeur OperationName (par exemple « ActivateGateway ») se trouve dans la liste des API,. Référence d'API pour Storage Gateway

Signature des requêtes

Storage Gateway exige l'authentification de chaque demande que vous envoyez en la signant. 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 vous avez utilisées pour signer la demande. Si la signature obtenue correspond à la signature de la demande, Storage Gateway traite la demande. Sinon, la demande est rejetée.

Storage Gateway prend en charge l'authentification à l'aide de AWS Signature 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 la même forme 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 : créer 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 de portée des informations d'identification pour créer une série de codes d'authentification de message basés sur le hachage ()HMACs.

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.

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 demande (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 demande 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. Cela est dû au fait qu'il n'existe aucun paramètre de requête pour cette API (ni pour aucune autre solution Storage Gateway APIs).

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 demande canonique issue de la tâche 1.

Pour Tâche 3 : créer 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 AWS Storage Gateway les erreurs. 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 demande. Toutefois, le code d'erreur d'opération n'`ActivationKeyInvalid`est renvoyé que pour l'ActivateGatewayAPI.

En fonction du type d'erreur, Storage Gateway peut retourner simplement 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 AWS Storage Gateway d'API. Lorsqu'une AWS Storage Gateway opération renvoie une réponse d'erreur, le corps de la réponse contient l'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
`IncompleteSignatureException`	La signature spécifiée est incomplète.	400 Requête erronée
`InternalFailure`	Le traitement de la demande a échoué en raison d'une erreur inconnue, d'une exception ou d'un échec.	500 Erreur de serveur interne
`InternalServerError`	Un des messages de code d'erreur d'opération Codes d'erreur d'opération.	500 Erreur de serveur interne
`InvalidAction`	L'action demandée ou le fonctionnement n'est pas valide.	400 Requête erronée
`InvalidClientTokenId`	Le certificat X.509 ou AWS l'ID de clé d'accès fourni n'existe pas dans nos archives.	403 Forbidden

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 clé AWS d'accès et votre méthode de signature.	400 Requête erronée
`MissingAction`	Il manque un paramètre d'action ou d'opération dans la demande.	400 Requête erronée
`MissingAuthenticationToken`	La demande doit contenir un ID de clé d' AWS accès valide (enregistré) ou un certificat X.509.	403 Forbidden
`RequestExpired`	La demande a dépassé la date d'expiration ou la date de la demande (l'un ou l'autre avec un remplissage de 15 minutes), ou la date de la demande 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 demande a échoué en raison d'une défaillance temporaire du serveur.	503 – Service non disponible
`SubscriptionRequiredException`	L'ID de clé d' AWS accès nécessite un abonnement pour le service.	400 Requête erronée
`ThrottlingException`	Taux dépassé.	400 Requête erronée

Exception	Message	HTTP Status Code
`TooManyRequests`	Nombre de demandes trop élevé.	429 Trop de demandes
`UnknownOperationException`	Une opération inconnue a été spécifiée. Les opérations valides sont répertoriées dans Actions de l'API 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 montre le mappage entre les codes d'erreur d' AWS Storage Gateway opération et APIs ceux qui peuvent renvoyer les codes. Tous les codes d'erreur de fonctionnement sont renvoyés avec l'une des deux exceptions générales (`InternalServerError` et `InvalidGatewayRequestException`) décrites 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
FileSystemAssociationEndpointConfigurationConflict	La configuration existante du point de terminaison de l'association de systèmes de fichiers est en conflit avec la configuration spécifiée.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	L'adresse IP du point de terminaison spécifiée est déjà utilisée.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	L'adresse IP du point de terminaison de l'association du système de fichiers est manquante.	AssociateFileSystem
FileSystemAssociationNotFound	L'association de système de fichiers spécifiée est introuvable.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	Le système de fichiers spécifié est introuvable.	AssociateFileSystem

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 paramètre s 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
`MaximumVolumeCountExceeded`	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
`UnsupportedOperationForGatewayType`	L’opération spécifiée n’est pas valide pour le type de passerelle.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Le volume spécifié existe déjà.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	Le volume spécifié n'est pas valide.	DeleteVolume
`VolumeInUse`	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 :

- Type de contenu : application/ -1.1 x-amz-json
- 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 deExceptions.

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' DescribeStorediSCSIVolumesAPI et spécifiez une entrée de demande 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 demande.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Actions de l'API Storage Gateway

Pour obtenir la liste des opérations Storage Gateway consultez Actions dans Référence d'API AWS Storage Gateway .

Historique du document pour le guide de l'utilisateur d'Amazon FSx File Gateway

Le tableau suivant décrit les modifications importantes apportées à chaque version de ce guide de l'utilisateur après avril 2018. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Avis de modification de disponibilité pour FSx File Gateway	Amazon FSx File Gateway n'est plus disponible pour les nouveaux clients. Les clients existants de FSx File Gateway peuvent continuer à utiliser le service normalement. Pour des fonctionnalités similaires à FSx File Gateway, consultez ce billet de blog.	28 octobre 2024
Avis de modification de disponibilité pour FSx File Gateway	AWS Storage Gateway's FSx File Gateway ne sera plus disponible pour les nouveaux clients à partir du 28/10/24. Pour utiliser le service, vous devez vous inscrire avant cette date. Les clients existants de FSx File Gateway peuvent continuer à utiliser le service normalement. Pour des fonctionnalités similaires à FSx File Gateway, consultez ce billet de blog.	26 septembre 2024
Ajout d'une option pour activer ou désactiver les mises à jour de maintenance	Storage Gateway reçoit régulièrement des mises à jour de maintenance qui peuvent	6 juin 2024

	inclure des mises à niveau du système d'exploitation et des logiciels, des correctif s pour améliorer la stabilité , les performances et la sécurité, ainsi que l'accès aux nouvelles fonctionnalités. Vous pouvez désormais configure r un paramètre pour activer ou désactiver ces mises à jour pour chaque passerelle individuelle de votre déploieme nt. Pour plus d'informations, voir Gestion des mises à jour de passerelle à l'aide de la AWS Storage Gateway console.	
CloudWatch Alarmes recommandées mises à jour	L' CloudWatch `HealthNot ifications` alarme s'applique désormais et est recommandée pour tous les types de passerelles et de plateformes hôtes. Les paramètres de configura tion recommandés ont également été mis à jour pour `HealthNotifications` et`AvailabilityNotifi cations` . Pour plus d'informations, voir Comprendr e les CloudWatch alarmes.	2 octobre 2023

Conseils GatewayClockOutOfSync de dépannage ajoutés	La section Dépannage : problèmes liés à la passerelle de fichiers inclut désormais des instructions de dépannage pour vous aider à diagnostiquer les problèmes que vous pourriez rencontrer si l'horloge du système de votre passerelle n'est pas synchronisée avec l'heure du serveur AWS Storage Gateway. Pour plus d'informations, consultez la section Erreur : GatewayClockOutOfSync.	19 octobre 2022
Ajout de conseils de résolution des problèmes liés à Active Directory Join Domain	La section Dépannage : problèmes liés à la passerelle de fichiers inclut désormais des instructions de dépannage pour vous aider à diagnostiquer les problèmes que vous pourriez rencontrer lorsque vous essayez de joindre votre passerelle à un domaine Active Directory. Pour plus d'informations, voir Résolution des problèmes : problèmes liés au domaine Active Directory.	19 octobre 2022

Mise à jour des procédures de création de passerelle	La procédure de création d'une nouvelle passerelle a été mise à jour pour refléter les modifications apportées à la console Storage Gateway. Pour plus d'informations, consultez Créer et activer une passerelle de fichiers Amazon S3.	12 octobre 2021
Prise en charge de plusieurs systèmes de fichiers	Amazon FSx File Gateway prend désormais en charge jusqu'à cinq systèmes de FSx fichiers Amazon attachés. Pour plus d'informations, consultez Joindre un système de fichiers Amazon FSx pour Windows File Server.	7 juillet 2021

Support des quotas de stockage FSx souples d'Amazon	Amazon FSx File Gateway prend désormais en charge les quotas de stockage souples (qui vous avertissent lorsque les utilisateurs dépassent leurs limites de données) lors de l'écriture sur des systèmes de FSx fichiers Amazon joints dans lesquels des quotas de stockage sont configurés. Les quotas stricts (qui imposent des limites de données en refusant l'accès en écriture) ne sont pas pris en charge. Les quotas souples fonctionnent pour tous les utilisateurs, à l'exception de l' FSxadministrateur Amazon. Pour plus d'informations sur la configuration des quotas de stockage, consultez la section Quotas de stockage du guide de l'utilisateur du serveur de fichiers Amazon FSx pour Windows.	7 juillet 2021

Nouveau guide	Outre la passerelle de fichiers d'origine (désormais connue sous le nom d'Amazon S3 File Gateway), Storage Gateway fournit Amazon FSx File Gateway (passerelle de FSx fichiers). FSx File Gateway fournit une faible latence et un accès efficace aux partages de fichiers dans le cloud FSx pour Windows File Server depuis votre installation sur site. Pour plus d'informations, consultez Qu'est-ce qu'Amazon FSx File Gateway ?	27 avril 2021
Conformité au programme FedRAMP	Storage Gateway est désormais conforme à FedRAMP. Pour plus d'informations, consultez la section Validation de conformité pour Storage Gateway.	24 novembre 2020
Migration de la passerelle de fichiers	File Gateway fournit désormais un processus documenté pour remplacer une passerelle de fichiers existante par une nouvelle passerelle de fichiers. Pour plus d'informations, voir Remplacement d'une passerelle de fichiers par une nouvelle passerelle de fichiers.	30 octobre 2020

Performances de lecture du cache à froid de File Gateway multipliées par 4	Storage Gateway a multiplié par 4 les performances de lecture du cache froid. Pour plus d'informations, consultez les 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 la AWS Storage Gateway console. Pour plus d'informations, consultez la section Utilisation de l'appliance matérielle AWS Storage Gateway.	12 août 2020
Support des points de terminaison FIPS (Federal Information Processing Standard) dans les nouvelles régions AWS	Vous pouvez désormais activer une passerelle avec des points de terminaison FIPS dans les régions suivantes : USA Est (Ohio), USA Est (Virginie du Nord), USA Ouest (Californie du Nord), USA Ouest (Oregon) et Canada (Centre). Pour plus d'informations, consultez Points de terminaison et quotas AWS Storage Gateway dans le document Références générales AWS.	31 juillet 2020

Le stockage en cache local de File Gateway a été multiplié par 4	Storage Gateway prend désormais en charge un cache local pouvant atteindre 64 To pour File Gateway, ce qui améliore les performances des applications sur site en fournissant un accès à faible latence à des ensembles de données de travail plus importants. Pour plus d'informations, consultez la section Tailles de disque locales recommandées pour votre passerelle dans le guide de l'utilisateur de Storage Gateway.	7 juillet 2020
Afficher les CloudWatch alarmes Amazon dans la console Storage Gateway	Vous pouvez désormais consulter les CloudWatc h alarmes dans la console Storage Gateway. Pour plus d'informations, consultez la section Comprendre les CloudWatch alarmes.	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, consultez la section Choix d'un point de terminais on de service.	22 mai 2020

Nouvelles AWS régions	Storage Gateway est maintenant disponible dans les régions Afrique (Le Cap) et Europe (Milan). Pour plus d'informations, consultez Points de terminaison et quotas AWS Storage Gateway dans le document Références générales AWS.	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 plus d'informations, consultez Classe de stockage pour optimiser automatiquement les objets fréquemment et rarement consultés dans le Guide de l'utilisateur Amazon Simple Storage Service.	30 avril 2020

Nouvelle AWS région	Storage Gateway est désormais disponible dans la région AWS GovCloud (USA Est). Pour plus d'informations, consultez Points de terminaison et quotas AWS Storage Gateway dans le Références générales AWS.	12 mars 2020
Prise en charge de l'hyperviseur KVM (machine virtuelle basée sur le noyau Linux)	Storage Gateway offre maintenant la possibilité 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 plus d'informations, consultez Hyperviseurs pris en charge et configuration requise de l'hôte dans le Guide de l'utilisateur Storage Gateway.	4 février 2020

Support pour VMware vSphere High Availability	Storage Gateway prend désormais en charge la haute disponibilité VMware afin de protéger les charges de travail de stockage contre les pannes matérielles, d'hypervi seurs ou de réseau. Pour plus d'informations, consultez la section Utilisation de VMware vSphere High Availability with Storage Gateway dans le guide de l'utilisateur de Storage Gateway. Cette version inclut également des améliorations de performan ces. Pour plus d'informations, consultez Performances dans le Guide de l'utilisateur Storage Gateway.	20 novembre 2019
Support pour Amazon CloudWatch Logs	Vous pouvez désormais configurer des passerelles de fichiers avec Amazon CloudWatch Log Groups pour être informé des erreurs et de l'état de votre passerelle et de ses ressources. Pour plus d'informations, consultez Getting Notified About Gateway Health and Errors With Amazon CloudWatch Log Groups dans le guide de l'utilisateur de Storage Gateway.	4 septembre 2019

Nouvelle Région AWS	Storage Gateway est désormais disponible dans la région Asie-Pacifique (Hong Kong). Pour plus d'informations, consultez Points de terminaison et quotas AWS Storage Gateway dans le Références générales AWS.	14 août 2019
Nouvelle Région AWS	Storage Gateway est désormais disponible dans la région Moyen-Orient (Bahreïn). Pour plus d'informations, consultez Points de terminaison et quotas AWS Storage Gateway dans le Références générales AWS.	29 juillet 2019
Prise en charge de l'activation d'une passerelle dans un cloud privé virtuel (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 cloud privé virtuel.	20 juin 2019

Support de File Gateway pour l'autorisation basée sur des balises	File Gateway prend désormais en charge l'autorisation basée sur des balises. Vous pouvez contrôler l'accès aux ressources de File Gateway en fonction des balises associées à ces ressource s. 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 AWS Storage Gateway en Europe	L'appliance matérielle AWS Storage Gateway est désormais disponible en Europe. Pour plus d'informations, consultez Régions d'appliance matérielle AWS Storage Gateway dans le document Références générales AWS. En outre, vous pouvez désormais augmenter le stockage utilisable sur l'appliance matérielle AWS Storage Gateway de 5 To à 12 To et remplacer la carte réseau en cuivre installée par une carte réseau à fibre optique de 10 gigabits. Pour plus d'informations, consultez Configuration de votre appliance matérielle.	25 février 2019
Support pour l'appliance matérielle AWS Storage Gateway	L'appliance matérielle AWS 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 plus d'informations, consultez Utilisation de l'appareil Storage Gateway Hardware Appliance.	18 septembre 2018

Mises à jour antérieures

Le tableau ci-après décrit les modifications importantes apportées dans chaque version du Guide de l'utilisateur AWS Storage Gateway avant mai 2018.

Modifier	Description	Date de modification
Nouveau Région AWS	La passerelle de bande est désormais disponible dans la région Asie-Pacifique (Singapour). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	3 avril 2018
Nouveau Région AWS	Storage Gateway est désormais disponible dans la Région Europe (Paris). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	18 décembre 2017
Support pour la version 6.5 de VMware ESXi l'hyperviseur	AWS Storage Gateway prend désormais en charge la version 6.5 de VMware ESXi l'hyperviseur. 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 compatibles avec Storage Gateway.	02 mai 2017
Prise en charge des passerelles	AWS Storage Gateway permet désormais de déployer une passerelle de fichiers dans Amazon EC2. Vous pouvez lancer une passerelle de fichiers dans	08 février 2017

Modifier	Description	Date de modification
de fichiers sur Amazon EC2	Amazon EC2 à l'aide de Amazon Machine Image (AMI) de Storage Gateway, désormais disponible en tant qu'AMI de communauté. Pour plus d'informations sur la façon de créer une passerelle de fichiers et de la déployer sur une instance EC2, consultezCréation et activation d'un Amazon FSx File Gateway. Pour plus d'informations sur le lancement d'une AMI de passerelle de fichiers, consultezDéployer un hôte Amazon EC2 par défaut pour File Gateway FSx. En outre, File Gateway prend désormais en charge la configuration du proxy HTTP. Pour de plus amples informations, veuillez consulter Routage de votre passerelle déployée sur Amazon EC2 via un proxy HTTP.	
Nouveau Région AWS	Storage Gateway est désormais disponible dans la région Europe (Londres). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	13 décembre 2016
Nouveau Région AWS	Storage Gateway est désormais disponible dans la région Canada (Centre). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	08 décembre 2016

Modifier	Description	Date de modification
Prise en charge de la passerelle de fichiers	En plus de la passerelle de volume et la passerelle de bande, Storage Gateway propose désormais la prise en charge de la passerelle de fichiers. La passerelle de fichiers associe 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). La passerelle permet d'accéder aux objets dans Amazon S3 sous forme de fichiers sur un point de montage NFS.	29 novembre 2016