Guide de l’utilisateur pour une passerelle de bande

AWS Storage Gateway

Version de l'API 2013-06-30

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

AWS Storage Gateway: Guide de l’utilisateur pour une passerelle de bande

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

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

Table of Contents

Qu’est-ce qu’une passerelle de bande ? 1
Fonctionnement d’une passerelle de bande 2
Passerelles de bande 2
Commencer avec AWS Storage Gateway 6
Inscrivez-vous pour AWS Storage Gateway 6
Création d'un utilisateur IAM doté de privilèges d'administrateur 7
Accès AWS Storage Gateway 9
Régions AWS compatibles avec Storage Gateway 9
Configuration requise pour Tape Gateway 11
Exigences en matière de matériel et de stockage 11
Configuration matérielle requise pour VMs 11
Exigences relatives aux types d' EC2 instances Amazon 12
..... 12
Besoins de stockage 12
Exigences pour le réseau et le pare-feu 13
Exigences pour les ports 14
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
Initiateurs iSCSI pris en charge 35
Applications de sauvegarde tierces prises en charge 36
Utilisation de l’appliance matérielle 38
Configuration de votre appliance matérielle 39
Installation physique de votre appliance matérielle 41
Accès à la console de l'appliance matérielle 43
Configuration des paramètres réseau de l'appliance matérielle 44
Activation de votre appliance matérielle 46
Création d'une passerelle sur votre appliance matérielle 47
Configuration d'une adresse IP de passerelle sur l'appliance matérielle 48
Suppression du logiciel de passerelle de votre appliance matérielle 51
Suppression de votre appliance matérielle 52
Création de votre passerelle 54
Présentation - Activation de la passerelle 54

Configuration d'une passerelle 54
Connect à AWS 55
Vérifier et activer 55
Présentation - Configuration de la passerelle 55
Présentation - Ressources de stockage 55
Création et activation d'une passerelle de bande 56
Configuration d'une passerelle de bande 56
Connectez votre Tape Gateway à AWS 57
Vérifier les paramètres et activer votre passerelle de bande 59
Configurer votre passerelle de bande 59
Création de bandes 62
Protection de bande WORM 63
Création manuelle de bandes 63
Autoriser la création automatique de bandes 65
Création de groupes de bandes personnalisés 69
Choix d'un type 69
Verrouillage de rétention de bande 70
Création d'un groupe de bandes personnalisé 71
Connexion de vos appareils VTL 72
Connexion à un client Microsoft Windows 72
Connexion à un client Linux 74
Test de votre passerelle 77
Arcserve Backup 78
Bacula Enterprise 82
Commvault 86
Dell EMC NetWorker 92
Protection des données IBM 96
OpenText Protecteur de données 100
Microsoft System Center DPM 107
NovaStor DataCenter/Réseau 112
Quest NetVault Backup 118
Veeam Backup & Replication 122
Veritas Backup Exec 125
Veritas NetBackup 130
Comment procéder ensuite ? 136
Activation d'une passerelle dans un cloud privé virtuel 137

Création d'une passerelle à l'aide d'un point de terminaison de VPC pour Storage Gateway ... 138
Gestion de votre Tape Gateway ... 140
Modification des informations de la passerelle ... 141
Gestion de la création automatique de bandes ... 142
Archivage des bandes ... 145
Déplacement de bandes vers S3 Glacier Deep Archive ... 145
Récupération des bandes archivées ... 146
Affichage des statistiques d'utilisation des cassettes ... 148
Suppression des bandes ... 149
Suppression de groupes de bandes personnalisés ... 150
Désactivation de votre passerelle de bande ... 151
Comprendre l'état de la bande ... 152
Comprendre les informations sur l'état d'une bande dans une VTL ... 152
Détermination de l'état d'une bande dans une archive ... 154
Déplacement de vos données vers une nouvelle passerelle ... 155
Déplacement de bandes virtuelles dans une nouvelle passerelle de bande ... 155
Surveillance de Storage Gateway ... 160
Présentation des métriques de la passerelle ... 160
Dimensions des métriques de Storage Gateway ... 164
Surveillance du tampon de chargement ... 165
Surveillance du stockage de cache ... 168
Comprendre les CloudWatch alarmes ... 169
Création d' CloudWatch alarmes recommandées ... 171
Création d'une CloudWatch alarme personnalisée ... 172
Surveillance de votre passerelle de bande ... 174
Obtention des journaux d'intégrité de la passerelle de bande ... 175
Utilisation d'Amazon CloudWatch Metrics ... 177
Comprendre les métriques des bandes virtuelles ... 178
Mesurer les performances entre votre Tape Gateway et AWS ... 181
Maintenance de votre passerelle ... 184
Gestion des disques locaux ... 184
Déterminer la quantité de stockage du disque local ... 185
Ajout de stockage de tampon de chargement ou de cache ... 189
Gestion de bande passante ... 190
Modification de la limitation de bande passante à l'aide de la console Storage Gateway ... 191

Planification de la limitation de bande passante 191
À l'aide du AWS SDK pour Java 193
À l'aide du AWS SDK pour .NET 195
À l'aide du AWS Tools for Windows PowerShell 197
Gestion des mises à jour de passerelle 199
Fréquence de mise à jour et comportement attendu 199
Activer ou désactiver les mises à jour de maintenance 200
Modifier le calendrier de la fenêtre de maintenance de la passerelle 201
Appliquer une mise à jour manuellement 202
Arrêt de la machine virtuelle de la passerelle 203
Démarrage et arrêt d'une passerelle de bande 204
Suppression de votre passerelle et suppression de ressources 205
Suppression de la passerelle à l'aide de la console Storage Gateway 206
Suppression de ressources à partir d'une passerelle déployée sur site 207
Suppression de ressources d'une passerelle déployée sur une EC2 instance Amazon 209
Exécution de tâches de maintenance à l'aide de la console locale 211
Accès à la console locale de la passerelle 211
Accès à la console locale de la passerelle avec Linux KVM 212
Accès à la console locale de Gateway avec VMware ESXi 212
Accéder à la console locale de passerelle avec Microsoft Hyper-V 213
Exécution des tâches sur la console locale de machine virtuelle 214
Connexion à la console locale Tape Gateway 215
Configuration d'un SOCKS5 proxy pour votre passerelle sur site 217
Configuration de votre passerelle réseau 218
Test de la connectivité de votre passerelle à Internet 225
Exécution de commandes de passerelle de stockage dans la console locale pour une passerelle locale 226
Affichage de l'état des ressources système de la passerelle 229
Exécution de tâches sur la console EC2 locale 230
Connexion à la console locale de votre EC2 passerelle 231
Configuration d'un proxy HTTP 231
Test de la connectivité réseau des passerelles 232
Affichage de l'état des ressources système de la passerelle 233
Exécution des commandes Storage Gateway sur la console locale 234
Performances et optimisation pour Tape Gateway 237
Recommandations en matière de performances pour les passerelles de bande 237

Optimisation des performances de la passerelle 240
Configuration recommandée 240
Ajouter des ressources à la passerelle 241
Optimiser les paramètres iSCSI 244
Utiliser une taille de bloc supérieure pour les lecteurs de bandes 245
Optimisation des performances de lecteurs de bandes virtuelles 245
Ajouter des ressources à votre environnement d'application 246
Sécurité 247
Protection des données 248
Chiffrement des données 249
Gestion de l'identité et des accès 250
Public ciblé 251
Authentification par des identités 252
Gestion des accès à l'aide de politiques 256
Comment AWS Storage Gateway fonctionne avec IAM 259
Exemples de politiques basées sur l'identité 266
Résolution des problèmes 269
Validation de conformité 271
Résilience 272
Sécurité de l'infrastructure 273
AWS Bonnes pratiques en matière de sécurité 274
Journalisation et surveillance 274
Informations sur Storage Gateway dans CloudTrail 274
Comprendre les entrées des fichiers journaux de Storage Gateway 275
Dépannage des problèmes de passerelle 278
Résolution des problèmes : problèmes de connexion à la passerelle 279
Vérifiez le pare-feu ou le proxy associé 279
Vérifiez s'il existe une inspection SSL ou approfondie des paquets en cours du trafic de votre passerelle 279
Vérifiez l'absence d'une panne de courant ou d'une défaillance matérielle sur l'hôte de l'hyperviseur 280
Vérifiez les problèmes liés à un disque de cache associé 280
Résolution des problèmes : problèmes d'activation de la passerelle 281
Résoudre les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison public 281

Résolvez les erreurs lors de l'activation de votre passerelle à l'aide d'un point de terminaison Amazon VPC ... 284
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 ... 289
Dépannage des problèmes de passerelle sur site ... 289
Activation Support pour aider à résoudre les problèmes de votre passerelle ... 294
Résolution des problèmes de configuration de Microsoft Hyper-V ... 295
Résolution des problèmes liés à EC2 la passerelle Amazon ... 300
L'activation de passerelle ne se produit pas au bout de quelques instants ... 301
Impossible de trouver l'instance de EC2 passerelle dans la liste des instances ... 301
Impossible d'associer un volume Amazon EBS à l'instance de EC2 passerelle ... 302
Message aucun disque disponible lorsque vous essayez d'ajouter des volumes de stockage ... 302
Comment supprimer un disque alloué en tant qu'espace de tampon de chargement pour réduire l'espace du tampon de chargement ... 302
Le débit à destination ou en provenance de la EC2 passerelle tombe à zéro ... 302
Activation Support pour aider à résoudre les problèmes liés à la passerelle ... 303
Connectez-vous à votre EC2 passerelle Amazon à l'aide de la console série ... 305
Résolution des problèmes des appliances matérielles ... 305
Comment déterminer l'adresse IP du service ... 305
Effectuer une réinitialisation d'usine ... 305
Réaliser un redémarrage à distance ... 306
Obtenir l'assistance pour Dell iDRAC ... 306
Trouver le numéro de série de l'appliance matérielle ... 306
Obtenir le support des appliances matérielles ... 306
Dépannage des problèmes de bandes virtuelles ... 307
Récupération d'une bibliothèque de bandes virtuelles à partir d'une passerelle irrécupérable ... 307
Résolution des problèmes de bandes irrécupérables ... 311
Notifications d'intégrité relatives à la haute disponibilité ... 313
Résolution des problèmes de haute disponibilité ... 313
Notifications d'intégrité ... 313
Métriques ... 315
Bonnes pratiques ... 316
Bonnes pratiques : récupération de vos données ... 316
Récupération après l'arrêt inattendu d'une machine virtuelle ... 317

Récupération de données d'une passerelle ou d'une machine virtuelle défaillante 317
Récupération des données d'une bande irrécupérable 318
Récupération des données d'un disque de cache défaillant 318
Récupération de données à partir d'un centre de données inaccessible 318
Nettoyage des ressources inutiles 319
Ressources supplémentaires 321
Configuration de l'hôte 322
Déployer un EC2 hôte Amazon par défaut pour Tape Gateway 323
Déployez une EC2 instance Amazon personnalisée pour Tape Gateway 325
Modifier les options de métadonnées de l' EC2 instance Amazon 329
Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux .. 330
Synchroniser l'heure de la machine virtuelle avec VMware celle de l'hôte 331
Configuration de contrôleurs de disque paravirtualisés 332
Configuration des adaptateurs réseau pour votre passerelle 333
Utilisation VMware de la haute disponibilité avec Storage Gateway 338
Utilisation des ressources de stockage Tape Gateway 344
Suppression de disques de votre passerelle 345
Volumes EBS pour passerelles EC2 346
Utilisation des dispositifs VTL 347
Utilisation des bandes 351
Obtention de la clé d'activation 353
Linux (curl) 354
Linux (bash/zsh) 355
Microsoft Windows PowerShell 356
Utilisation de votre console locale 356
Connexion aux initiateurs iSCSI 357
Connexion d'appareils VTL à un client Windows 358
Connexion de (appareils VTL) à un client Linux 361
Personnalisation des paramètres iSCSI 363
Configuration de l'authentification CHAP 368
Utilisation AWS Direct Connect avec Storage Gateway 374
Obtenir l'adresse IP de la passerelle 375
Obtenir une adresse IP auprès d'un EC2 hôte Amazon 375
Comprendre les ressources et les ressources IDs 376
Travailler avec Resource IDs 377
Balisage des ressources 378

Utilisation des balises 379
Composants open source 380
Quotas Storage Gateway 380
Quotas pour les bandes 381
Tailles des disques locaux recommandées pour votre passerelle 381
Référence d'API 383
En-têtes de requête obligatoires 383
Signature des requêtes 386
Exemple de calcul de signature 387
Réponses d'erreur 388
Exceptions 389
Codes d'erreur d'opération 391
Réponses d'erreur 411
Opérations 413
Historique de la documentation 414
Mises à jour antérieures 434
Notes de mise à jour 456
..... cdlxiii

Qu’est-ce qu’une passerelle de bande ?

AWS Storage Gateway connecte une appliance logicielle sur site à un stockage basé sur le cloud afin de permettre une intégration fluide des fonctionnalités de sécurité des données entre votre environnement informatique sur site et l'infrastructure AWS de stockage. Vous pouvez utiliser le service pour stocker des données dans le cloud Amazon Web Services et profiter d’un stockage évolutif et économique qui vous aide à garantir la sécurité des données.

Vous pouvez déployer Storage Gateway sur site en tant qu'appliance de machine virtuelle exécutée sur VMware ESXi un hyperviseur KVM ou Microsoft Hyper-V, en tant qu'appliance matérielle ou en AWS tant qu'instance Amazon. EC2 Vous pouvez utiliser des passerelles hébergées sur EC2 des instances pour la reprise après sinistre, la mise en miroir des données et le stockage des applications hébergées sur Amazon. EC2

Pour découvrir le large éventail de cas d'utilisation qui AWS Storage Gateway permettent de le rendre possible, voir AWS Storage Gateway. Pour obtenir des informations actualisées sur les tarifs, consultez Tarification sur la page de détails d’ AWS Storage Gateway .

AWS Storage Gateway propose des solutions de stockage basées sur des fichiers (passerelle de FSx fichiers S3 et passerelle de fichiers), sur volume (passerelle de volume) et sur bande (passerelle de bande).

Ce guide de l'utilisateur fournit des informations relatives à Tape Gateway.

Tape Gateway fournit un stockage sur bande virtuel basé sur le cloud. Avec Tape Gateway, vous pouvez archiver les données de sauvegarde de manière rentable et durable dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Tape Gateway fournit une infrastructure de bandes virtuelles qui s'adapte parfaitement aux besoins de votre entreprise et élimine la charge opérationnelle liée au provisionnement, à la mise à l'échelle et à la maintenance d'une infrastructure de bandes physiques.

Pour une présentation de l’architecture, consultez Fonctionnement d’une passerelle de bande.

Dans ce guide de l'utilisateur, vous trouverez une section de mise en route qui couvre les informations de configuration communes à tous les types de passerelles. Vous trouverez également les exigences de configuration de Tape Gateway , ainsi que les sections qui décrivent comment déployer, activer, configurer et gérer votre Tape Gateway .

Les procédures décrites dans ce guide de l'utilisateur se concentrent principalement sur l'exécution des opérations de passerelle à l'aide du AWS Management Console. Pour réaliser ces opérations par programme, consultez Référence AWS Storage Gateway API.

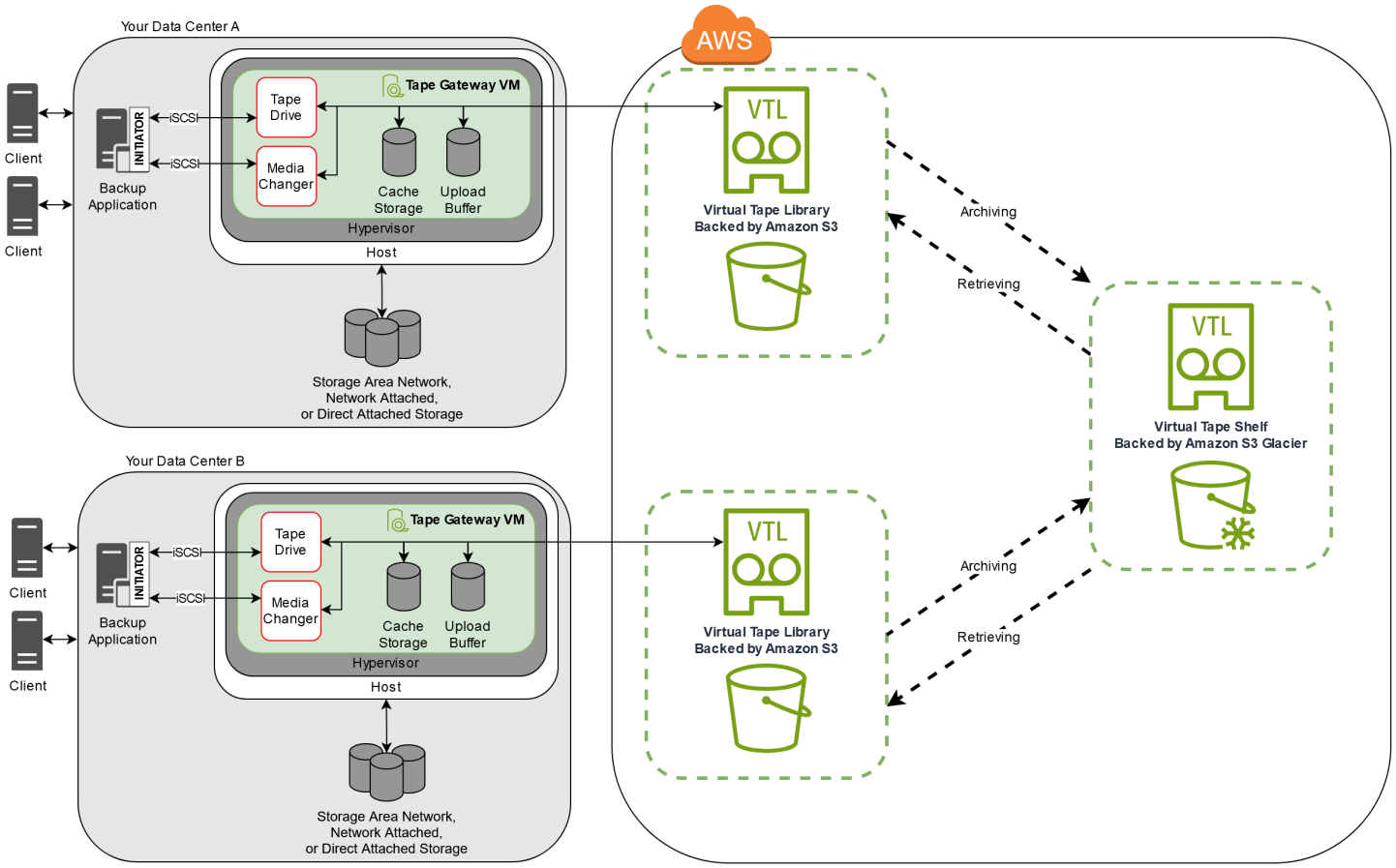
Fonctionnement d'une passerelle de bande

Voici une présentation de l'architecture de la solution de passerelle de bande.

Passerelles de bande

L'architecture de passerelle de bande propose une solution durable et rentable pour archiver vos données dans le cloud Amazon Web Services. Grâce à l'interface de la bibliothèque de bandes virtuelles (VTL), vous tirez parti de votre infrastructure de sauvegarde sur bande existante pour stocker des données sur des cartouches de bandes virtuelles que vous créez sur votre passerelle de bande. Chaque passerelle de bande est préconfigurée avec un changeur de média et des lecteurs de bandes. Ceux-ci sont disponibles pour vos applications de sauvegarde client existantes en tant qu'appareils iSCSI. Vous ajoutez des cartouches de bandes en fonction de vos besoins pour archiver vos données.

Le diagramme suivant présente le déploiement d'une passerelle de bande.



Le schéma identifie les composants suivants de la passerelle de bande :

- Bande virtuelle : une bande virtuelle est identique à une cartouche de bande physique. Cependant, les données de bandes virtuelles sont stockées dans le cloud Amazon Web Services. A l'instar des bandes physiques, les bandes virtuelles peuvent être vides ou contenir des données. Vous pouvez créer des bandes virtuelles à l'aide de la console Storage Gateway ou par programme en utilisant l'API Storage Gateway. Chaque passerelle peut contenir jusqu'à 1 500 bandes ou jusqu'à 1 Pio de données au total simultanément. La taille de chaque bande virtuelle, que vous pouvez configurer lorsque vous créez la bande, est située entre 100 Gio et 15 Tio.
- Bibliothèque de bandes virtuelles (VTL) : une VTL est comme une bibliothèque de bandes physiques disponible sur site avec des bras robotisés et des lecteurs de bandes. Votre VTL comprend la collection de bandes virtuelles stockées. Chaque passerelle de bande intègre une VTL.

  Les bandes virtuelles que vous créez apparaissent dans la VTL de la passerelle. Les bandes incluses dans la VTL sont prises en charge par Amazon S3. A mesure que votre logiciel de sauvegarde écrit les données sur la passerelle, cette dernière stocke les données localement, puis les charge de façon asynchrone sur les bandes virtuelles de votre VTL, c'est-à-dire Amazon S3.

  - Lecteur de bandes : un lecteur de bandes VTL est identique à un lecteur de bandes physiques qui peut effectuer des E/S et rechercher des opérations sur une bande. Chaque VTL est associée à un ensemble de 10 lecteurs de bandes, qui sont disponibles pour votre application de sauvegarde en tant qu'appareils iSCSI.
  - Changeur de média : un changeur de média VTL est identique à un robot qui déplace les bandes dans des emplacements de stockage et des lecteurs de bandes de la bibliothèque de bandes physiques. Chaque VTL est fournie avec un changeur de média, qui est disponible pour votre application de sauvegarde en tant qu'appareil iSCSI.
- Archive : une archive est identique à un site de stockage de bandes hors site. Vous pouvez archiver des bandes de la VTL de votre passerelle vers l'archive. Si nécessaire, vous pouvez ré-extraire des bandes de l'archive vers la VTL de votre passerelle.
  - Archivage des bandes : lorsque le logiciel de sauvegarde éjecte une bande, la passerelle transfère la bande vers l'archive pour un stockage à long terme. L'archive est située dans la région AWS dans laquelle vous avez activé la passerelle. Les bandes de l'archive sont stockées dans l'étagère des bandes virtuelles (VTS). L'étagère de bandes virtuelles (VTS) est soutenue par S3 Glacier Flexible Retrieval ou S3 GlacierDeep Archive, un service de stockage à faible coût pour l'archivage des données, la sauvegarde et la conservation des données à long terme.
  - Extraction des bandes – Vous ne pouvez pas lire directement les bandes archivées. Pour lire une bande archivée, vous devez tout d'abord la transférer sur votre passerelle de bande à l'aide de la console Storage Gateway ou de l'API Storage Gateway.

> **Important**
>
> Si vous archivez une bande dans S3 Glacier Flexible Retrieval, vous pouvez la récupérer généralement en 3 à 5 heures. Si vous archivez la bande dans S3 Glacier Deep Archive, vous pouvez la récupérer généralement dans un délai de 12 heures.

Une fois que vous avez déployé et activé une passerelle de bande, vous installez les lecteurs de bandes virtuelles et le changeur de média sur vos serveurs d'applications sur site en tant qu'appareils iSCSI. Vous créez des bandes virtuelles selon vos besoins. Vous utilisez ensuite votre application logicielle de sauvegarde pour écrire des données sur les bandes virtuelles. Le changeur de média charge et décharge les bandes virtuelles dans les lecteurs de bandes virtuelles pour les opérations de lecture et d'écriture.

Allocation des disques locaux pour la machine virtuelle de la passerelle

La machine virtuelle de votre passerelle nécessite des disques locaux, que vous allouez dans les buts suivants :

- Stockage de cache : le stockage du cache fait office de stockage durable des données en attente de chargement sur Amazon S3 à partir du tampon de chargement.

  Si votre application lit des données d'une bande virtuelle, la passerelle enregistre les données sur le stockage de cache. La passerelle stocke les données récemment consultées dans le stockage de cache pour l'accès à faible latence. Si votre application demande des données sur bande, la passerelle vérifie d'abord la présence de ces données dans le cache avant de les télécharger AWS.
- Tampon de chargement : le tampon de chargement fournit une zone de transit pour la passerelle avant le chargement des données vers une bande virtuelle. Le tampon de chargement joue également un rôle essentiel pour la création de points de récupération que vous pouvez utiliser pour récupérer les bandes d'échecs inattendus. Pour plus d'informations, consultez Vous avez besoin de récupérer une bande virtuelle à partir d'une passerelle de bande défaillante.

A mesure que votre application de sauvegarde écrit les données sur votre passerelle, la passerelle copie les données à la fois vers le stockage de cache et le tampon de chargement. Elle reconnaît ensuite la fin de l'opération d'écriture sur votre application de sauvegarde.

Pour connaître les instructions sur la quantité d'espace disque à allouer pour le stockage de cache et le tampon de chargement, consultez Déterminer la quantité de stockage du disque local.

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 Tape 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

- Inscrivez-vous pour AWS Storage Gateway- 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.

Inscrivez-vous pour AWS Storage Gateway

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.

   Une partie de la procédure d'inscription consiste à recevoir un appel téléphonique ou un message texte et à saisir un code de vérification sur le clavier 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 AWS Identity and Access Management (IAM) pour vous-même, puis ajoutez cet utilisateur à un groupe doté d'autorisations administratives. Pour plus d'informations sur l'utilisation du AWS Identity and Access Management service pour contrôler l'accès aux ressources Storage Gateway, consultezIdentity and Access Management pour AWS Storage Gateway.

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

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des identifiants à court terme pour accéder à AWS. Telles sont les meilleures pratiques en matière de sécurité. Pour plus d'informations sur les bonnes pratiques, veuillez consulter Security best practices in IAM (français non garanti) dans le Guide de l'utilisateur IAM.	Suivre les instructions de la section Mise en route dans le AWS IAM Identity Center Guide de l'utilisateur.	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 des identifiants à long terme pour accéder à AWS.	Suivez les instructions de la section Créer un utilisateur IAM pour un accès d'urgence dans le guide de l'utilisateur IAM.	Configurez l'accès programmatique en gérant les 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 création, la gestion et la suppression de bandes dans les de votre librairie de bandes virtuelle, 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 AWS Identity and Access Management, 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 EC2 instances Amazon 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.

- 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, voir AWS Storage Gateway Endpoints and Quotas dans le. Références générales AWS
- Storage Gateway Hardware Appliance : pour connaître les AWS régions prises en charge que vous pouvez utiliser avec l'appliance matérielle, voir Régions de l'appliance AWS Storage Gateway matérielle dans le. Références générales AWS

Exigences relatives à la configuration de Tape Gateway

Sauf mention contraire, les critères suivants sont communs à toutes les configurations de la passerelle.

Rubriques

- 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
- Initiateurs iSCSI pris en charge
- Applications de sauvegarde tierces prises en charge pour une passerelle de bande

Exigences en matière de matériel et de stockage

Cette section décrit les exigences matérielles minimales et les paramètres pour votre passerelle, et la quantité minimale d'espace disque à allouer pour le stockage requis.

Configuration matérielle requise pour VMs

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

- Quatre processeurs virtuels attribués à la machine virtuelle.
- Pour une passerelle de bande, votre matériel doit dédier les quantités de RAM suivantes :
  - 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
- 80 Gio d'espace disque pour l'installation de l'image de la machine virtuelle et les données système.

Pour plus d'informations, consultez Optimisation des performances de la passerelle. Pour obtenir des informations sur la façon dont votre matériel affecte les performances de la machine virtuelle de la passerelle, consultez AWS Storage Gateway quotas.

Exigences relatives aux types d' EC2 instances Amazon

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

> **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.

Pour Tape Gateway, votre EC2 instance Amazon doit consacrer les quantités de RAM suivantes en fonction de la taille du cache que vous prévoyez d'utiliser pour votre passerelle :

- 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

Utilisez l’un des types d’instance suivants recommandés pour votre type de passerelle.

Recommandé pour Tape Gateway

- Famille d’instances à usage général : type d’instance m4, m5, ou m6.
- Famille d'instances optimisée pour le calcul : types d'instances c4, c5, c6 ou c7. Sélectionnez la taille d’instance 2xlarge ou une taille supérieure pour répondre aux exigences de RAM.
- Famille d'instances optimisée pour la mémoire : types d'instances r3, r5, r6 ou r7.
- Famille d'instances optimisée pour le stockage : types d'instances i3, i4 ou i7.

Besoins de stockage

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

Le tableau suivant recommande des tailles pour le stockage du disque local associé à la passerelle déployée.

Type de passerelle	Cache (minimum)	Cache (maximum)	Tampon de chargement (minimum)	Tampon de chargement (maximum)	Autres disques locaux requis
Passerelle de bande	150 Gio	64 Tio	150 Gio	2 Tio	—

> **Note**
>
> Vous pouvez configurer un ou plusieurs disques locaux pour votre cache et votre tampon de chargement, dans la limite de leur capacité maximale.
> Lorsque vous ajoutez du cache ou de la mémoire tampon de téléchargement à une passerelle existante, il est important de créer de nouveaux disques sur votre hôte (hyperviseur ou EC2 instance Amazon). Ne modifiez pas la taille des disques existants si les disques ont été alloués entant que tampons de cache ou de chargement.

Pour obtenir des informations sur les quotas de passerelle, consultez AWS Storage Gateway quotas.

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. 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 Storage Gateway 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'adresses AWS 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.

> **Note**
>
> 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. Dans certains cas, vous pouvez déployer Storage Gateway sur Amazon EC2 ou utiliser d'autres types de déploiement

Rubriques

- Exigences pour les 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 Amazon EC2 Gateway

Exigences pour les ports

Tape 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.

Exigences relatives aux ports pour Tape Gateway

Élément de réseau	De	Pour	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

Élément de réseau	De	Pour	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								la clé d'activation 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

Élément de réseau	De	Pour	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								requis de 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

Élément de réseau	De	Pour	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
								accès au port 80 de votre passerelle.
Navigateur Web	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	443	✓	✓	✓	AWS Console de gestion (toutes les autres opérations)

Élément de réseau	De	Pour	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
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	Pour	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	Pour	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	Pour	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	Pour	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	Pour	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

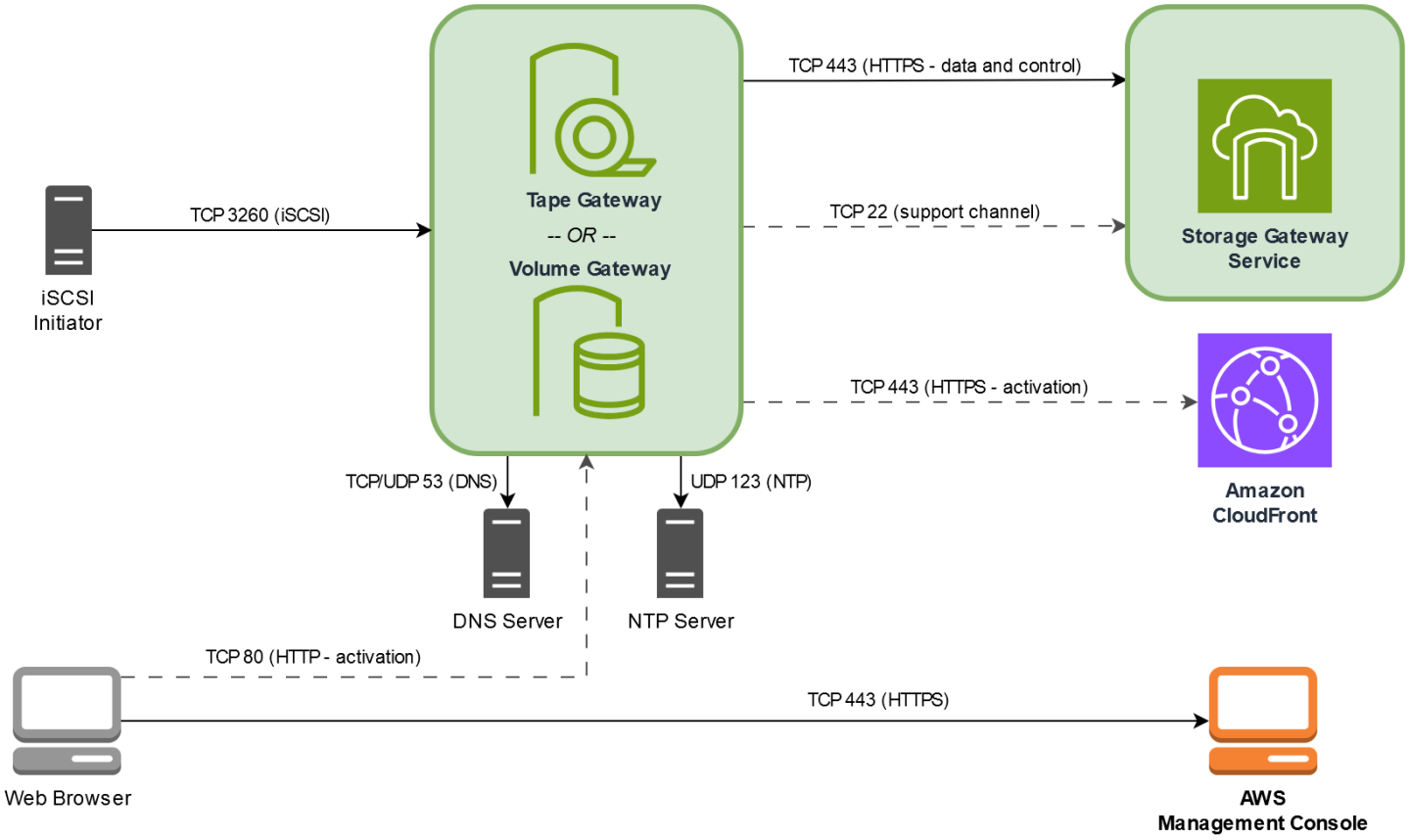
Élément de réseau	De	Pour	Protocole	Port	Entrant	Sortant	Obligatoire	Remarques
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS TCP	1027		✓	✓*	Plan de contrôle Anon (pour activation) *Obligatoire uniquement lors de l'utilisation de points de terminaison VPC
VPC	Machine virtuelle Storage Gateway	AWS	HTTPS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

Élément de réseau	De	Pour	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	Pour	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	Pour	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
Client iSCSI	client iSCSI	Machine virtuelle Storage Gateway	TCP	3260	✓	✓	✓	Pour que les systèmes locaux se connectent aux cibles iSCSI exposées par la passerelle.

L'illustration suivante montre le flux de trafic réseau pour un déploiement de base de Tape Gateway.



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 :

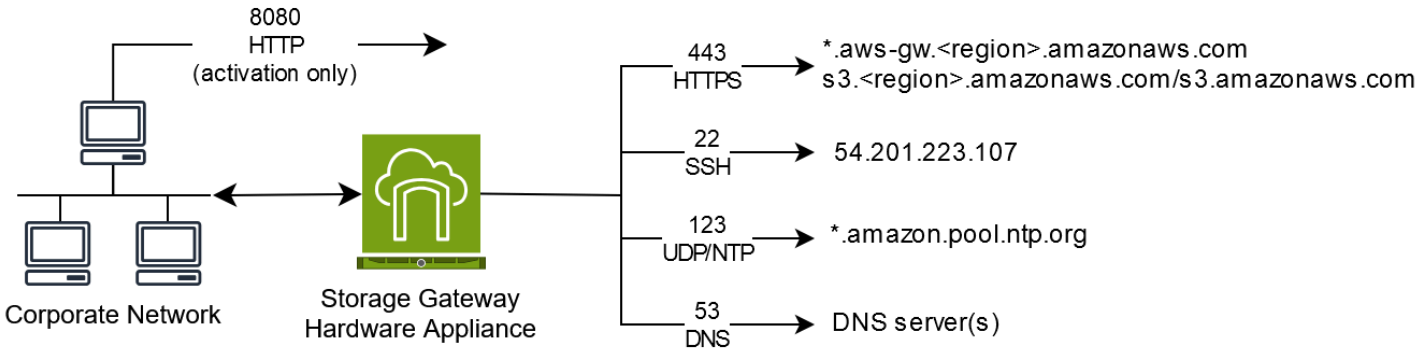
- Accès à Internet : une connexion réseau permanente à Internet via une interface réseau sur le serveur.
- Services DNS : des services DNS qui assurent la communication entre l'appliance matérielle et le serveur DNS.
- Synchronisation horaire : un service de temps Amazon NTP doit être accessible.
- Adresse 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.

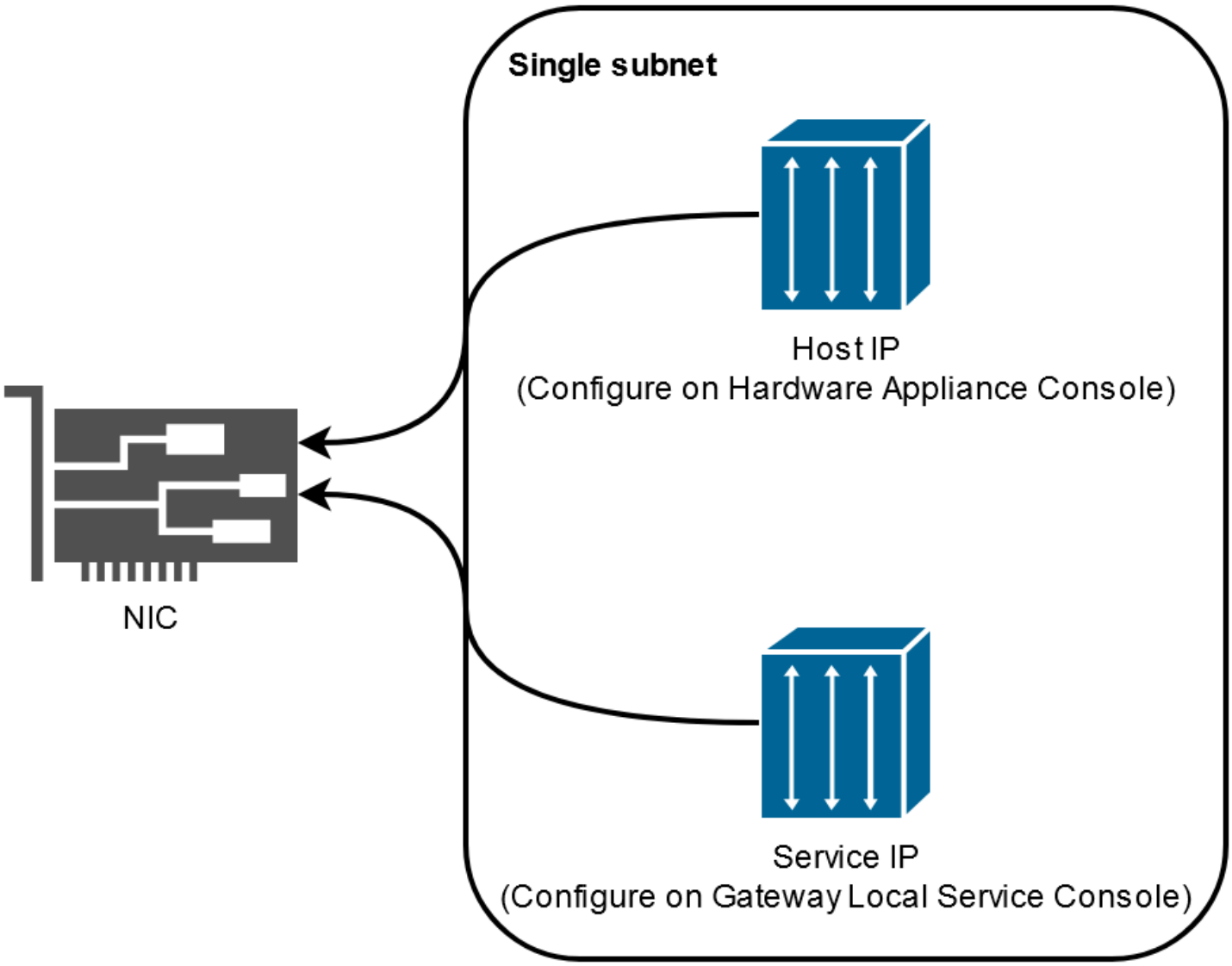
Protocole	Port	Direction	Source	Destination	Utilisation
SSH	22	Sortant	Appliance matérielle	`54.201.223.107`	canal de support
DNS	53	Sortant	Appliance matérielle	Serveurs DNS	Résolution de noms
UDP/NTP	123	Sortant	Appliance matérielle	`*.amazon.pool.ntp.org`	Synchronisation du temps
HTTPS	443	Sortant	Appliance matérielle	`*.amazonaws.com`	Transfert de données
HTTP	8080	Entrant	AWS	Appliance matérielle	Activation (brève)

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

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

> **Note**
>
> Pour accéder à une illustration de l'arrière du serveur avec ses ports, consultez Installation 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 en savoir plus sur l'activation et la configuration d'une appliance matérielle, consultez Utilisation de l'appliance matérielle 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 de service suivants pour communiquer avec AWS. Si vous utilisez un pare-feu ou un routeur pour filtrer ou limiter le trafic réseau, vous devez les configurer afin de permettre les communications sortantes 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**
>
> En fonction de AWS la région de votre passerelle, remplacez *region* le point de terminaison du service par la chaîne de région appropriée.

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
```

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

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

- Storage Gateway : pour 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 les AWS régions prises en charge que vous pouvez utiliser avec l'appliance matérielle, voir les régions de l'appliance matérielle Storage Gateway dans le. Références générales AWS

Configuration des groupes de sécurité pour votre instance Amazon EC2 Gateway

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

- Le groupe de sécurité ne doit pas autoriser les connexions entrantes en provenance d'Internet. Il doit autoriser uniquement les instances du groupe de sécurité de la passerelle à communiquer avec la passerelle. Si vous avez besoin d'autoriser les instances à se connecter à la passerelle en dehors de son groupe de sécurité, nous vous recommandons d'autoriser les connexions uniquement sur les ports 3260 (pour les connexions iSCSI) et 80 (pour l'activation).
- Si vous souhaitez activer votre passerelle depuis un EC2 hôte Amazon ne faisant pas partie du groupe de sécurité de 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 EC2 .

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

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

Pour obtenir des informations sur les ports à ouvrir pour votre passerelle, consultez Exigences pour les ports.

Hyperviseurs pris en charge et exigences pour l'hôte

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

> **Note**
>
> Lorsqu'un fabricant met fin à la prise en charge générale d'une version d'hyperviseur, Storage Gateway met également fin à la prise en charge de cette version. Pour obtenir des informations détaillées sur la prise en charge de versions spécifiques d'un hyperviseur, consultez la documentation du fabricant.

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.
- Microsoft Hyper-V Hypervisor (versions 2012 R2, 2016, 2019 ou 2022) – Une version autonome gratuite d'Hyper-V est disponible dans le Centre de téléchargement Microsoft. Pour cette configuration, vous aurez besoin d'un Microsoft Hyper-V Manager sur un ordinateur client Microsoft Windows pour vous connecter à l'hôte.
- 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 distributions CentOS/RHEL 7.7, Ubuntu 16.04 LTS et Ubuntu 18.04 LTS. Toute autre distribution Linux moderne peut fonctionner, mais l'interopérabilité ou les performances ne sont pas garanties. Nous recommandons cette option si vous disposez déjà d'un environnement KVM et que vous connaissez déjà le fonctionnement de KVM.
- EC2 Instance Amazon — Storage Gateway fournit une Amazon Machine Image (AMI) qui contient l'image de la machine virtuelle de la passerelle. Seuls les types de fichiers, de volumes mis en cache et de passerelle de bande peuvent être déployés sur Amazon EC2. Pour plus d'informations sur le déploiement d'une passerelle sur Amazon EC2, consultezDéployez une EC2 instance Amazon personnalisée pour Tape Gateway.
- Appliance matérielle Storage Gateway – fournit une appliance matérielle physique en tant qu'option de déploiement sur site pour les lieux ayant une infrastructure de machine virtuelle limitée.

> **Note**
>
> Storage Gateway ne prend pas en charge la restauration 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 à partir de votre Amazon EC2 AMI. 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.

Initiateurs iSCSI pris en charge

Lorsque vous déployez une passerelle de bande, celle-ci est préconfigurée avec un changeur de média et 10 lecteurs de bande. Ces lecteurs de bandes et le changeur média sont disponibles pour vos applications de sauvegarde client existantes en tant qu'appareils iSCSI.

Pour la connexion à ces appareils iSCSI, Storage Gateway prend en charge les initiateurs iSCSI suivants :

- Microsoft Windows Server 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- VMware ESX Initiator, qui fournit une alternative à l'utilisation d'initiateurs dans les systèmes d'exploitation clients de votre VMs

> **Important**
>
> Storage Gateway ne prend pas en charge MPIO à partir de clients Windows.
>
> Storage Gateway permet de connecter plusieurs hôtes au même volume, si les hôtes coordonnent leur accès en utilisant le cluster de basculement Windows Server (WSFC). Toutefois, la connexion de plusieurs hôtes au même volume (par exemple, le partage d'un système de fichiers NTFS/ext4 en mode non-cluster) ne peut se faire sans utiliser WSFC.

Applications de sauvegarde tierces prises en charge pour une passerelle de bande

Vous utilisez une application de sauvegarde pour lire, écrire et gérer les bandes avec une passerelle de bande. Le type de changeur de média que vous choisissez dépend de l’application de sauvegarde que vous comptez utiliser.

AWS a testé les applications de sauvegarde tierces présentées dans le tableau suivant afin de garantir leur compatibilité avec les fonctionnalités et fonctions de Tape Gateway suivantes :

- Fonctionnalités de découverte, notamment la connectivité à l'initiateur iSCSI, le changeur de support, le rescan, le mappage automatique et manuel des périphériques.
- Fonctions sur bande, notamment la création, la suppression, l'importation, l'exportation, l'inventaire et la visibilité des codes-barres.
- Effacement du contenu de la bande et vérification de l'absence de données dans les restaurations ultérieures.
- Sauvegarde des données sur une ou plusieurs bandes, vérification que les tâches de sauvegarde dépassant la capacité de la bande seront interrompues pour attendre l'arrivée de bandes supplémentaires.
- Restauration de données complètes ou partielles à partir de bandes magnétiques et vérification de l'intégrité des données.
- Vérification de la fonctionnalité et de l'intégrité des données après des événements d'arrêt et de redémarrage de la passerelle pendant les opérations de sauvegarde.

Application de sauvegarde	Version	Type de changeur de média	Version de passerelle testée
Arcserve Backup	19	Passerelle AWS-VTL	2.12.3
Bacula Enterprise	15,0.2	AWS-Gateway-VTL ou STK-L700	2.12.3
Commvault	2024E/11,36,35	STK-L700	2.12.3
Dell EMC NetWorker	19,10	Passerelle AWS-VTL	2.12.3

Application de sauvegarde	Version	Type de changeur de média	Version de passerelle testée
IBM Storage Protect	8,110	IBM-03584L32-0402	Tous
Protecteur de données Micro Focus	24,4	Passerelle AWS-VTL	2.12.3
Gestionnaire de protection des données Microsoft System Center	2025	STK-L700	2.12.3
NovaStor DataCenter	9.5.3	STK-L700	2.12.3
Quest NetVault Backup	13,3	STK-L700	2.12.3
Veeam Backup & Replication	12	Passerelle AWS-VTL	Tous
Veritas Backup Exec	24	Passerelle AWS-VTL	Tous
Veritas NetBackup	10.5	Passerelle AWS-VTL	2.12.3

Important

Nous vous recommandons vivement de choisir un changeur de média répertorié pour votre application de sauvegarde. Les autres changeurs de média risquent de ne pas fonctionner correctement. Une fois la passerelle activée, vous pouvez opter pour un changeur de média différent. Pour plus d'informations, consultez Sélection d'un changeur de média après l'activation de la passerelle.

Utilisation de l'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.

L'appareil Storage Gateway Hardware Appliance 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 à partir de 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 Storage Gateway est disponible pour activation et utilisation, consultez la section Régions de l'appliance matérielle 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 Storage Gateway.

Rubriques

- Configuration de votre appliance matérielle 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 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 de votre appliance matérielle Storage Gateway

Configuration 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 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 de votre appliance matérielle Storage Gateway.
4. Créez une passerelle sur votre appliance matérielle. Pour de plus amples informations, veuillez consulter Création et activation d'une passerelle de bande.

   Vous configurez les passerelles sur votre appliance matérielle de la même manière que vous configurez les passerelles sur VMware ESXi Microsoft Hyper-V, Linux Kernel-based Virtual Machine (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 SFP/SFP+ en cuivre 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 à un stockage cloud pratiquement illimité.

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).

Prérequis

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

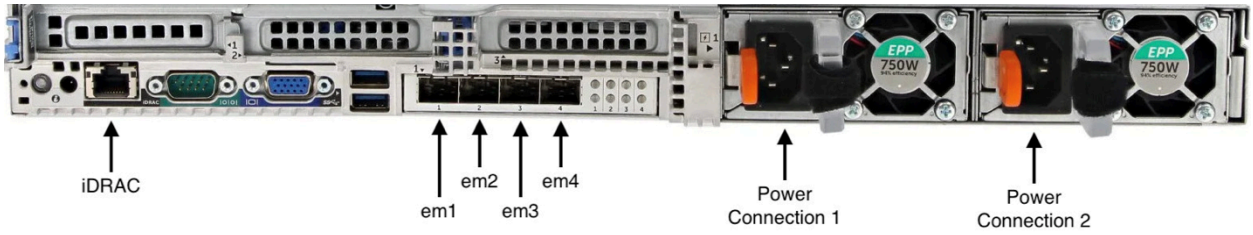
- Câble électriques : un obligatoire, deux recommandés.
- Câblage réseau pris en charge (en fonction de la carte d'interface réseau (NIC) incluse dans l'appliance matérielle). Câble DAC en cuivre Twinax, module optique SFP+ (compatible Intel) ou émetteur-récepteur cuivre SFP vers Base-T.
- Clavier et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

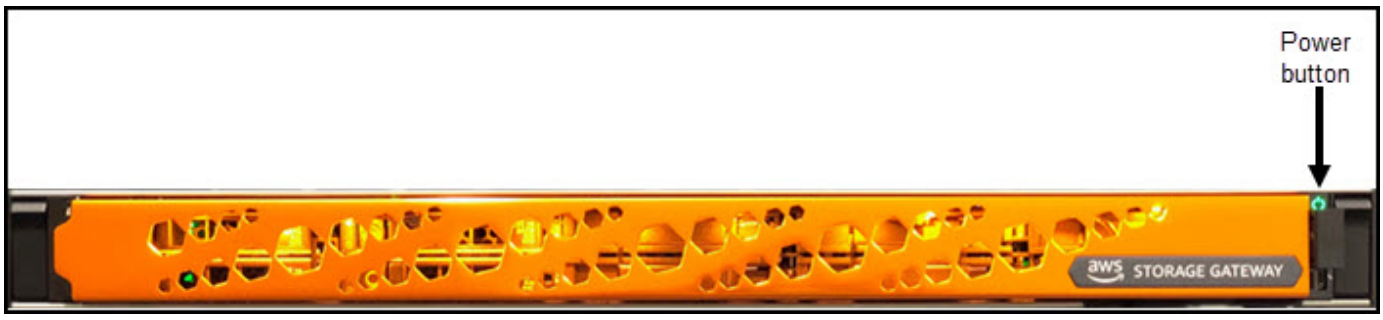


dispositif matériel, un à l'arrière, avec étiquettes de connexion réseau et d'alimentation.

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 à un stockage cloud pratiquement illimité.

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 relatives aux 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 à un stockage cloud pratiquement illimité.

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 auxquels votre appliance matérielle peut se connecter 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 `Enter` pour revenir à la page d'accueil.
2. Choisissez Déconnexion et appuyez `Enter` pour revenir à la page d'accueil.

Étape suivante

Activation de votre appliance matérielle Storage Gateway

Activation 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 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 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 la 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 de commandes de passerelle de stockage dans la console locale pour une passerelle 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 à partir de 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 .

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 de l'appliance matérielle 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 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 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 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' EC2 instance Amazon dans votre environnement AWS 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 et activation d'une passerelle de bande

Dans cette section, vous trouverez des instructions sur le téléchargement, le déploiement et l'activation d'une passerelle de bande.

Rubriques

- Configuration d'une passerelle de bande
- Connectez votre Tape Gateway à AWS
- Vérifier les paramètres et activer votre passerelle de bande
- Configurer votre passerelle de bande

Configuration d'une passerelle de bande

Pour configurer une passerelle de bande

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. Vous pouvez rechercher ce nom pour trouver votre passerelle sur les pages de liste de la console Storage Gateway.
    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 Passerelle de bande.
5. Dans la section Options de plateforme, procédez comme suit :
    a. Pour Plateforme hôte, choisissez la plateforme sur laquelle vous souhaitez déployer votre passerelle, puis suivez les instructions spécifiques à la plateforme, affichées sur la page de la console Storage Gateway, pour configurer votre plateforme hôte. Choisissez parmi les options suivantes :
        - VMware ESXi- Téléchargez, déployez et configurez la machine virtuelle de passerelle à l'aide de VMware ESXi.

- Microsoft Hyper-V : téléchargez, déployez et configurez la machine virtuelle de passerelle à l'aide de Microsoft Hyper-V.
- Linux KVM : téléchargez, déployez et configurez la machine virtuelle de la passerelle à l'aide de Linux KVM.
- Amazon EC2 - Configurez et lancez une EC2 instance Amazon pour héberger votre passerelle. Cette option n'est pas disponible pour les passerelles de Volume stocké.
- Appliance matérielle : commandez une appliance matérielle physique dédiée AWS auprès de laquelle 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. Dans la section Paramètres de l'application de sauvegarde, pour Application de sauvegarde, choisissez l'application que vous souhaitez utiliser pour sauvegarder les données de vos bandes vers les bandes virtuelles associées à votre passerelle de bande.
7. Choisissez Suivant pour continuer.

Maintenant que votre passerelle est configurée, vous devez choisir la manière dont vous souhaitez qu'elle se connecte et communique avec elle AWS. Pour obtenir des instructions, reportez-vous à la section Connect your Tape Gateway to AWS.

Connectez votre Tape Gateway à AWS

Pour connecter une nouvelle Tape Gateway à AWS

1. Suivez la procédure décrite dans Configuration d'une passerelle de bande si ce n'est pas déjà fait. Lorsque vous avez terminé, sélectionnez Suivant pour ouvrir la page Connexion à AWS dans la console Storage Gateway.
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 FIPS activé pour indiquer si la connexion doit être conforme aux normes fédérales de traitement de l'information (FIPS).

> **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 de service FIPS n'est disponible que dans certaines régions AWS . Pour plus d'informations, consultez Points de terminaison et quotas Storage Gateway dans le document Références générales AWS.

- Hébergé par VPC : votre passerelle communique avec AWS via une connexion privée avec votre VPC, ce qui vous permet de contrôler les paramètres de votre réseau. Si vous sélectionnez cette option, vous devez spécifier un point de terminaison de VPC existant en choisissant l'ID du point de terminaison de VPC dans le menu déroulant, ou en fournissant le nom DNS ou l'adresse IP du point de terminaison de VPC. Pour plus d'informations, consultez Activation de votre passerelle dans un cloud privé virtuel.

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 des détails de votre EC2 instance Amazon.

   - 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. Choisissez cette option si l'adresse IP de votre passerelle n'est pas disponible.

4. Choisissez Suivant pour continuer.

Maintenant que vous avez choisi le mode de connexion de votre passerelle AWS, vous devez l'activer. Pour obtenir des instructions, consultez Vérifier les paramètres et activer votre passerelle de bande.

Vérifier les paramètres et activer votre passerelle de bande

Pour activer une nouvelle passerelle de bande

1. Suivez les procédures décrites dans les rubriques suivantes si vous ne l'avez pas déjà fait :

   - Configuration d'une passerelle de bande
   - Connectez votre Tape Gateway à AWS

   Lorsque vous avez terminé, choisissez Suivant pour ouvrir la page Vérifier et activer dans la console Storage Gateway.
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.

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

Maintenant que vous avez activé votre passerelle, vous devez effectuer une première configuration pour allouer des disques de stockage locaux et configurer la journalisation. Pour obtenir des instructions, consultez Configurer votre passerelle de bande.

Configurer votre passerelle de bande

Pour effectuer la première configuration sur nouvelle passerelle de bande

1. Suivez les procédures décrites dans les rubriques suivantes si vous ne l'avez pas déjà fait :

   - Configuration d'une passerelle de bande
   - Connectez votre Tape Gateway à AWS
   - Vérifier les paramètres et activer votre passerelle de bande

Lorsque vous avez terminé, sélectionnez Suivant pour ouvrir la page Configurer la passerelle dans la console Storage Gateway.

2. Dans la section Configurer le stockage, utilisez les menus déroulants pour allouer au moins un disque d'une capacité d'au moins 165 Gio pour le STOCKAGE EN CACHE, et au moins un disque d'une capacité d'au moins 150 Gio pour le TAMPON DE CHARGEMENT. 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 le menu déroulant correspondant.
   - 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 la 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 vous informer des indicateurs 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 : ne recevez aucune CloudWatch notification concernant les 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 Storage Gateway. Répétez cette étape pour ajouter autant de balises que vous désirez.

6. Choisissez Configurer pour terminer la création de votre passerelle.

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

Maintenant que vous avez créé votre passerelle, vous devez créer des bandes virtuelles qu'elle pourra utiliser. Pour obtenir des instructions, consultez Création de bandes.

Création de nouvelles bandes virtuelles pour Tape Gateway

Cette section décrit comment créer de nouvelles bandes virtuelles à l'aide de AWS Storage Gateway. Vous pouvez créer de nouvelles bandes virtuelles manuellement à l'aide de la AWS Storage Gateway console ou de l'API Storage Gateway. Vous pouvez également configurer votre passerelle de bande pour les créer automatiquement, ce qui permet de réduire le besoin de gestion manuelle des bandes, de simplifier vos déploiements de grande envergure et d'adapter les besoins de stockage sur site et d'archivage.

La passerelle de bande prend en charge la bandes à inscription unique et lecture multiple (WORM) et le verrouillage de rétention de bande sur les bandes virtuelles. Les bandes virtuelles activées par WORM permettent de garantir que les données des bandes actives de votre bibliothèque de bandes virtuelles ne peuvent pas être remplacées ou effacées. Pour plus d'informations sur la protection WORM pour les bandes virtuelles, reportez-vous à la section suivante,the section called "Protection de bande WORM".

Grâce au verrouillage de rétention de bande, vous pouvez définir le mode et la durée de conservation des bandes virtuelles archivées, empêchant ainsi leur suppression pendant une durée fixe pouvant aller jusqu'à 100 ans. Cela inclut les contrôles d'autorisation permettant de déterminer qui peut supprimer des bandes ou modifier les paramètres de rétention. Pour plus d'informations sur le verrouillage de rétention de bande, consultez the section called "Verrouillage de rétention de bande".

> **Note**
>
> Vous êtes facturé uniquement pour la quantité de données que vous écrivez sur la bande, pas pour la capacité de la bande.
> Vous pouvez utiliser AWS Key Management Service (AWS KMS) pour chiffrer des données écrites sur une bande virtuelle stockée dans Amazon Simple Storage Service (Amazon

S3). Actuellement, vous pouvez le faire en utilisant l' AWS Storage Gateway API ou AWS Command Line Interface (AWS CLI). Pour plus d'informations, reportez-vous CreateTapesà la section Create-tapes.

Protection de bande à inscription unique et lecture multiple (WORM)

Vous pouvez empêcher le remplacement ou l'effacement de bandes virtuelles en activant la protection WORM pour les bandes virtuelles dans AWS Storage Gateway. La protection WORM pour les bandes virtuelles est activée lors de la création de bandes.

Les données écrites sur des bandes virtuelles WORM ne peuvent pas être remplacées. Seules de nouvelles données peuvent être ajoutées aux bandes virtuelles WORM, et les données existantes ne peuvent pas être effacées. L'activation de la protection WORM pour les bandes virtuelles permet de protéger ces bandes pendant leur utilisation active, avant qu'elles ne soient éjectées et archivées.

La configuration WORM ne peut être définie que lors de la création de bandes et cette configuration ne peut pas être modifiée une fois les bandes créées.

Création manuelle de bandes

Vous pouvez créer de nouvelles bandes virtuelles manuellement à l'aide de la AWS Storage Gateway console ou de l'API Storage Gateway. La console offre une interface pratique pour la création de bandes, offrant la possibilité de spécifier un préfixe pour un code-barres généré de manière aléatoire. Si vous devez personnaliser entièrement les codes-barres de vos bandes (par exemple, pour qu'ils correspondent au numéro de série d'une bande physique correspondante), vous devez utiliser l'API. Pour plus d'informations sur la création de bandes à l'aide de l'API Storage Gateway, reportez-vous CreateTapeWithBarcodeau manuel Storage Gateway API Reference.

Pour créer des bandes virtuelles manuellement à l'aide de la console Storage Gateway ou de l'API Storage Gateway.

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez l'onglet Passerelles.
3. Choisissez Créer des bandes pour ouvrir le volet Créer une bande.
4. Pour Passerelle, choisissez une passerelle. La bande est créée pour cette passerelle.

5. Pour le Type de bande, choisissez Standard pour créer des bandes virtuelles standard. Choisissez WORM pour créer des bandes virtuelles à inscription unique et lecture multiple (WORM). Pour plus d'informations, consultez la section Protection des bandes à inscription unique et lecture multiple (WORM).
6. Pour Number of tapes (Nombre de bandes), choisissez le nombre de bandes que vous souhaitez créer. Pour plus d'informations sur les quotas de bande, consultez AWS Storage Gateway quotas.
7. Pour Capacity (Capacité), entrez la taille de la bande virtuelle que vous souhaitez créer. La taille des bandes doit être supérieure à 100 Gio. Pour plus d'informations sur les quotas de capacité, consultez AWS Storage Gateway quotas.
8. Pour Barcode prefix (Préfixe de code-barres), entrez le préfixe que vous souhaitez ajouter au code à barres de vos bandes virtuelles.

   > **Note**
   >
   > Les bandes virtuelles sont identifiées de manière unique par un code-barres et vous pouvez ajouter un préfixe à ce dernier. Vous pouvez utiliser un préfixe pour vous aider à identifier des bandes virtuelles. Le préfixe doit être en majuscules (A-Z) et comporter entre un et quatre caractères.

9. Pour Groupe, choisissez Groupe Glacier, Groupe Deep Archive ou un groupe personnalisé que vous avez créé. Le groupe définit la classe de stockage dans laquelle votre bande est stockée lorsqu'elle est éjectée par votre logiciel de sauvegarde.

   - Choisissez Groupe Glacier si vous souhaitez archiver la bande dans la classe de stockage S3 Glacier Flexible Retrieval. Lorsque le logiciel de sauvegarde éjecte la bande, elle est automatiquement archivée dans S3 Glacier Flexible Retrieval. Vous utilisez S3 Glacier Flexible Retrieval pour des archives plus actives, au sein desquelles vous pouvez récupérer une bande dans un délai compris entre 3 et 5 heures. Pour plus d'informations, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.
   - Choisissez Groupe Deep Archive si vous souhaitez archiver la bande dans la classe de stockage S3 Glacier Deep Archive. Lorsque le logiciel de sauvegarde éjecte la bande, celle-ci est automatiquement archivée dans S3 Glacier Deep Archive. Vous utilisez S3 Glacier Deep Archive pour la conservation des données à long terme et l'archivage numérique où les données sont consultées une à deux fois par an. Vous pouvez extraire une bande

archivée dans S3 Glacier Deep Archive généralement dans un délai de 12 heures. Pour plus d'informations, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.

- Choisissez un groupe personnalisé, si disponible. Vous configurez des groupes de bandes personnalisés pour utiliser le Groupe Deep Archive ou le Groupe Glacier. Les bandes sont archivées dans la classe de stockage configurée lorsqu'elles sont éjectées par votre logiciel de sauvegarde.

Si vous archivez une bande dans S3 Glacier Flexible Retrieval, vous pouvez la déplacer vers S3 Glacier Deep Archive ultérieurement. Pour plus d'informations, consultez Déplacement de bandes vers la classe de stockage S3 Glacier Deep Archive.

> **Note**
>
> Les bandes créées avant le 27 mars 2019 sont archivées directement dans S3 Glacier Flexible Retrieval lorsque le logiciel de sauvegarde les éjecte.

10. (Facultatif) Pour les Balises, choisissez Ajouter une nouvelle balise et entrez une clé et une valeur pour ajouter des balises à votre bande. Une balise est une paire clé-valeur sensible à la casse qui vous aide à gérer, filtrer et rechercher vos bandes.
11. Choisissez Créer des bandes.
12. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.

L'état des bandes virtuelles est défini initialement sur CRÉATION lorsque les bandes virtuelles sont créées. Une fois les bandes créées, leur état passe à DISPONIBLE. Pour de plus amples informations, veuillez consulter Comprendre l'état de la bande.

Autoriser la création automatique de bandes

La passerelle de bande crée automatiquement de nouvelles bandes virtuelles pour conserver le nombre minimal de bandes disponibles que vous configurez. Elle rend ensuite ces nouvelles bandes

disponibles pour l'importation par l'application de sauvegarde, afin que vos tâches de sauvegarde puissent s'exécuter sans interruption. Autoriser la création automatique de bandes élimine le besoin de créer des scripts personnalisés en plus du processus manuel de création de bandes virtuelles.

La passerelle de bande génère automatiquement une nouvelle bande lorsqu'il contient moins de bandes que le nombre minimum de bandes disponibles spécifié pour la création automatique de bandes. Une nouvelle bande est générée lorsque :

- Une bande est importée depuis un emplacement d'importation/exportation.
- Une bande est importée sur le lecteur de bande.

La passerelle gère un nombre minimum de bandes avec le préfixe de code-barres spécifié dans la politique de création automatique de bandes. S'il y a moins de bandes que le nombre minimum de bandes avec le préfixe de code-barres, la passerelle crée automatiquement suffisamment de nouvelles bandes pour atteindre le nombre minimum de bandes spécifié dans la politique de création automatique de bandes.

Lorsque vous éjectez une bande et qu'elle entre dans le import/export slot, that tape does not count toward the minimum number of tapes specified in your automatic tape creation policy. Only tapes in the import/export slot, vous êtes considérée comme « disponible ». L'exportation d'une bande ne déclenche pas la création automatique de bande. Seules les importations ont une incidence sur le nombre de bandes disponibles.

Déplacer une cassette de son import/export slot to a tape drive or storage slot reduces the number of tapes in the import/export emplacement avec le même préfixe de code-barres. La passerelle crée de nouvelles bandes afin de maintenir le nombre minimum de bandes disponibles pour ce préfixe de code-barres.

Pour autoriser la création automatique de bandes

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez l'onglet Passerelles.
3. Choisissez la passerelle pour laquelle vous souhaitez créer automatiquement des bandes.
4. Dans le menu Actions, choisissez Configure tape auto-create (Configurer la création automatique de bandes).

La page Création automatique de bandes s'affiche. Vous pouvez ajouter, modifier ou supprimer les options de création automatique de bandes ici.

5. Pour autoriser la création automatique de bandes, choisissez Ajouter un nouvel élément, puis configurez les paramètres de création automatique de bandes.
6. Pour le Type de bande, choisissez Standard pour créer des bandes virtuelles standard. Choisissez WORM pour créer des bandes virtuelles write-once-read-many(WORM). Pour plus d'informations, consultez la section Protection des bandes à inscription unique et lecture multiple (WORM).
7. Pour Nombre minimum de bandes, entrez le nombre minimum de bandes virtuelles qui doivent être disponibles sur la passerelle de bande à tout moment. La plage valable pour cette valeur va de 1 à 10.
8. Pour Capacity (Capacité), entrez la taille, en octets, de la capacité de bande virtuelle. La plage valable pour cette valeur va de 100 Gio à 15 Tio.
9. Pour Barcode prefix (Préfixe de code-barres), entrez le préfixe que vous souhaitez ajouter au code à barres de vos bandes virtuelles.

   > **Note**
   >
   > Les bandes virtuelles sont identifiées de manière unique par un code-barres et vous pouvez ajouter un préfixe à ce dernier. Le préfix est facultatif, mais vous pouvez l'utiliser pour faciliter l'identification de vos bandes virtuelles. Le préfixe doit être en majuscules (A-Z) et comporter entre un et quatre caractères.

10. Pour Groupe, choisissez Groupe Glacier, Groupe Deep Archive ou un groupe personnalisé que vous avez créé. Le groupe définit la classe de stockage dans laquelle votre bande est stockée lorsqu'elle est éjectée par votre logiciel de sauvegarde.

    - Choisissez Groupe Glacier si vous souhaitez archiver la bande dans la classe de stockage S3 Glacier Flexible Retrieval. Lorsque le logiciel de sauvegarde éjecte la bande, elle est automatiquement archivée dans S3 Glacier Flexible Retrieval. Vous utilisez S3 Glacier Flexible Retrieval pour des archives plus actives, au sein desquelles vous pouvez récupérer une bande dans un délai compris entre 3 et 5 heures. Pour plus d'informations, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.

- Choisissez Groupe Deep Archive si vous souhaitez archiver la bande dans la classe de stockage S3 Glacier Deep Archive. Lorsque le logiciel de sauvegarde éjecte la bande, celle-ci est automatiquement archivée dans S3 Glacier Deep Archive. Vous utilisez S3 Glacier Deep Archive pour la conservation des données à long terme et l'archivage numérique où les données sont consultées une à deux fois par an. Vous pouvez extraire une bande archivée dans S3 Glacier Deep Archive généralement dans un délai de 12 heures. Pour plus d'informations, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.
- Choisissez un groupe personnalisé, si disponible. Vous configurez des groupes de bandes personnalisés pour utiliser le Groupe Deep Archive ou le Groupe Glacier. Les bandes sont archivées dans la classe de stockage configurée lorsqu'elles sont éjectées par votre logiciel de sauvegarde.

Si vous archivez une bande dans S3 Glacier Flexible Retrieval, vous pouvez la déplacer vers S3 Glacier Deep Archive ultérieurement. Pour plus d'informations, consultez Déplacement de bandes vers la classe de stockage S3 Glacier Deep Archive.

> **Note**
>
> Les bandes créées avant le 27 mars 2019 sont archivées directement dans S3 Glacier Flexible Retrieval lorsque le logiciel de sauvegarde les éjecte.

11. Lorsque vous avez terminé de configurer les paramètres, choisissez Enregistrer les modifications.
12. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.

    L'état des bandes virtuelles disponibles est défini initialement sur CRÉATION lorsque les bandes sont créées. Une fois les bandes créées, leur état passe à DISPONIBLE. Pour de plus amples informations, veuillez consulter Comprendre l'état de la bande.

Pour plus d'informations sur la modification des politiques de création automatique de bandes ou sur la suppression de la création automatique de bandes à partir d'une passerelle de bande, consultez Gestion de la création automatique de bandes.

Étape suivante

Utilisation de votre passerelle de bande

Création d'un groupe de bandes personnalisé

Cette section décrit comment créer un nouveau groupe de bandes personnalisé dans AWS Storage Gateway.

Rubriques

- Choix d'un type de groupe de bandes
- Utilisation d'un verrouillage de rétention de bande
- Création d'un groupe de bandes personnalisé

Choix d'un type de groupe de bandes

AWS Storage Gateway utilise des pools de bandes pour déterminer la classe de stockage dans laquelle vous souhaitez que les bandes soient archivées lorsqu'elles sont éjectées. Storage Gateway propose deux groupes de bandes standard :

- Groupe Glacier : archive la bande dans la classe de stockage S3 Glacier Flexible Retrieval. Lorsque le logiciel de sauvegarde éjecte la bande, elle est automatiquement archivée dans S3 Glacier Flexible Retrieval. Vous utilisez S3 Glacier Flexible Retrieval pour des archives plus actives, au sein desquelles vous pouvez récupérer les bandes dans un délai compris entre 3 et 5 heures. Pour plus d'informations, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.
- Groupe Deep Archive : archive la bande dans la classe de stockage S3 Glacier Deep Archive. Lorsque le logiciel de sauvegarde éjecte la bande, celle-ci est automatiquement archivée dans S3 Glacier Deep Archive. Vous utilisez S3 Glacier Deep Archive pour la conservation des données à long terme et l'archivage numérique où les données sont consultées une à deux fois par an. Vous pouvez extraire les bandes archivées dans S3 Glacier Deep Archive généralement dans un

délai de 12 heures. Pour obtenir des informations détaillées, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.

Si vous archivez une bande dans S3 Glacier Flexible Retrieval, vous pouvez la déplacer vers S3 Glacier Deep Archive ultérieurement. Pour plus d'informations, consultez Déplacement de bandes vers la classe de stockage S3 Glacier Deep Archive.

Storage Gateway prend également en charge la création de groupes de bandes personnalisés, qui vous permettent d'activer le verrouillage de rétention des bandes afin d'empêcher la suppression ou le déplacement des bandes archivées vers un autre groupe pendant une durée déterminée, jusqu'à 100 ans. Cela inclut le verrouillage des contrôles d'autorisation permettant de déterminer qui peut supprimer des bandes ou modifier les paramètres de rétention.

Utilisation d'un verrouillage de rétention de bande

Grâce au verrouillage de rétention de bande, vous pouvez verrouiller les bandes archivées. Le verrouillage de rétention de bande est une option pour les bandes d'un groupe de bandes personnalisé. Les bandes sur lesquelles le verrouillage de rétention de bande est activé ne peuvent pas être supprimées ou déplacées vers un autre groupe pendant une durée déterminée, allant jusqu'à 100 ans.

Vous pouvez configurer le verrouillage de rétention de bande dans l'un des deux modes suivants :

- Mode de gouvernance : lorsqu'il est configuré en mode gouvernance, seuls les utilisateurs AWS Identity and Access Management (IAM) disposant des autorisations nécessaires `storagegateway:BypassGovernanceRetention` peuvent retirer des bandes du pool. Si vous utilisez l' AWS Storage Gateway API pour retirer la bande, vous devez également `BypassGovernanceRetention` définir sur`true`.
- Mode de conformité : lorsqu'elle est configurée en mode de conformité, la protection ne peut être supprimée par aucun utilisateur, y compris le Compte AWS racine.

  Lorsqu'un objet est verrouillé en mode de conformité, son type de verrouillage de rétention ne pas être modifié et sa période de rétention ne peut pas être raccourcie. Le type de verrouillage en mode de conformité garantit qu'une bande ne peut pas être écrasée ou supprimée pendant la durée de la période de rétention.

> **Important**
>
> La configuration d'un groupe personnalisé ne peut pas être modifiée après sa création.

Vous pouvez activer le verrouillage de rétention de bande lorsque vous créez un groupe de bandes personnalisé. Toutes les nouvelles bandes connectées à un groupe personnalisé héritent du type de verrou de rétention, de la période et de la classe de stockage de ce groupe.

Vous pouvez également activer le verrouillage de rétention de bande sur les bandes archivées avant le lancement de cette fonctionnalité en déplaçant les bandes entre le groupe par défaut et le groupe personnalisé que vous créez. Si la bande est archivée, le verrouillage de rétention de bande prend effet immédiatement.

> **Note**
>
> Si vous déplacez des bandes archivées entre les classes de stockage S3 Glacier Deep Archive et S3 Glacier Deep Archive, des frais vous sont facturés pour le déplacement d'une bande. Le déplacement d'une bande d'un groupe par défaut vers un groupe personnalisé est gratuit si la classe de stockage reste la même.

Création d'un groupe de bandes personnalisé

Suivez les étapes suivantes créer un groupe de bandes personnalisé à l'aide de la console AWS Storage Gateway .

Pour créer un groupe de bandes personnalisé

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez la Bibliothèque de bandes et choisissez Groupes pour afficher les groupes disponibles.
3. Choisissez Créer un groupe pour ouvrir le volet Créer un groupe.
4. Dans Nom, entrez un nom unique pour identifier votre groupe de bandes personnalisé. Le nom doit comporter entre 2 et 100 caractères.
5. Pour la Classe de stockage, choisissez Glacier ou Glacier Deep Archive.

6. Pour le Type de verrouillage de rétention, choisissez Aucun, Conformité ou Gouvernance.

> **Note**
>
> Si vous choisissez Conformité, le verrouillage de rétention de bande ne peut être supprimé par aucun utilisateur, y compris le Compte AWS racine.

7. Si vous choisissez un type de verrouillage de rétention de bande, entrez la Période de rétention en jours. La période de rétention maximale est de 36 500 jours (100 ans).
8. (Facultatif) Pour les Balises, choisissez Ajouter une nouvelle balise pour ajouter une balise à votre groupe de bandes personnalisé. Une balise est une paire clé-valeur sensible à la casse qui vous aide à gérer, filtrer et rechercher votre groupes de bandes personnalisé.

   Saisissez une Clé et, éventuellement, une Valeur pour la balise. Vous pouvez ajouter jusqu'à 50 balises au groupe de bandes.
9. Choisissez Créer un groupe pour créer votre nouveau groupe de bandes personnalisé.

Connexion de vos appareils VTL

Vous trouverez ci-dessous des instructions sur la connexion de vos appareils VTL (Virtual Tape Library) à votre client Microsoft Windows ou Red Hat Enterprise Linux (RHEL).

Rubriques

- Connexion à un client Microsoft Windows
- Connexion à un client Linux

Connexion à un client Microsoft Windows

La procédure suivante présente un résumé des étapes à suivre pour vous connecter à un client Windows.

Pour connecter vos appareils VTL à un client Windows

1. Démarrer `iscsicpl.exe`.

> **Note**
>
> Vous devez avoir des droits d'administrateur sur l'ordinateur client pour pouvoir exécuter l'initiateur iSCSI.

2. Démarrez le service de l'initiateur Microsoft iSCSI.
3. Dans la boîte de dialogue iSCSI Initiator Properties (Propriétés de l'initiateur iSCSI), choisissez l'onglet Discovery (Découverte), puis sélectionnez Discover Portal (Découvrir le portail).
4. Indiquez l'adresse IP de votre passerelle de bande pour l'Adresse IP ou le nom DNS.
5. Choisissez l'onglet Cibles, puis sélectionnez Actualiser. Les dix lecteurs de bandes et le changeur de média apparaissent dans la zone Cibles découvertes. L'état des cibles est Inactif.
6. Sélectionnez le premier appareil et connectez-le. Vous connectez les appareils un à la fois.
7. Connectez toutes les cibles.

Sur un client Windows, le fournisseur de pilotes pour le lecteur de bandes doit être Microsoft. Utilisez la procédure suivante pour vérifier le fournisseur de pilotes et mettez à jour le pilote et le fournisseur si nécessaire:

Pour vérifier et mettre à jour le pilote et fournisseur

1. Sur le client Windows, démarrez le gestionnaire d'appareils.
2. Développez Lecteurs de bande, ouvrez le menu contextuel (clic droit) d'un lecteur de bandes, puis sélectionnez Propriétés.
3. Dans l'onglet Pilote de la boîte de dialogue Propriétés de l'appareil, vérifiez que le Fournisseur de pilote est Microsoft.
4. Si le Fournisseur de pilote n'est pas Microsoft, définissez la valeur comme suit :
    a. Choisissez Mettre à jour le pilote.
    b. Dans la boîte de dialogue Mettre à jour le pilote, choisissez Parcourir mon ordinateur pour rechercher le logiciel du pilote.
    c. Dans la boîte de dialogue Mettre à jour le logiciel de pilote, sélectionnez Me laisser choisir parmi une liste de pilotes d'appareils sur mon ordinateur.
    d. Sélectionnez Lecteur de bandes LTO, puis choisissez Suivant.

5. Choisissez Fermer pour fermer la fenêtre Mettre à jour le logiciel de pilote et vérifiez que la valeur du Fournisseur de pilote est maintenant définie sur Microsoft.
6. Répétez ces étapes pour mettre à jour le pilote et le fournisseur pour tous les lecteurs de bandes.

Connexion à un client Linux

La procédure suivante présente un résumé des étapes à suivre pour vous connecter à un client RHEL.

Pour connecter un client Linux aux appareils VTL

1. Installez le package RPM `iscsi-initiator-utils`.

   Vous pouvez utiliser la commande suivante pour installer le package.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. Veillez à ce que le démon iSCSI soit en cours d'exécution.

   Pour RHEL 8 ou 9, utilisez la commande suivante.

   ```
   sudo service iscsid status
   ```

3. Découvrez le volume ou les cibles d'appareils VTL définis pour une passerelle. Utilisez la commande de découverte suivante.

   ```
   sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
   ```

   Le résultat de la commande de découverte ressemble à l'exemple de sortie suivant.

   Pour les passerelles de volume : *[GATEWAY_IP]*`:3260, 1 iqn.1997-05.com.amazon:myvolume`

   Pour les passerelles de bande : `iqn.1997-05.com.amazon:`*[GATEWAY_IP]*`-tapedrive-01`

4. Connectez-vous à une cible.

   Assurez-vous de spécifier le bon *[GATEWAY_IP]* IQN dans la commande de connexion.

Utilisez la commande suivante de l'.

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Vérifiez que le volume est attaché à l'ordinateur client (l'initiateur). Pour cela, utilisez la commande suivante.

```
ls -l /dev/disk/by-path
```

La sortie de la commande doit ressembler à celle de l'exemple suivant.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

Pour les passerelles de volume, une fois que vous avez configuré votre initiateur, nous vous recommandons vivement de personnaliser vos paramètres iSCSI comme indiqué dans Personnalisation de vos paramètres iSCSI Linux.

Vérifiez que l'appareil de VTL est attaché à la machine client (l'initiateur). Pour cela, utilisez la commande suivante.

```
ls -l /dev/tape/by-path
```

La sortie de la commande doit ressembler à celle de l'exemple suivant.

```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
```

```
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-lun-0
 -> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-
lun-0-nst -> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-lun-0
 -> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-
lun-0-nst -> ../../nst1
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-lun-0
 -> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-
lun-0-nst -> ../../nst2
```

```
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-lun-0
 -> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-
lun-0-nst -> ../../nst5
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-lun-0
 -> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-
lun-0-nst -> ../../nst3
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-lun-0
 -> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-
lun-0-nst -> ../../nst4
```

Étape suivante

Utilisation d'un logiciel de sauvegarde pour tester la configuration de votre passerelle

Utilisation de votre logiciel de sauvegarde pour tester la configuration de votre passerelle

Pour tester la configuration de la passerelle de bande effectuez les tâches suivantes à l'aide de votre application de sauvegarde :

1. Configurez l'application de sauvegarde afin de détecter vos périphériques de stockage.

> **Note**
>
> Pour améliorer les performances des E/S, nous recommandons de configurer la taille du bloc des lecteurs de bandes dans votre application de sauvegarde sur 1 Mo. Pour plus d'informations, consultez Utiliser une taille de bloc supérieure pour les lecteurs de bandes.

2. Sauvegardez les données sur une bande.
3. Archivez la bande.
4. Récupérez la bande dans l'archive.
5. Restaurez les données de la bande.

Pour tester votre configuration, utilisez une application de sauvegarde compatible, comme indiqué ci-dessous.

> **Note**
>
> Sauf indication contraire, toutes les applications de sauvegarde ont été qualifiées sur Microsoft Windows.

Pour plus d'informations sur les applications de sauvegarde compatibles, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Test de votre configuration à l'aide d'Arcserve Backup
- Test de votre configuration à l'aide de Bacula Enterprise
- Test de votre configuration à l'aide de Commvault
- Test de votre configuration à l'aide de Dell EMC NetWorker
- Test de votre configuration à l'aide d'IBM Data Protect
- Test de votre configuration à l'aide de OpenText Data Protector
- Test de votre configuration à l'aide de Microsoft System Center DPM
- Tester votre configuration en utilisant NovaStor DataCenter
- Test de votre configuration à l'aide de Quest NetVault Backup
- Tester votre configuration à l'aide de Veeam Backup and Replication
- Test de votre configuration à l'aide de Veritas Backup Exec
- Tester votre configuration à l'aide de Veritas NetBackup

Test de votre configuration à l'aide d'Arcserve Backup

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer vos périphériques VTL (Virtual Tape Library) à l'aide d'Arcserve Backup. Dans cette rubrique, vous trouverez une documentation de base pour configurer Arcserve Backup avec une passerelle de bande et réaliser une opération de sauvegarde et de restauration. Pour des informations détaillées sur l'utilisation d'Arcserve Backup, reportez-vous à la documentation Arcserve Backup.

Rubriques

- Configuration d'Arcserve pour utiliser les appareils VTL
- Chargement de bandes dans un pool de médias
- Sauvegarde de données sur une bande
- Archivage d'une bande
- Restauration des données d'une bande

Configuration d'Arcserve pour utiliser les appareils VTL

Une fois que vous avez connecté vos appareils de la bibliothèque de bandes virtuelles (VTL) à votre client, recherchez vos appareils.

Pour rechercher des appareils VTL

1. Dans le gestionnaire de sauvegarde Arcserve, choisissez le menu Utilities (Utilitaires).
2. Choisissez Media Assure and Scan (Protection et analyse des médias).

Chargement de bandes dans un pool de médias

Lorsque le logiciel Arcserve se connecte à votre passerelle et que vos bandes deviennent disponibles, Arcserve charge automatiquement ces dernières. Si votre passerelle n'apparaît pas dans le logiciel Arcserve, essayez de redémarrer le moteur de bandes dans Arcserve.

Pour redémarrer le moteur de bandes

1. Choisissez Quick Start (Démarrage rapide), Administration, puis Device (Périphérique).
2. Dans le menu de navigation, cliquez avec le bouton droit sur votre passerelle, puis choisissez un emplacement d'importation/exportation.
3. Choisissez Quick Import (Importation rapide) et affectez votre bande à un emplacement vide.
4. Ouvrez le menu contextuel (clic droit) de la passerelle, puis choisissez Inventory/Offline Slots (Inventaire/Emplacements hors connexion).
5. Sélectionnez Quick Inventory (Inventaire rapide) pour récupérer les informations de média à partir de la base de données.

Si vous ajoutez une bande, vous devez analyser votre passerelle afin de localiser la nouvelle bande pour qu'elle s'affiche dans Arcserve. Si les nouvelles bandes ne s'affichent pas, vous devez importer les bandes.

Pour importer des bandes

1. Choisissez le menu Quick Start (Démarrage rapide), puis Back up (Sauvegarder) et enfin Destination tap (Bande de destination).
2. Choisissez votre passerelle, ouvrez le menu contextuel (clic droit) d'une bande et choisissez Import/Export Slot (Emplacement d'importation/exportation).
3. Ouvrez le menu contextuel (clic droit) de chaque bande et choisissez Inventory (Inventaire).
4. Ouvrez le menu contextuel (clic droit) de chaque nouvelle bande et choisissez Format (Formater).

Le code-barres de chaque bande s'affiche maintenant dans votre console Storage Gateway et chaque bande est prête à être utilisée.

Sauvegarde de données sur une bande

Lorsque vos bandes ont été chargées dans Arcserve, vous pouvez y sauvegarder des données. Le processus de sauvegarde est le même que celui de la sauvegarde de bandes physiques.

Pour sauvegarder des données sur une bande

1. Dans le menu Quick Start (Démarrage rapide), ouvrez la session de restauration d'une sauvegarde.
2. Choisissez l'onglet Source, puis choisissez le système de fichiers ou de base de données que vous souhaitez sauvegarder.
3. Choisissez l'onglet Schedule (Planification) et choisissez la méthode de répétition que vous voulez utiliser.
4. Choisissez l'onglet Destination, puis la bande que vous voulez utiliser. Si le volume des données que vous sauvegardez est supérieur à la capacité de la bande, Arcserve vous invite à monter une nouvelle bande.
5. Choisissez Submit (Soumettre) pour sauvegarder vos données.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci risque d'échouer. Pour terminer la tâche de sauvegarde qui a échoué, vous devez la soumettre à nouveau.

Archivage d'une bande

Lorsque vous archivez une bande, la passerelle de bande la transfère de la bibliothèque de bandes vers le stockage hors connexion. Avant d'éjecter et d'archiver une bande, vous pouvez en vérifier le contenu.

Pour archiver une bande

1. Dans le menu Quick Start (Démarrage rapide), ouvrez la session de restauration d'une sauvegarde.
2. Choisissez l'onglet Source, puis choisissez le système de fichiers ou de base de données que vous souhaitez sauvegarder.
3. Choisissez l'onglet Schedule (Planification) et choisissez la méthode de répétition que vous voulez utiliser.
4. Choisissez votre passerelle, ouvrez le menu contextuel (clic droit) d'une bande et choisissez Import/Export Slot (Emplacement d'importation/exportation).
5. Affectez un connecteur de messagerie pour charger la bande. Dans la console Storage Gateway, l'état devient Archivage. Le processus d'archivage peut être long.

La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT À VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande éjectée n'est plus répertoriée dans la bibliothèque de bandes virtuelles (VTL), mais elle est archivée dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

Restauration des données d'une bande

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Extrayez la bande archivée vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez Arcserve pour restaurer les données. Ce processus est le même que celui de la restauration des données des bandes physiques. Pour obtenir des instructions, reportez-vous à la documentation Arcserve Backup.

Pour restaurer les données d'une bande, utilisez la procédure suivante.

Pour restaurer les données d'une bande

1. Dans le menu Quick Start (Démarrage rapide), ouvrez la session de restauration d'une restauration.
2. Choisissez l'onglet Source, puis le système de fichiers ou de base de données que vous souhaitez restaurer.
3. Choisissez l'onglet Destination et acceptez les paramètres par défaut.
4. Choisissez l'onglet Schedule (Planification), la méthode de répétition que vous souhaitez utiliser, puis Submit (Soumettre).

Étape suivante

Nettoyage des ressources inutiles

Test de votre configuration à l'aide de Bacula Enterprise

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les périphériques de votre bibliothèque de bandes virtuelles (VTL) à l'aide de Bacula Enterprise. Dans cette rubrique, vous trouverez une documentation de base sur la configuration de l'application de sauvegarde Bacula version 10 pour une passerelle de bande et sur la réalisation des opérations de sauvegarde et de restauration. Pour des informations détaillées sur l'utilisation de Bacula, consultez les manuels et la documentation de Bacula Systems ou contactez Bacula Systems.

> **Note**
>
> Bacula est pris en charge uniquement sur Linux.

Configuration de Bacula Enterprise

Une fois que vous avez connecté les appareils de la bibliothèque de bandes virtuelles (VTL) à votre client Linux, vous configurez le logiciel Bacula pour identifier vos appareils. Pour plus d'informations sur la connexion des appareils VTL à votre client, consultez Connexion de vos appareils VTL.

Pour configurer Bacula

1. Procurez-vous une copie sous licence du logiciel de sauvegarde Bacula Enterprise auprès de Bacula Systems.
2. Installez le logiciel Bacula Enterprise sur votre ordinateur sur site ou dans le cloud.

   Pour obtenir des informations sur la façon d'obtenir le logiciel d'installation, consultez la page Enterprise Backup pour Amazon S3 et Storage Gateway. Pour obtenir plus d'instructions d'installation, consultez le livre blanc Using Cloud Services and Object Storage with Bacula Enterprise Edition (Utilisation de services cloud et de solutions de stockage d'objets avec Bacula Enterprise Edition).

Configuration de Bacula pour fonctionner avec des appareils VTL

Ensuite, configurez Bacula pour fonctionner avec vos appareils VTL. Vous trouverez ci-dessous des étapes de configuration de base.

Pour configurer Bacula

1. Installez le Bacula Director et le démon Bacula Storage. Pour obtenir des instructions, consultez le chapitre 7 du livre blanc Bacula Using Cloud Services and Object Storage with Bacula Enterprise Edition (Utilisation de services cloud et de solutions de stockage d'objets avec Bacula Enterprise Edition).
2. Connectez-vous au système qui exécute Bacula Director et configurez l'initiateur iSCSI. Pour ce faire, utilisez le script fourni dans l'étape 7.4 du livre blanc Bacula Using Cloud Services and Object Storage with Bacula Enterprise Edition (Utilisation de services cloud et de solutions de stockage d'objets avec Bacula Enterprise Edition).
3. Configurez les périphériques de stockage. Utilisez le script fourni dans le livre blanc Bacula mentionné ci-dessus.
4. Configurez le Bacula Director local, ajoutez des cibles de stockage et définissez des pools de média pour vos bandes. Utilisez le script fourni dans le livre blanc Bacula mentionné ci-dessus.

Sauvegarde de données sur une bande

1. Créez des bandes dans la console Storage Gateway. Pour plus d'informations sur la création de bandes, consultez Création de bandes.

2. Transférez les bandes de l'emplacement I/E vers l'emplacement de stockage à l'aide de la commande suivante.

   ```
   /opt/bacula/scripts/mtx-changer
   ```

   Par exemple, la commande suivante permet de transférer les bandes de l'emplacement I/E 1601 vers l'emplacement de stockage 1.

   ```
   /opt/bacula/scripts/mtx-changer transfer 1601 1
   ```

3. Lancez la console Bacula à l'aide de la commande suivante.

   ```
   /opt/bacula/bin/bconsole
   ```

   > **Note**
   >
   > Lorsque vous créez et transférez une bande vers Bacula, utilisez la commande de la console Bacula (bconsole) `update slots storage=VTL` afin que Bacula soit au courant des nouvelles bandes que vous avez créées.

4. Étiquetez la bande avec le code-barres en tant que nom ou étiquette du volume à l'aide de la commande bconsole suivante.

   ```
   label storage=VTL pool=pool.VTL barcodes === label the tapes with the barcode as the volume name / label
   ```

5. Montez la bande à l'aide de la commande suivante.

   ```
   mount storage=VTL slot=1 drive=0
   ```

6. Créez une tâche de sauvegarde qui utilise les pools de médias que vous avez créés, puis écrivez des données sur la bande virtuelle en suivant les mêmes procédures que pour les bandes physiques.

7. Démontez la bande de la console Bacula à l'aide de la commande suivante.

   ```
   umount storage=VTL slot=1 drive=0
   ```

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque pendant une tâche de sauvegarde en cours, celle-ci échouera et le statut de la bande dans Bacula Enterprise

passera à FULL. Si vous savez que la bande n'a pas été entièrement utilisée, vous pouvez redéfinir manuellement le statut de la bande sur APPEND et poursuivre le travail de sauvegarde en utilisant la même bande. Vous pouvez également poursuivre le travail sur une autre bande si d'autres bandes présentant le statut APPEND sont disponibles.

Archivage d'une bande

Lorsque toutes les tâches de sauvegarde d'une bande spécifique sont terminées, vous pouvez archiver cette bande. Utilisez le script mtx-changer pour transférer la bande de l'emplacement de stockage vers l'emplacement I/E. Cette action est semblable à l'action d'éjection proposée par d'autres applications de sauvegarde.

Pour archiver une bande

1. Transférez la bande de l'emplacement de stockage vers l'emplacement I/E à l'aide de la commande `/opt/bacula/scripts/mtx-changer`.

   Par exemple, la commande suivante permet de transférer une bande de l'emplacement de stockage 1 vers l'emplacement I/E 1601.

   ```
   /opt/bacula/scripts/mtx-changer transfer 1 1601
   ```

2. Vérifiez que la bande est archivée dans le stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive) et qu'elle dispose de l'état Archivé.

Restauration de données à partir d'une bande archivée et extraite

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Récupérez les bandes archivées de l'archive vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Restaurez vos données à l'aide du logiciel Bacula :

   a. Importez les bandes dans l'emplacement de stockage en utilisant la commande `/opt/bacula/scripts/mtx-changer` pour les transférer vers l'emplacement I/E.

Par exemple, la commande suivante permet de transférer les bandes de l'emplacement I/E 1601 vers l'emplacement de stockage 1.

```
/opt/bacula/scripts/mtx-changer transfer 1601 1
```

b. Utilisez la console Bacula pour mettre à jour les emplacements, puis montez la bande.

c. Exécutez la commande de restauration pour restaurer vos données. Pour obtenir des instructions, consultez la documentation Bacula.

Test de votre configuration à l'aide de Commvault

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer vos périphériques VTL (Virtual Tape Library) à l'aide de Commvault. Dans cette rubrique, vous trouverez la documentation de base sur la façon de configurer l'application de sauvegarde Commvault pour une passerelle de bande, d'effectuer un archivage de sauvegarde et de récupérer vos données à partir de bandes archivées. Pour obtenir des informations détaillées sur l'utilisation de Commvault, consultez la documentation de Commvault.

Rubriques

- Configuration de Commvault pour utiliser les appareils VTL
- Création d'une stratégie de stockage et d'une stratégie de sous-client
- Sauvegarde des données sur une bande dans Commvault
- Archivage d'une bande dans Commvault
- Restauration des données d'une bande

Configuration de Commvault pour utiliser les appareils VTL

Une fois que vous avez connecté les appareils VTL au client Windows, vous configurez Commvault pour les reconnaître. Pour plus d'informations sur la connexion des appareils VTL au client Windows, consultez Connexion de vos appareils VTL à un client Windows.

L'application de sauvegarde Commvault ne reconnaît pas automatiquement des appareils VTL. Vous devez ajouter manuellement des appareils pour les exposer à l'application de sauvegarde Commvault, puis découvrir les appareils.

Pour configurer Commvault

1. Dans le menu principal de la CommCell console, choisissez Storage, puis Expert Storage Configuration pour ouvrir la boîte de MediaAgents dialogue de sélection.
2. Choisissez l'agent multimédia disponible que vous souhaitez utiliser et sélectionnez Add, puis OK.
3. Dans la boîte de dialogue Expert Storage Configuration, choisissez Start, puis Detect/Configure Devices.
4. Laissez les options Device Type sélectionnées et choisissez Exhaustive Detection, puis OK.
5. Dans la boîte de dialogue de confirmation Confirm Exhaustive Detection, choisissez Yes.
6. Dans la boîte de dialogue Device Selection, choisissez votre bibliothèque et tous ses lecteurs, puis cliquez sur OK. Attendez que vos appareils soient détectés, puis choisissez Close pour fermer le rapport de journal.
7. Cliquez avec le bouton droit de la souris sur votre bibliothèque et choisissez Configure, puis Yes. Fermez la boîte de dialogue de configuration.
8. Dans la boîte de dialogue Does this library have a barcode reader ? (Cette bibliothèque a-t-elle un lecteur de code-barres ?), choisissez Yes (Oui), puis pour le type d'appareil, choisissez IBM ULTRIUM V5.
9. Dans le CommCell navigateur, sélectionnez Ressources de stockage, puis cliquez sur Bibliothèques pour afficher votre bibliothèque de bandes.
10. Pour voir vos bandes dans votre bibliothèque, ouvrez le menu contextuel (clic droit) de votre bibliothèque, puis choisissez Discover Media (Rechercher un média) Media location (Emplacement du média), Media Library (Bibliothèque de médias).
11. Pour monter vos bandes, ouvrez le menu contextuel (clic droit) de votre média, puis sélectionnez Load (Charger).

Création d'une stratégie de stockage et d'une stratégie de sous-client

Chaque tâche de sauvegarde et de restauration est associée à une stratégie de stockage et à une stratégie de sous-client.

Une stratégie de stockage mappe l'emplacement d'origine des données de votre média.

Pour créer une stratégie de stockage

1. Dans le CommCell navigateur, sélectionnez Policies.

2. Ouvrez le menu contextuel (clic droit) de Storage Policies (Stratégies de stockage), puis sélectionnez New Storage Policy (Nouvelle stratégie de stockage).
3. Dans l'assistant Create Storage Policy, choisissez Data Protection and Archiving, puis Next.
4. Saisissez un nom pour Storage Policy Name, puis choisissez Incremental Storage Policy. Pour associer cette stratégie de stockage à des chargements incrémentiels, choisissez l'une des options. Sinon, laissez les options désélectionnées, puis cliquez sur Next.
5. Dans la boîte de dialogue Do you want to Use Global Deduplication Policy ? (Voulez-vous utiliser une stratégie de déduplication globale ?), choisissez votre préférence pour Deduplication (Déduplication), puis choisissez Next.
6. Dans Library for Primary Copy (Bibliothèque de copie principale), sélectionnez votre bibliothèque VTL, puis choisissez Next (Suivant).
7. Vérifiez que vos paramètres d'agent multimédia sont corrects, puis choisissez Next.
8. Vérifiez que vos paramètres de groupe scratch sont corrects, puis choisissez Next.
9. Configurez vos politiques de conservation dans iData Agent Backup data, puis choisissez Next.
10. Vérifiez les paramètres de chiffrement, puis choisissez Next.
11. Pour afficher votre stratégie de stockage, choisissez Storage Policies.

Vous créez une stratégie de sous-client et vous l'associez à votre stratégie de stockage. Une stratégie de sous-client vous permet de configurer de nombreux clients de système de fichiers similaires à partir d'un modèle central pour ne pas avoir à les configurer manuellement.

Pour créer une stratégie de sous-client

1. Dans le CommCell navigateur, sélectionnez Clients Computers, puis sélectionnez votre ordinateur client. Choisissez Système de fichiers, puis choisissez defaultBackupSet.
2. Cliquez avec defaultBackupSetle bouton droit de la souris, sélectionnez Toutes les tâches, puis choisissez Nouveau sous-client.
3. Dans la zone Propriétés du sous-client, tapez un nom dans SubClient Nom, puis cliquez sur OK.
4. Choisissez Browse, accédez aux fichiers à sauvegarder, choisissez Add, puis fermez la boîte de dialogue.
5. Dans la zone de propriétés Subclient, sélectionnez l'onglet Storage Device et choisissez une stratégie de stockage dans Storage policy, puis choisissez OK.
6. Dans la fenêtre Backup Schedule (Calendrier de sauvegarde) qui s'affiche, associez le nouveau sous-client à un calendrier de sauvegarde.

7. Choisissez Do Not Schedule (Ne pas programmer) pour les sauvegardes ponctuelles/à la demande, puis choisissez OK.

   Vous devriez maintenant voir votre sous-client dans l'defaultBackupSetonglet.

Sauvegarde des données sur une bande dans Commvault

Vous créez une tâche de sauvegarde et vous écrivez des données sur une bande virtuelle en utilisant les mêmes procédures que pour les bandes physiques. Pour plus d'informations, consultez la documentation de Commvault.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci risque d'échouer. Dans certains cas, vous pouvez sélectionner une option pour reprendre la tâche qui a échoué. Sinon, vous devez soumettre une autre tâche. Si Commvault indique que la bande est inutilisable après l'échec d'une tâche, vous devez la recharger la bande dans le lecteur pour continuer à y écrire. Si plusieurs bandes sont disponibles, Commvault peut poursuivre la tâche de sauvegarde échouée sur une autre bande.

Archivage d'une bande dans Commvault

Vous démarrez le processus d'archivage en éjectant la bande. Lorsque vous archivez une bande, la passerelle de bande la transfère de la bibliothèque de bandes vers le stockage hors connexion. Avant d'éjecter et d'archiver une bande, vous pouvez d'abord en vérifier le contenu.

Pour archiver une bande

1. Dans le CommCell navigateur, choisissez Ressources de stockage, Bibliothèques, puis sélectionnez Votre bibliothèque. Choisissez Media By Location, puis Media In Library.
2. Ouvrez le menu contextuel (clic droit) de la bande que vous voulez archiver et choisissez All Tasks, puis Export et enfin, OK.

La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT À VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande n'est plus répertoriée dans la VTL.

Dans le logiciel Commvault, vérifiez que la bande ne se trouve plus dans l'emplacement de stockage.

Dans le volet de navigation de la console Storage Gateway, sélectionnez Bandes. Vérifiez que l'état de votre bande archivée est ARCHIVÉ.

Restauration des données d'une bande

Vous pouvez restaurer des données à partir d'une bande qui n'a jamais été archivée et extraite ou à partir d'une bande qui a été archivée et extraite. Pour les bandes qui n'ont jamais été archivées et extraites (bandes non extraites), deux possibilités s'offrent à vous pour restaurer les données :

- Restaurer par sous-client
- Restaurer par ID de tâche

Pour restaurer des données à partir d'une bande non extraite par sous-client

1. Dans le CommCell navigateur, sélectionnez Clients Computers, puis sélectionnez votre ordinateur client. Choisissez Système de fichiers, puis choisissez defaultBackupSet.
2. Ouvrez le menu contextuel (clic droit) de votre sous-client et choisissez Browse and Restore (Parcourir et restaurer), puis View Content (Afficher le contenu).
3. Choisissez les fichiers à restaurer, puis choisissez Recover All Selected (Récupérer la sélection).
4. Choisissez Home (Accueil), puis Job Controller (Contrôleur de travaux) pour surveiller le statut de votre tâche de restauration.

Pour restaurer des données à partir d'une bande non extraite ID de tâche

1. Dans le CommCell navigateur, sélectionnez Clients Computers, puis sélectionnez votre ordinateur client. Cliquez avec le bouton droit de la souris sur File System (Système de fichiers) et choisissez View (Afficher), puis Backup History (Historique de sauvegarde).
2. Dans la catégorie Backup Type (Type de sauvegarde), choisissez le type de tâche de sauvegarde de votre choix, puis cliquez sur OK. Un onglet avec l'historique des tâches de sauvegarde s'affiche.
3. Recherchez le Job ID (ID de tâche) à restaurer, cliquez avec le bouton droit de la souris sur celui-ci, puis choisissez Browse and Restore (Parcourir et restaurer).
4. Dans la boîte de dialogue Browse and Restore Options (Options de recherche et de restauration), choisissez View Content (Afficher le contenu).

5. Choisissez les fichiers à restaurer, puis choisissez Recover All Selected (Récupérer la sélection).
6. Choisissez Home (Accueil), puis Job Controller (Contrôleur de travaux) pour surveiller le statut de votre tâche de restauration.

Pour restaurer des données à partir d'une bande archivée et extraite

1. Dans le CommCell navigateur, choisissez Ressources de stockage, Bibliothèques, puis Votre bibliothèque. Choisissez Media By Location, puis Media In Library.
2. Cliquez avec le bouton droit de la souris sur la bande extraite et choisissez All Tasks, puis Catalog.
3. Dans la boîte de dialogue Catalog Media, choisissez Catalog only, puis OK.
4. Choisissez CommCell Home (Accueil), puis Job Controller (Contrôleur de travaux) pour surveiller le statut de votre tâche de restauration.
5. Une fois la tâche exécutée avec succès, ouvrez le menu contextuel (clic droit) de votre bande et choisissez View (Afficher), puis View Catalog Contents (Afficher le contenu du catalogue). Notez l'ID de tâche pour une utilisation ultérieure.
6. Choisissez Recatalog/Merge. Assurez-vous de sélectionner Merge only (Fusionner uniquement) dans la boîte de dialogue Catalog Media (Média de catalogue).
7. Choisissez Home (Accueil), puis Job Controller (Contrôleur de travaux) pour surveiller le statut de votre tâche de restauration.
8. Une fois la tâche terminée, choisissez CommCell Accueil, Panneau de configuration, puis choisissez Browse/Search/Recovery.
9. Choisissez Show aged data during browse and recovery, cliquez sur OK, puis fermez le Control Panel.
10. Dans le CommCell navigateur, cliquez avec le bouton droit sur Ordinateurs clients, puis sélectionnez votre ordinateur client. Choisissez View, puis Job History.
11. Dans la boîte de dialogue Job History Filter, choisissez Advanced.
12. Choisissez Include Aged Data, puis OK.
13. Dans la boîte de dialogue Job History, cliquez sur OK pour ouvrir l'onglet History of jobs.
14. Recherchez la tâche à restaurer, ouvrez le menu contextuel (clic droit) qui lui correspond, puis choisissez Browse and Restore (Parcourir et restaurer).
15. Dans la boîte de dialogue Browse and Restore (Parcourir et restaurer, choisissez View Content (Afficher le contenu).

16. Choisissez les fichiers à restaurer, puis choisissez Recover All Selected (Récupérer la sélection).
17. Choisissez Home (Accueil), puis Job Controller (Contrôleur de travaux) pour surveiller le statut de votre tâche de restauration.

Test de votre configuration à l'aide de Dell EMC NetWorker

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les périphériques de votre bibliothèque de bandes virtuelles (VTL) à l'aide de Dell EMC NetWorker. Dans cette rubrique, vous trouverez de la documentation de base sur la configuration du NetWorker logiciel Dell EMC pour qu'il fonctionne avec une passerelle sur bande et effectue une sauvegarde, notamment sur la configuration des périphériques de stockage, l'écriture de données sur une bande, l'archivage d'une bande et la restauration de données à partir d'une bande.

Pour obtenir des informations détaillées sur l'installation et l'utilisation du NetWorker logiciel Dell EMC, consultez la NetWorker documentation.

Pour plus d'informations sur les applications de sauvegarde compatibles, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Configuration pour utiliser les appareils VTL
- Autorisation de l'importation de bandes WORM dans Dell EMC NetWorker
- Sauvegarde de données sur bande dans Dell EMC NetWorker
- Archivage d'une bande dans Dell EMC NetWorker
- Restauration de données à partir d'une bande archivée dans Dell EMC NetWorker

Configuration pour utiliser les appareils VTL

Après avoir connecté vos appareils de bibliothèque de bandes virtuelles (VTL) au client Microsoft Windows, une configuration devra être effectuée pour identifier vos appareils. Pour plus d'informations sur la connexion des appareils VTL au client Windows, consultez Connexion de vos appareils VTL.

ne reconnaît pas automatiquement les appareils d'une passerelle de bande. Pour exposer vos appareils VTL au NetWorker logiciel et faire en sorte que le logiciel les découvre, vous configurez le logiciel manuellement. Ci-après, nous supposerons que vous avez installé correctement le logiciel

et que vous savez utiliser la console de gestion. Pour plus d'informations sur la console de gestion, consultez la section relative à l'interface de la console de NetWorker gestion du guide d' NetWorker administration Dell EMC.

Pour configurer le NetWorker logiciel Dell EMC pour les appareils VTL

1. Démarrez l'application Dell EMC NetWorker Management Console, choisissez Enterprise dans le menu, puis localhost dans le volet de gauche.
2. Ouvrez le menu contextuel (clic droit) pour localhost, puis choisissez Lancer l'application.
3. Choisissez l'onglet Appareils, ouvrez le menu contextuel (clic droit) pour Bibliothèques, puis choisissez Rechercher les appareils.
4. Dans l'assistant Rechercher les appareils, sélectionnez Démarrer l'analyse, puis choisissez OK dans la boîte de dialogue qui s'affiche.
5. Développez l'arborescence du dossier Bibliothèques pour voir toutes les bibliothèques et appuyez sur F5 pour actualiser. Ce processus peut avoir besoin de quelques secondes pour charger les appareils dans la bibliothèque.
6. Ouvrez une fenêtre de commande (cmd.exe) avec des privilèges d'administrateur et exécutez l'`jbconfig`utilitaire installé avec Dell EMC NetWorker 19.5.
    a. À l'invite du menu, entrez le chiffre correspondant pour sélectionner Configurer un juke-box SCSI à détection automatique.
    b. Lorsque vous êtes invité à fournir un nom pour le juke-box, entrez un nom tel que. `AWSVTL`
    c. Lorsque vous êtes invité à activer NetWorker le nettoyage automatique, entrez`no`.
    d. Lorsque vous êtes invité à contourner la configuration automatique, entrez`no`.
    e. Lorsque vous êtes invité à configurer un autre juke-box, entrez. no
7. Lorsque « jbconfig » est terminé, revenez à l'interface graphique de Networker et appuyez sur F5 pour actualiser.
8. Choisissez votre bibliothèque pour afficher vos bandes dans le volet de gauche et la liste des emplacements de volume vides correspondante dans le volet droit.
9. Dans la liste de volumes, sélectionnez les volumes que vous souhaitez activer (les volumes sélectionnés sont mis en évidence), ouvrez le menu contextuel (clic droit) pour les volumes sélectionnés, puis choisissez Dépôt. Cette action transfère la bande de l'emplacement I/E vers l'emplacement du volume.
10. Dans la boîte de dialogue qui s'affiche, sélectionnez Oui puis, dans la boîte de dialogue Charger les cartouches dans, choisissez Oui.

11. Si vous n’avez plus de bandes à déposer, choisissez Non ou Ignorer. Dans le cas contraire, choisissez Oui pour déposer les bandes supplémentaires.

Autorisation de l'importation de bandes WORM dans Dell EMC NetWorker

Vous êtes maintenant prêt à importer des bandes depuis votre Tape Gateway dans la NetWorker bibliothèque Dell EMC.

Les bandes virtuelles sont des bandes WORM (Write Once Read Many), mais Dell EMC NetWorker prévoit des bandes non WORM. Pour que Dell EMC NetWorker puisse utiliser vos bandes virtuelles, vous devez activer l'importation de bandes dans des pools de médias autres que WORM.

Autoriser l’importation de bandes WORM dans des pools de médias autres que WORM

1. Sur NetWorker la console, choisissez Media, ouvrez le menu contextuel (clic droit) de localhost, puis choisissez Propriétés.
2. Dans la fenêtre Propriétés du NetWorker serveur, choisissez l'onglet Configuration.
3. Dans la section Gestion des bandes Worm, désactivez la case à cocher Bandes WORM uniquement dans les pools WORM, puis choisissez OK.

Sauvegarde de données sur bande dans Dell EMC NetWorker

La sauvegarde des données sur une bande est un processus en deux étapes.

1. Etiquetez les bandes sur lesquelles vous souhaitez sauvegarder vos données, créez le pool de médias cible et ajoutez les bandes au pool.

   Vous créez pool de médias et vous écrivez des données sur une bande virtuelle en utilisant les mêmes procédures que pour les bandes physiques. Pour des informations détaillées, consultez la section Sauvegarde des données du Guide d' NetWorker administration Dell EMC.
2. Ecrivez les données sur la bande. Vous sauvegardez les données en utilisant l'application NetWorker utilisateur Dell EMC au lieu de la console de NetWorker gestion Dell EMC. L'application NetWorker utilisateur Dell EMC s'installe dans le cadre de l' NetWorkerinstallation.

> **Note**
>
> Vous utilisez l'application NetWorker utilisateur Dell EMC pour effectuer des sauvegardes, mais vous pouvez consulter l'état de vos tâches de sauvegarde et de restauration dans la console de gestion EMC. Pour afficher l'état, choisissez le menu Appareils et affichez l'état dans la fenêtre Journal.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque pendant une tâche de sauvegarde en cours, celle-ci échouera et le statut de la bande dans Dell EMC Networker passera à Write Protected (protégée en écriture). Vous pouvez archiver la bande ou continuer à lire les données qu'elle contient. Vous pouvez reprendre la tâche de sauvegarde suspendue sur une autre bande.

Archivage d'une bande dans Dell EMC NetWorker

Lorsque vous archivez une bande, Tape Gateway déplace la bande de la bibliothèque de NetWorker bandes Dell EMC vers le stockage hors ligne. Lancez l'archivage de bande en éjectant une bande du lecteur de bande vers l'emplacement de stockage. Vous retirez ensuite la bande du slot pour l'archiver à l'aide de votre application de sauvegarde, à savoir le logiciel Dell EMC NetWorker .

Pour archiver une bande à l'aide de Dell EMC NetWorker

1. Dans l'onglet Appareils de la fenêtre NetWorker Administration, sélectionnez localhost ou votre serveur EMC, puis choisissez Libraries.
2. Sélectionnez la bibliothèque que vous avez importée de la bibliothèque de bandes virtuelles.
3. Dans la liste des bandes sur lesquelles vous avez écrit des données, ouvrez le menu contextuel (clic droit) pour la bande que vous souhaitez archiver, puis choisissez Ejecter/Retirer.
4. Dans la zone de confirmation qui s'affiche, choisissez OK.

La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT À VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande n'est plus répertoriée dans la VTL.

Dans le NetWorker logiciel Dell EMC, vérifiez que la bande ne se trouve plus dans le slot de stockage.

Dans le volet de navigation de la console Storage Gateway, sélectionnez Bandes. Vérifiez que l'état de votre bande archivée est ARCHIVÉ.

Restauration de données à partir d'une bande archivée dans Dell EMC NetWorker

La restauration des données archivées est un processus en deux étapes :

1. Extrayez la bande archivée vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez le NetWorker logiciel Dell EMC pour restaurer les données. Pour cela, restaurez un fichier du dossier, comme vous le faites lors de la restauration des données à partir de bandes physiques. Pour obtenir des instructions, consultez la section Utilisation du programme NetWorker User du guide d' NetWorker administration Dell EMC.

Étape suivante

Nettoyage des ressources inutiles

Test de votre configuration à l'aide d'IBM Data Protect

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les périphériques de votre bibliothèque de bandes virtuelles (VTL) à l'aide d'IBM Data Protect with AWS Storage Gateway. (IBM Data Protect était auparavant connu sous le nom de Tivoli Storage Manager.)

Cette rubrique contient des informations de base sur la configuration du logiciel de sauvegarde IBM Data Protect pour une passerelle Tape Gateway. Il inclut également des informations de base sur les opérations de sauvegarde et de restauration avec IBM Data Protect. Pour plus d'informations sur l'administration du logiciel de sauvegarde IBM Data Protect, reportez-vous à la documentation IBM Data Protect.

Le logiciel de sauvegarde IBM Data Protect est compatible avec AWS Storage Gateway les systèmes d'exploitation suivants.

- Microsoft Windows Server
- Red Hat Linux

Pour plus d'informations sur les appareils pris en charge par IBM Data Protect pour Windows, consultez la section Appareils pris en charge par IBM Data Protect (anciennement Tivoli Storage Manager) pour AIX, HP-UX, Solaris et Windows.

Pour plus d'informations sur les appareils pris en charge par IBM Data Protect pour Linux, consultez la section Appareils pris en charge par IBM Data Protect (anciennement Tivoli Storage Manager) pour Linux.

Rubriques

- Configuration d'IBM Data Protect
- Configuration d'IBM Data Protect pour qu'il fonctionne avec des appareils VTL
- Écrire des données sur une bande dans IBM Data Protect
- Restauration de données à partir d'une bande archivée dans IBM Data Protect

Configuration d'IBM Data Protect

Après avoir connecté vos appareils VTL à votre client, vous configurez le logiciel IBM Data Protect pour qu'il les reconnaisse. Pour plus d'informations sur la connexion des appareils VTL à votre client, consultez Connexion de vos appareils VTL.

Pour configurer IBM Data Protect

1. Obtenez une copie sous licence du logiciel IBM Data Protect auprès d'IBM.
2. Installez le logiciel IBM Data Protect sur votre environnement sur site ou sur une instance Amazon EC2 dans le cloud. Pour plus d'informations, consultez la documentation d'installation et de mise à niveau d'IBM Data Protect.

   Pour plus d'informations sur la configuration du logiciel IBM Data Protect, voir Configuration des AWS librairies de bandes virtuelles Tape Gateway pour un serveur IBM Data Protect.

Configuration d'IBM Data Protect pour qu'il fonctionne avec des appareils VTL

Configurez ensuite IBM Data Protect pour qu'il fonctionne avec vos appareils VTL. Vous pouvez configurer IBM Data Protect pour qu'il fonctionne avec des appareils VTL sur Microsoft Windows Server ou Red Hat Linux.

Configuration d'IBM Data Protect pour Windows

Pour obtenir des instructions complètes sur la configuration d'IBM Data Protect sous Windows, consultez Tape Device Driver-W12 6266 pour Windows 2012 sur le site Web de Lenovo. Voici une documentation de base sur le processus.

Pour configurer IBM Data Protect pour Microsoft Windows

1. Obtenez le package de pilotes approprié pour votre changeur de média. Pour le pilote de périphérique à bande, IBM Data Protect nécessite la version W12 6266 pour Windows 2012. Pour obtenir des instructions sur l'obtention des pilotes, consultez le document Tape Device Driver-W12 6266 for Windows 2012 (Pilote d'appareil de bande W12 6266 pour Windows 2012) sur le site Web de Lenovo.

   > **Note**
   >
   > Assurez-vous d'installer le jeu de pilotes « non exclusif ».

2. Sur votre ordinateur, ouvrez Gestion de l'ordinateur, développez Changeurs de médias, puis vérifiez que le type de changeur de média est défini sur IBM 3584 Tape Library (Bibliothèque de bandes IBM 3584).
3. Assurez-vous que le code-barres de toute bande de la bibliothèque de bandes virtuelles ne comporte pas plus de huit caractères. Si vous essayez d'attribuer à votre bande un code-barres de plus de huit caractères, vous obtenez le message d'erreur suivant : `"Tape barcode is too long for media changer"`.
4. Assurez-vous que tous vos lecteurs de bandes et changeurs de média apparaissent dans IBM Data Protect. Pour ce faire, utilisez la commande suivante : `\Tivoli\TSM \server>tsmdlst.exe`

Configuration d'IBM Data Protect pour Linux

Vous trouverez ci-dessous une documentation de base sur la configuration d'IBM Data Protect pour qu'il fonctionne avec des appareils VTL sous Linux.

Pour configurer IBM Data Protect pour Linux

1. Accédez à IBM Fix Central sur le site Web de support IBM et choisissez Sélectionner un produit.
2. Pour Product Group (Groupe de produits), choisissez System Storage (Stockage système).

3. Pour Select from System Storage (Sélectionner depuis le stockage système), choisissez Tape systems (Systèmes sur bande).
4. Pour Tape systems, (Systèmes de bandes), choisissez Tape drivers and software (Pilotes de bandes et logiciels).
5. Pour Select from Tape drivers and software (Sélectionner depuis les logiciels et les pilotes de bande), choisissez Tape device drivers (Pilotes d'appareil de bande).
6. Pour Platform (Plateforme), choisissez votre système d'exploitation, puis Continue (Continuer).
7. Choisissez la version du pilote de l'appareil que vous souhaitez télécharger. Suivez ensuite les instructions de la page de téléchargement de Fix Central pour télécharger et configurer IBM Data Protect.
8. Assurez-vous que le code-barres de toute bande de la bibliothèque de bandes virtuelles ne comporte pas plus de huit caractères. Si vous essayez d'attribuer à votre bande un code-barres de plus de huit caractères, vous obtenez le message d'erreur suivant : `"Tape barcode is too long for media changer"`.

Écrire des données sur une bande dans IBM Data Protect

Vous écrivez des données sur une bande virtuelle de la passerelle de bande en utilisant les mêmes procédures et politiques de sauvegarde qu'avec les bandes physiques. Créez la configuration nécessaire pour les tâches de sauvegarde et de restauration. Pour plus d'informations sur la configuration d'IBM Data Protect, voir Présentation des tâches d'administration pour IBM Data Protect.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci risque d'échouer. Si la tâche de sauvegarde échoue, l'état de la bande dans IBM Data Protect passe à ReadOnly. Si vous savez que la bande n'a pas été entièrement utilisée, vous pouvez rétablir manuellement l'état de la bande ReadWrite, puis reprendre ou renvoyer le travail de sauvegarde en utilisant la même bande. IBM Data Protect peut poursuivre la tâche de sauvegarde ayant échoué sur une autre bande si d'autres bandes en ReadWriteétat sont disponibles.

Restauration de données à partir d'une bande archivée dans IBM Data Protect

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Récupérez les bandes archivées de l'archive vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Restaurez les données à l'aide du logiciel de sauvegarde IBM Data Protect. Pour cela, créez un point de récupération, comme vous le faites lors de la restauration des données de bandes physiques. Pour plus d'informations sur la configuration d'IBM Data Protect, voir Présentation des tâches d'administration pour IBM Data Protect.

Étape suivante

Nettoyage des ressources inutiles

Test de votre configuration à l'aide de OpenText Data Protector

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les périphériques de votre bibliothèque de bandes virtuelles (VTL) à l'aide de OpenText Data Protector. Dans cette rubrique, vous trouverez une documentation de base expliquant comment configurer le logiciel OpenText Data Protector pour une passerelle Tape Gateway et effectuer une opération de sauvegarde et de restauration. Pour des informations détaillées sur l'utilisation du logiciel OpenText Data Protector, consultez la documentation OpenText Data Protector. Pour plus d'informations sur les applications de sauvegarde compatibles, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Configuration de OpenText Data Protector pour qu'il fonctionne avec les appareils VTL
- Préparation de bandes virtuelles à utiliser avec Data Protector
- Chargement de bandes dans un pool de médias
- Sauvegarde de données sur une bande
- Archivage d'une bande
- Restauration des données d'une bande

Configuration de OpenText Data Protector pour qu'il fonctionne avec les appareils VTL

Après avoir connecté les périphériques VTL (Virtual Tape Library) au client, vous configurez OpenText Data Protector pour qu'il reconnaisse vos appareils. Pour plus d'informations sur la connexion des appareils VTL au client , consultez Connexion de vos appareils VTL.

Le logiciel OpenText Data Protector ne reconnaît pas automatiquement les périphériques Tape Gateway. Pour qu'il les reconnaisse, ajoutez manuellement les appareils, puis découvrez les appareils VTL, comme décrit ci-dessous.

Pour ajouter les appareils VTL

1. Dans la fenêtre principale de OpenText Data Protector, choisissez l'étagère Appareils et médias dans la liste en haut à gauche.

   Ouvrez le menu contextuel (clic droit) de Devices, puis choisissez Add Device.
2. Dans l'onglet Add Device, tapez une valeur pour Device Name. Pour Device Type, choisissez SCSI Library, puis Next.
3. Dans l'écran suivant, procédez comme suit :

   a. Pour SCSI address of the library robotic, sélectionnez votre adresse spécifique.

   b. Pour Select what action Data Protector should take if the drive is busy, sélectionnez « Abort » ou l'action que vous souhaitez.

   c. Choisissez d'activer les options suivantes :

      - Barcode reader support
      - Automatically discover changed SCSI address
      - SCSI Reserve/Release (robotic control)

   d. Décochez Use barcode as medium label on initialization, sauf si votre système a besoin de cette option.

   e. Choisissez Next (Suivant) pour continuer.
4. Dans l'écran suivant, spécifiez les emplacements à utiliser avec HP Data Protector. Utilisez un trait d'union (« - ») entre les chiffres pour indiquer une plage d'emplacements, par exemple 1–6. Lorsque vous avez indiqué les emplacements à utiliser, choisissez Next.
5. Pour le type de support standard utilisé par l'appareil physique, choisissez LTO_Ultrium, puis choisissez Finish pour terminer l'installation.

Votre bibliothèque de bandes est maintenant prête à être utilisée. Pour y charger des bandes, consultez la section suivante.

Préparation de bandes virtuelles à utiliser avec Data Protector

Avant de pouvoir sauvegarder des données dans une bande virtuelle, vous devez préparer les bandes à utiliser. Cela implique les opérations suivantes :

- Charger une bande virtuelle dans une bibliothèque de bandes
- Charger la bande virtuelle dans un emplacement
- Créer un pool de médias
- Charger la bande virtuelle dans le pool de médias

Dans les sections suivantes, vous trouverez des étapes pour vous guider dans ce processus.

Chargement de bandes virtuelles dans une bibliothèque de bandes

Votre bibliothèque de bandes doit désormais être répertoriée dans la liste Devices. Si ce n'est pas le cas, appuyez sur F5 pour actualiser l'écran. Lorsque votre bibliothèque apparaît dans la liste, vous pouvez y charger des bandes virtuelles.

Pour charger des bandes virtuelles dans votre bibliothèque de bandes

1. Choisissez le signe (+) en regard de votre bibliothèque de bandes pour afficher les nœuds des chemins, disques et emplacements des robots.
2. Ouvrez le menu contextuel (clic droit) pour Drives, choisissez Add Drive, tapez un nom pour votre bande et choisissez Next pour continuer.
3. Sélectionnez le lecteur de bandes que vous souhaitez ajouter pour SCSI address of data drive, choisissez Automatically discover changed SCSI address, puis Next.
4. Sur l'écran suivant, choisissez Advanced. La fenêtre contextuelle Advanced Options s'affiche.

    a. Dans l'onglet Settings, vous devez tenir compte des options suivantes :

    - CRC Check (pour détecter des modifications de données accidentelles)
    - Detect dirty drive (pour vous assurer que le disque est propre avant la sauvegarde)
    - SCSI Reserve/Release(drive) (pour éviter les conflits entre les bandes)

    À des fins de test, vous pouvez laisser ces options désactivées (décochées).

b. Sur l'onglet Sizes, définissez Block size (kB) sur Default (256).

c. Choisissez OK pour fermer l'écran des options avancées, puis choisissez Next pour continuer.

5. Dans l'écran suivant, sélectionnez ces options sous Device Policies :

   - Device may be used for restore
   - Device may be used as source device for object copy

6. Choisissez Finish pour terminer l'ajout de votre lecteur de bandes à votre bibliothèque de bandes.

Chargement de bandes virtuelles dans des emplacements

Maintenant que vous avez un lecteur de bandes dans votre bibliothèque de bandes, vous pouvez charger des bandes virtuelles dans des emplacements.

Pour charger une bande dans un emplacement

1. Dans le nœud de l'arborescence des bibliothèque de bandes, ouvrez le nœud nommé Slots. L'état de chaque emplacement est représenté par une icône :

   - Une bande verte représente une bande déjà chargée dans l'emplacement.
   - Un emplacement grisé représente un emplacement vide.
   - Un point d'interrogation cyan indique que la bande de cet emplacement n'est pas formatée.

2. Pour un emplacement vide, ouvrez le menu contextuel (clic droit), puis choisissez Enter. Si vous disposez de bandes existantes, choisissez-en une à charger dans cet emplacement.

Création d'un pool de médias

Un pool de médias est un groupe logique utilisé pour organiser vos bandes. Pour configurer une sauvegarde sur bandes, vous créez un pool de médias.

Pour créer un pool de médias

1. Dans Devices & Media, ouvrez le nœud de l'arborescence de Media, ouvrez le menu contextuel (clic droit) pour le nœud Pools, puis choisissez Add Media Pool.
2. Tapez un nom pour Pool name.
3. Pour Media Type, choisissez LTO_Ultrium, puis Next.

4. Sur l’écran suivant, acceptez les valeurs par défaut, puis choisissez Next.
5. Choisissez Finish pour terminer la création d’un pool de médias.

Chargement de bandes dans un pool de médias

Avant de pouvoir sauvegarder des données sur vos bandes, vous devez charger les bandes dans le pool de médias que vous avez créé.

Pour charger une bande virtuelle dans un pool de médias

1. Dans le nœud de l’arborescence des bibliothèque de bandes, choisissez le nœud Slots.
2. Choisissez une bande chargée, c’est-à-dire une bande avec une icône verte. Ouvrez le menu contextuel (clic droit), choisissez Format, puis Next.
3. Sélectionnez le pool de médias créé, puis Next.
4. Pour Medium Description, choisissez Use barcode, puis Next.
5. Pour Options, choisissez Force Operation, puis Finish.

L’état de l’emplacement que vous avez choisi doit passer de non attribué (grisé) à bande insérée (vert). Une série de messages s’affichent pour confirmer l’initialisation de votre média.

À ce stade, tout doit être configuré pour commencer à utiliser votre librairie de bandes virtuelles avec Data Protector. Pour vérifier que c’est le cas, utilisez la procédure suivante.

Pour vérifier que votre bibliothèque de bandes est configurée pour être utilisée

- Choisissez Drives, ouvrez le menu contextuel (clic droit) de votre lecteur, puis choisissez Scan.

Si votre configuration est correcte, un message confirme que votre média a été analysé avec succès.

Sauvegarde de données sur une bande

Lorsque vos bandes ont été chargées dans un pool de médias, vous pouvez y sauvegarder des données.

Pour sauvegarder des données sur une bande

1. Choisissez Backup dans le menu déroulant situé dans le coin supérieur gauche de la fenêtre.
2. Développez l'arborescence de navigation Backup depuis le volet de gauche.

3. Cliquez avec le bouton droit sur Système de fichiers pour ouvrir le menu contextuel, puis choisissez Add Backup.
4. Sur l'écran Create New Backup, sous Filesystem, choisissez Blank File System Backup, puis OK.
5. Sur le nœud de l'arborescence qui indique votre système hôte, sélectionnez le système de fichiers ou des systèmes de fichiers que vous souhaitez sauvegarder, puis sélectionnez Next pour continuer.
6. Ouvrez le nœud de l'arborescence de la bibliothèque de bandes que vous voulez utiliser, ouvrez le menu contextuel (clic droit) du lecteur de bandes à utiliser, puis choisissez Properties.
7. Choisissez votre pool de médias, OK, puis Next.
8. Pour les trois écrans suivants, acceptez les valeurs par défauts, puis choisissez Next.
9. Sur l'écran Perform finishing steps in your backup/template design, choisissez Save as pour enregistrer cette session. Dans la fenêtre contextuelle, nommez la sauvegarde et assignez-la au groupe dans lequel vous souhaitez enregistrer votre nouvelle spécification de sauvegarde.
10. Choisissez Start Interactive Backup.

Si le système hôte contient un système de base de données, vous pouvez le choisir en tant que système de sauvegarde cible. Les écrans et les sélections sont semblables à ceux de la sauvegarde de système de fichiers qui vient d'être décrite.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci échouera, et le lecteur de bande dans Data Protector sera marqué comme Dirty (corrompu). Data Protector indique également que la qualité de la bande est Poor (mauvaise) et empêche toute écriture sur la bande. Pour continuer à lire les données de la bande, vous devez nettoyer le lecteur et remonter la bande. Pour terminer la tâche de sauvegarde qui a échoué, vous devez la soumettre à nouveau sur une nouvelle bande.

Archivage d'une bande

Lorsque vous archivez une bande, la passerelle de bande la transfère de la bibliothèque de bandes vers le stockage hors connexion. Avant d'éjecter et d'archiver une bande, vous pouvez en vérifier le contenu.

Pour vérifier le contenu d'une bande avant de l'archiver

1. Choisissez Slots, puis choisissez la bande à vérifier.
2. Choisissez Objects et vérifiez le contenu de la bande.

Lorsque vous avez choisi une bande à archiver, utilisez la procédure suivante.

Pour éjecter et archiver une bande

1. Ouvrez le menu contextuel (clic droit) d'une bande, puis choisissez Eject.
2. Sur la console Storage Gateway, sélectionnez votre passerelle, puis choisissez Cartouches de bandes VTL et vérifiez le statut de la bande virtuelle que vous archivez.

Une fois que la bande a été éjectée, elle est automatiquement archivée dans le stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT A VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande éjectée n'est plus répertoriée dans la bibliothèque de bandes virtuelles (VTL), mais elle est archivée dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

Restauration des données d'une bande

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Extrayez la bande archivée vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez Data Protector pour restaurer les données. Ce processus est le même que celui de la restauration des données des bandes physiques.

Pour restaurer les données d'une bande, utilisez la procédure suivante.

Pour restaurer les données d'une bande

1. Choisissez Restaurer dans le menu déroulant situé dans le coin supérieur gauche de la fenêtre.

2. Choisissez le système de fichiers ou le système de base de données que vous souhaitez restaurer dans l'arborescence de navigation de gauche. Assurez-vous que la case de la sauvegarde que vous voulez restaurer est cochée. Choisissez Restore (Restaurer).
3. Dans la fenêtre Start Restore Session, choisissez Needed Media. Choisissez All media. La bande initialement utilisée pour la sauvegarde doit s'afficher. Sélectionnez cette bande, puis choisissez Close.
4. Dans la fenêtre Start Restore Session, acceptez les paramètres par défaut, choisissez Next, puis Finish.

Étape suivante

Nettoyage des ressources inutiles

Test de votre configuration à l'aide de Microsoft System Center DPM

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les périphériques de votre bibliothèque de bandes virtuelles (VTL) à l'aide de Microsoft System Center Data Protection Manager (DPM). Dans cette rubrique, vous trouverez une documentation de base sur la configuration de l'application de sauvegarde DPM pour une passerelle de bande et sur la réalisation d'une opération de sauvegarde et de restauration.

Pour plus d'informations sur l'utilisation de DPM, consultez la Documentation DPM sur le site Web de Microsoft System Center. Pour plus d'informations sur les applications de sauvegarde compatibles, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Configuration de DPM pour reconnaître les appareils VTL
- Importation d'une bande dans DPM
- Ecriture de données sur une bande dans DPM
- Archivage d'une bande à l'aide de DPM
- Restauration des données d'une bande archivée dans DPM

Configuration de DPM pour reconnaître les appareils VTL

Après avoir connecté les appareils de la bibliothèque de bandes virtuelles (VTL) au client Windows, vous configurez DPM afin d'identifier les appareils. Pour plus d'informations sur la connexion des appareils VTL au client Windows, consultez Connexion de vos appareils VTL.

Par défaut, le serveur DPM ne reconnaît pas les appareils d'une passerelle de bande. Pour configurer le serveur à utiliser avec les appareils d'une passerelle de bande, effectuez les tâches suivantes :

1. Vous mettez à jour les pilotes d'appareils VTL pour les exposer au serveur DPM.
2. Vous mappez manuellement les appareils VTL à la bibliothèque de bandes DPM.

Pour mettre à jour les pilotes d'appareils VTL

- Dans le gestionnaire d'appareils, mettez à jour le pilote du changeur de média. Pour obtenir des instructions, consultez Mise à jour le pilote d'appareil pour votre changeur de média.

Vous utilisez le DPMDrive MappingTool pour mapper vos lecteurs de bande à la librairie de bandes DPM.

Pour mapper les lecteurs de bandes à la bibliothèque de bandes du serveur DPM

1. Créez au moins une bande pour la passerelle. Pour plus d'informations sur la façon de procéder, consultez Création de bandes.
2. Importez la bande dans la bibliothèque DPM. Pour plus d'informations sur la procédure à utiliser, consultez Importation d'une bande dans DPM.
3. Si le service DPMLA est en cours d'exécution, arrêtez-le en ouvrant un terminal de commande et en tapant ce qui suit sur la ligne de commande.

   ```
   net stop DPMLA
   ```

4. Localisez le fichier suivant sur le serveur DPM : `%ProgramFiles%\System Center\DPM\DPM\Config\DPMLA.xml`.

   > **Note**
   >
   > Le chemin du répertoire peut changer en fonction de votre version de System Center ou de DPM.
   > Si ce fichier existe, il le DPMDrive MappingTool remplace. Si vous souhaitez conserver votre fichier d'origine, créez une copie de sauvegarde.

5. Ouvrez un terminal de commande, choisissez le répertoire `%ProgramFiles%\System Center\DPM\DPM\Bin` et exécutez la commande suivante.

> **Note**
>
> Le chemin du répertoire peut changer en fonction de votre version de System Center ou de DPM.

```
C:\Microsoft System Center\DPM\DPM\bin>DPMDriveMappingTool.exe
```

La sortie de la commande ressemble à ce qui suit.

```
Performing Device Inventory ...
Mapping Drives to Library ...
Adding Standalone Drives ...
Writing the Map File ...
Drive Mapping Completed Successfully.
```

Importation d'une bande dans DPM

Vous êtes maintenant prêt à importer des bandes de la passerelle de bande vers la bibliothèque de l'application de sauvegarde DPM.

Pour importer des bandes dans la bibliothèque de l'application de sauvegarde DPM

1. Sur le serveur DPM, ouvrez la console de gestion, choisissez Réanalyser, puis sélectionnez Actualiser. La console de gestion affiche votre changeur de support et vos lecteurs de bande.
2. Ouvrez le menu contextuel (clic droit) pour le changeur de média dans la section Bibliothèque, puis choisissez Ajouter une bande (port I/E) pour ajouter une bande à la liste Emplacements.

> **Note**
>
> Le processus d'ajout de bandes peut prendre plusieurs minutes.

L'étiquette de la bande indique Inconnu et la bande n'est pas utilisable. Pour que la bande soit utilisable, vous devez l'identifier.

3. Ouvrez le menu contextuel (clic droit) pour la bande à identifier, puis choisissez Identifier la bande inconnue.

> **Note**
>
> Le processus d'identification des bandes peut prendre quelques secondes ou quelques minutes.
> Si les cassettes n'affichent pas correctement les codes-barres, vous devez remplacer le pilote du changeur de média par Sun/ LibraryStorageTek . Pour de plus amples informations, veuillez consulter Affichage des codes-barres pour les bandes dans Microsoft System Center DPM.

Lorsque l'identification est terminée, l'étiquette de la bande indique Disponible. Cela signifie que la bande est disponible et que des données peuvent y être inscrites.

Ecriture de données sur une bande dans DPM

Vous écrivez des données sur une bande virtuelle de passerelle de bande en utilisant les mêmes procédures et politiques de protection qu'avec les bandes physiques. Vous créez un groupe de protection et vous ajoutez les données que vous voulez sauvegarder, puis vous sauvegarder les données en créant un point de récupération. Pour plus d'informations sur l'utilisation de DPM, consultez la Documentation DPM sur le site Web de Microsoft System Center.

Par défaut, la capacité d'une bande est de 30 Go. Lorsque vous sauvegardez les données d'une taille supérieure à la capacité d'une bande, une d'erreur d'E/S de périphérique se produit. Si la position où l'erreur s'est produite est supérieure à la taille de la bande, Microsoft DPM traite l'erreur comme une indication de fin de bande. Si la position où l'erreur s'est produite est inférieure à la taille de la bande, la tâche de sauvegarde échoue. Pour résoudre le problème, modifiez la valeur

de `TapeSize` dans l'entrée de registre pour correspondre à la taille de votre bande. Pour plus d'informations sur la façon de procéder, consultez Error ID: 30101 dans le Microsoft System Center.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci échouera. Pour terminer la tâche de sauvegarde qui a échoué, vous devez la soumettre à nouveau.

Archivage d'une bande à l'aide de DPM

Lorsque vous archivez une bande, la passerelle de bande la transfère de la bibliothèque de bandes DPM vers le stockage hors connexion. Vous commencez l'archivage des bandes en retirant la bande de l'emplacement à l'aide de votre application de sauvegarde, c'est-à-dire DPM.

Pour archiver une bande dans DPM

1. Ouvrez le menu contextuel (clic droit) pour la bande que vous voulez archiver, puis choisissez Supprimer la bande (port E/S).
2. Dans la boîte de dialogue qui s'affiche, cliquez sur Oui. Cette opération éjecte la bande de l'emplacement de stockage du changeur de média et la transfère dans l'un des emplacements d'I/E de la passerelle. Lorsqu'une bande est transférée dans l'emplacement I/E de la passerelle, elle est envoyée immédiatement pour l'archivage.
3. Sur la console Storage Gateway, sélectionnez votre passerelle, puis choisissez Cartouches de bandes VTL et vérifiez le statut de la bande virtuelle que vous archivez.

   La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT A VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande n'est plus répertoriée dans la VTL.

Restauration des données d'une bande archivée dans DPM

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Récupérez les bandes archivées de l'archive vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.

2. Utilisez l'application de sauvegarde DPM pour restaurer les données. Pour cela, créez un point de récupération, comme vous le faites lors de la restauration des données de bandes physiques. Pour plus d'informations, consultez Récupération des données informatiques du client sur le site Web de DPM.

Étape suivante

Nettoyage des ressources inutiles

Tester votre configuration en utilisant NovaStor DataCenter

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les périphériques de votre bibliothèque de bandes virtuelles (VTL) à l'aide de NovaStor DataCenter/Network. In this topic, you can find basic documentation on how to configure the NovaStor DataCenter/Network backup application for a Tape Gateway and perform backup and restore operations. For detailed information about how to use NovaStor DataCenter/Network, refer to the NovaStor DataCenter/Network la documentation.

NovaStor DataCenterConfiguration/réseau

Après avoir connecté vos périphériques VTL (Virtual Tape Library) à votre client Microsoft Windows, vous configurez le NovaStor logiciel pour qu'il reconnaisse vos appareils. Pour plus d'informations sur la connexion des appareils VTL à votre client Windows, consultez Connexion de vos appareils VTL.

NovaStor DataCenter/Network nécessite des pilotes fournis par les fabricants de pilotes. Vous pouvez utiliser les pilotes Windows, mais vous devez d'abord désactiver les autres applications de sauvegarde.

Configuration de NovaStor DataCenter /Network pour fonctionner avec des appareils VTL

Lorsque vous configurez vos appareils VTL pour qu'ils fonctionnent avec NovaStor DataCenter / Network, le message d'erreur suivant peut s'afficher. `External Program did not exit correctly` Ce problème nécessite une solution de contournement, que vous devez effectuer avant de pouvoir continuer.

Pour empêcher le problème, créez la solution de contournement avant de commencer la configuration de vos appareils VTL. Pour plus d'informations sur la création d'une solution de

contournement, consultez Résolution d'une erreur de type « External Program Did Not Exit Correctly ».

Pour configurer NovaStor DataCenter /Network pour qu'il fonctionne avec les appareils VTL

1. Dans la console NovaStor DataCenter /Network Admin, choisissez Media Management, puis Storage Management.
2. Dans le menu Storage Targets, ouvrez le menu contextuel (clic droit) de Media Management Servers, choisissez New, puis OK pour créer et préremplir un nœud de stockage.

   Si vous voyez un message d'erreur indiquant `External Program did not exit correctly`, résolvez le problème avant de continuer. Ce problème nécessite une solution de contournement. Pour plus d'informations sur la façon de résoudre ce problème, consultez Résolution d'une erreur de type « External Program Did Not Exit Correctly ».

   > **Important**
   >
   > Cette erreur se produit parce que la plage d'assignation des éléments comprise entre AWS Storage Gateway les unités de stockage et les lecteurs de bande dépasse le nombre autorisé par NovaStor DataCenter /Network.

3. Ouvrez le menu contextuel (clic droit) du nœud de stockage créé et choisissez New Library.
4. Sélectionnez le serveur de bibliothèque dans la liste. La liste des bibliothèques est automatiquement renseignée.
5. Attribuez un nom à la bibliothèque et choisissez OK.
6. Choisissez la bibliothèque pour afficher toutes les propriétés de la bibliothèque de bandes virtuelles de Storage Gateway.
7. Dans le menu Storage Targets, développez Backup Servers, ouvrez le menu contextuel (clic droit) du serveur et choisissez Attach Library.
8. Dans la boîte de dialogue Joindre une bibliothèque qui apparaît, choisissez le type de LTO5support, puis cliquez sur OK.
9. Développez Backup Servers pour afficher la bibliothèque de bandes virtuelles Storage Gateway et la partition de bibliothèque répertoriant tous les lecteurs de bandes montés.

Création d'un groupe de bandes

Un pool de bandes est créé dynamiquement dans le logiciel NovaStor DataCenter /Network et ne contient donc pas un nombre fixe de supports. Un groupe de bandes qui nécessite une bande obtient celle-ci dans le groupe scratch. Un groupe scratch est un réservoir de bandes mises gratuitement à la disposition d'un ou plusieurs groupes de bandes. Un groupe de bandes renvoie vers le groupe scratch tous les médias ayant dépassé leur délai de rétention et qui ne sont plus utiles.

La création d'un groupe de bandes se fait en trois étapes :

1. Créer un groupe scratch.
2. Attribuer des bandes au groupe scratch.
3. Créer un groupe de bandes.

Pour créer un groupe scratch

1. Dans le menu de navigation de gauche, sélectionnez l'onglet Scratch Pools.
2. Ouvrez le menu contextuel (clic droit) de Scratch Pools et choisissez Create Scratch Pool.
3. Dans la boîte de dialogue Scratch Pools, attribuez un nom à votre groupe scratch et choisissez votre type de média.
4. Choisissez Label Volumeet créez une limite inférieure pour le groupe scratch. Lorsque le groupe scratch atteint cette limite inférieure, un avertissement s'affiche.
5. Dans la boîte de dialogue d'avertissement qui s'affiche, choisissez OK pour créer le groupe scratch.

Pour attribuer des bandes à un groupe scratch

1. Dans le menu de navigation de gauche, choisissez Tape Library Management.
2. Sélectionnez l'onglet Library pour afficher l'inventaire de votre bibliothèque.
3. Choisissez les bandes que vous souhaitez attribuer au groupe scratch. Assurez-vous que les bandes sont définies sur le type de média approprié.
4. Ouvrez le menu contextuel (clic droit) de la bibliothèque et choisissez Add to Scratch Pool.

Vous disposez à présent d'un groupe scratch plein que vous pouvez utiliser pour les groupes de bandes.

Pour créer un groupe de bandes

1. Dans le menu de navigation de gauche, choisissez Tape Library Management.
2. Ouvrez le menu contextuel (clic droit) de l’onglet Media Pools et choisissez Create Media Pool.
3. Attribuez un nom au groupe de médias et choisissez Backup Server.
4. Choisissez une partition de bibliothèque pour le groupe de médias.
5. Choisissez le groupe scratch dans lequel vous souhaitez que le groupe récupère les bandes.
6. Pour Schedule, choisissez Not Scheduled.

Configuration de l’importation et de l’exportation de médias vers/depuis des bandes d’archivage

NovaStor DataCenter/Network can use import/exportemplacements s'ils font partie du changeur de média.

Pour une exportation, NovaStor DataCenter /Network doit savoir quelles bandes vont être physiquement retirées de la bibliothèque.

Pour une importation, NovaStor DataCenter /Network reconnaît les supports de bande exportés dans la bibliothèque de bandes et propose de les importer tous, soit depuis un emplacement de données, soit depuis un emplacement d'exportation. Votre passerelle de bande archive les bandes dans le stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive).

Pour configurer l’importation et l’exportation de médias

1. Accédez à Tape Library Management, choisissez un serveur pour Media Management Server, puis choisissez Library.
2. Sélectionnez l’onglet Off-site Locations.
3. Ouvrez le menu contextuel (clic droit) de la zone blanche et choisissez Add pour ouvrir un nouveau volet.
4. Dans le panneau, tapez **`S3 Glacier Flexible Retrieval`** ou **`S3 Glacier Deep Archive`** et ajoutez éventuellement une description dans la zone de texte.

Sauvegarde de données sur une bande

Pour créer une tâche de sauvegarde et écrire des données sur une bande virtuelle, utilisez les mêmes procédures que pour les bandes physiques. Pour obtenir des informations détaillées

sur la sauvegarde des données à l'aide du NovaStor logiciel, consultez la section NovaStor DataCenterDocumentation/Réseau.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci échouera t il sera impossible d'écrire sur la bande. Vous pouvez archiver la bande ou continuer à lire les données qu'elle contient. Pour terminer la tâche de sauvegarde qui a échoué, vous devez la soumettre à nouveau sur une nouvelle bande.

Archivage d'une bande

Lorsque vous archivez une bande, la passerelle de bande éjecte la bande du lecteur de bande vers l'emplacement de stockage. Il exporte ensuite la bande du slot vers l'archive à l'aide de votre application de sauvegarde, à savoir /Network. NovaStor DataCenter

Pour archiver une bande

1. Dans le menu de navigation de gauche, choisissez Tape Library Management.
2. Sélectionnez l'onglet Library pour afficher l'inventaire de la bibliothèque.
3. Mettez en évidence les bandes que vous voulez archiver, ouvrez le menu contextuel (clic droit) des bandes et choisissez l'emplacement d'archivage hors site.

La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT À VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande n'est plus répertoriée dans la VTL.

Dans NovaStor DataCenter /Network, vérifiez que la bande ne se trouve plus dans l'emplacement de stockage.

Dans le volet de navigation de la console Storage Gateway, sélectionnez Bandes. Vérifiez que l'état de votre bande archivée est ARCHIVÉ.

Restauration de données à partir d'une bande archivée et extraite

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Récupérez les bandes archivées de l'archive vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez le logiciel NovaStor DataCenter /Network pour restaurer les données. Pour ce faire, actualisez l'emplacement de messagerie et déplacez chaque bande à récupérer vers un emplacement vide, comme vous le faites pour restaurer des données à partir de bandes physiques. Pour plus d'informations sur la restauration des données, consultez la section NovaStor DataCenter Documentation/Réseau.

Écriture simultanée de plusieurs tâches de sauvegarde dans un lecteur de bande

Dans le NovaStor logiciel, vous pouvez écrire plusieurs tâches simultanément sur un lecteur de bande à l'aide de la fonction de multiplexage. Cette fonctionnalité est disponible lorsqu'un groupe de médias dispose d'un multiplexeur. Pour plus d'informations sur l'utilisation du multiplexage, consultez la section NovaStor DataCenterDocumentation/Network.

Résolution d'une erreur de type « External Program Did Not Exit Correctly »

Lorsque vous configurez vos appareils VTL pour qu'ils fonctionnent avec NovaStor DataCenter / Network, le message d'erreur suivant peut s'afficher. `External Program did not exit correctly` Cette erreur se produit parce que la plage d'assignation des éléments définie par Storage Gateway pour les unités de stockage et les lecteurs de bande dépasse le nombre autorisé par NovaStor DataCenter /Network.

Storage Gateway renvoie 3 200 import/export slots, which is more than the 2400 limit that NovaStor DataCenter/Network allows. To resolve this issue, you add a configuration file that activates the NovaStor software to limit the number of storage and import/export emplacements de stockage et préconfigure la plage d'assignation des éléments.

Pour appliquer la solution de contournement d'une erreur de type « external program did not exit correctly »

1. Accédez au dossier Tape de l'ordinateur sur lequel vous avez installé le NovaStor logiciel.
2. Dans le dossier de bandes, créez un fichier texte et nommez-le `hijacc.ini`.
3. Copiez le contenu qui suit et collez-le dans le fichier `hijacc.ini`, puis enregistrez le fichier.

```
port:12001
```

```
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. Ajoutez et attachez la bibliothèque au serveur de gestion de médias (Media Management Server).
5. Déplacez une bande du slot d'importation/exportation vers la bibliothèque à l'aide de la commande suivante. Remplacez le nom de bibliothèque d'exemple par le nom de la bibliothèque de votre déploiement.

   ```
   C:\Program Files\NovaStor\DataCenter\Hitback\tape\ophijacc.exe -c VTL-ec2amaz-uko8jfj-ec2amaz-uko8jfj.lcfg
   ```
6. Attachez la bibliothèque au serveur de sauvegarde.
7. Dans le NovaStor logiciel, importez toutes les cassettes depuis les emplacements d'importation/exportation vers la bibliothèque.

Test de votre configuration à l'aide de Quest NetVault Backup

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les périphériques de votre bibliothèque de bandes virtuelles (VTL) à l'aide de Quest (anciennement Dell) NetVault Backup.

Dans cette rubrique, vous trouverez une documentation de base expliquant comment configurer l'application Quest NetVault Backup pour une passerelle Tape Gateway et comment effectuer une opération de sauvegarde et de restauration.

Pour obtenir des informations détaillées sur l'utilisation de l'application Quest NetVault Backup, consultez le guide d'administration NetVault de Quest Backup. Pour plus d'informations sur les applications de sauvegarde compatibles, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Configuration de Quest NetVault Backup pour qu'il fonctionne avec les appareils VTL
- Sauvegarde des données sur bande dans le Quest NetVault Backup
- Archivage d'une bande à l'aide de Quest Backup NetVault
- Restauration de données à partir d'une bande archivée dans Quest NetVault Backup

Configuration de Quest NetVault Backup pour qu'il fonctionne avec les appareils VTL

Après avoir connecté les appareils de la bibliothèque de bandes virtuelles (VTL) au client Windows, vous configurez Quest NetVault Backup pour qu'il reconnaisse vos appareils. Pour plus d'informations sur la connexion des appareils VTL au client Windows, consultez Connexion de vos appareils VTL.

L'application Quest NetVault Backup ne reconnaît pas automatiquement les périphériques Tape Gateway. Vous devez ajouter manuellement les appareils pour les exposer à l'application Quest NetVault Backup, puis découvrir les appareils VTL.

Ajout d'appareils VTL

Pour ajouter les appareils VTL

1. Dans Quest NetVault Backup, choisissez Manage Devices dans l'onglet Configuration.
2. Sur la page Gérer les appareils, sélectionnez Ajouter des appareils.
3. Dans l'assistant d'ajout de stockage, sélectionnez Tape library / media changer (Bibliothèque de bandes/Changeur de média), puis sélectionnez Next (Suivant).
4. Sur la page suivante, choisissez l'ordinateur client qui est physiquement attaché à la bibliothèque, puis sélectionnez Next (Suivant) pour rechercher les appareils.
5. Si des appareils sont trouvés, ils sont affichés. Dans ce cas, votre changeur de média est affiché dans la zone des appareils.
6. Sélectionnez le changeur de média, puis choisissez Next (Suivant). Des informations détaillées sur l'appareil sont affichées dans l'assistant.
7. Sur la page Add Tapes to Bays (Ajouter des bandes dans les baies), sélectionnez Scan For Devices (Rechercher des appareils), sélectionnez l'ordinateur client, puis choisissez Next (Suivant).

   Quest NetVault Backup affiche tous vos disques, ainsi que les 10 baies auxquelles vous pouvez les ajouter. Les baies sont affichées une à la fois.

8. Choisissez le lecteur que vous voulez ajouter à la baie qui s'affiche, puis sélectionnez Next (Suivant).

> **Important**
>
> Lorsque vous ajoutez un lecteur à une baie, les numéros de lecteur et de baie doivent correspondre. Par exemple, si la baie 1 s'affiche, vous devez ajouter le lecteur 1. Si un lecteur n'est pas connecté, laissez la baie correspondante vide.

9. Lorsque votre ordinateur client s'affiche, choisissez-le, puis sélectionnez Next (Suivant). L'ordinateur client peut apparaître plusieurs fois.
10. Lorsque les lecteurs sont affichés, répétez les étapes 7 à 9 pour ajouter tous les lecteurs aux baies.
11. Dans l'onglet Configuration, choisissez Manage devices (Gérer les appareils), puis, sur la page Manage devices (Gérer les appareils), développez le changeur de média pour afficher les appareils que vous avez ajoutés.

Sauvegarde des données sur bande dans le Quest NetVault Backup

Vous créez une tâche de sauvegarde et vous écrivez des données sur une bande virtuelle en utilisant les mêmes procédures que pour les bandes physiques. Pour obtenir des informations détaillées sur la sauvegarde des données, consultez le guide d'administration NetVault de Quest Backup.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci échouera. Pour terminer la tâche de sauvegarde qui a échoué, vous devez la soumettre à nouveau.

Archivage d'une bande à l'aide de Quest Backup NetVault

Lorsque vous archivez une bande, la passerelle de bande éjecte la bande du lecteur de bande vers l'emplacement de stockage. Il exporte ensuite la bande du slot vers l'archive à l'aide de votre application de sauvegarde, à savoir Quest Backup NetVault .

Pour archiver une bande dans Quest NetVault Backup

1. Dans l'onglet Configuration NetVault de Quest Backup, choisissez et agrandissez votre changeur de support pour afficher vos cassettes.
2. Cliquez sur l'icône des paramètres des machines à sous pour ouvrir le navigateur de machines à sous du changeur de média.
3. Dans les emplacements, choisissez la bande que vous souhaitez archiver, puis sélectionnez Exporter.

La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT À VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande n'est plus répertoriée dans la VTL.

Dans le logiciel Quest NetVault Backup, vérifiez que la bande ne se trouve plus dans l'emplacement de stockage.

Dans le volet de navigation de la console Storage Gateway, sélectionnez Bandes. Vérifiez que l'état de votre bande archivée est ARCHIVÉ.

Restauration de données à partir d'une bande archivée dans Quest NetVault Backup

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Récupérez les bandes archivées de l'archive vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez l'application Quest NetVault Backup pour restaurer les données. Pour cela, restaurez un fichier du dossier, comme vous le faites lors de la restauration des données à partir de bandes physiques. Pour obtenir des instructions sur la création d'une tâche de restauration, consultez le guide d'administration NetVault de Quest Backup.

Étape suivante

Nettoyage des ressources inutiles

Tester votre configuration à l'aide de Veeam Backup and Replication

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les appareils de votre bibliothèque de bandes virtuelles (VTL) à l'aide de Veeam Backup & Replication. Dans cette rubrique, vous trouverez une documentation de base sur la configuration du logiciel Veeam Backup & Replication pour une passerelle de bande, et sur les opérations de sauvegarde et de restauration. Pour des informations détaillées sur l'utilisation du logiciel Veeam, consultez la documentation de Veeam Backup & Replication. Pour plus d'informations sur les applications de sauvegarde compatibles, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Configuration de Veeam pour utiliser les appareils VTL
- Importation d'une bande dans Veeam
- Sauvegarde des données sur une bande dans Veeam
- Archivage d'une bande à l'aide de Veeam
- Restauration des données d'une bande archivée dans Veeam

Configuration de Veeam pour utiliser les appareils VTL

Une fois que vous avez connecté les appareils de la bibliothèque de bandes virtuelles (VTL) au client Windows, vous configurez Veeam Backup & Replication pour identifier vos appareils. Pour plus d'informations sur la connexion des appareils VTL au client Windows, consultez Connexion de vos appareils VTL.

Mise à jour de pilotes d'appareils VTL

Pour configurer le logiciel de façon à ce qu'il fonctionne avec les appareils d'une passerelle de bande, mettez à jour les pilotes des appareils VTL pour les exposer au logiciel Veeam, afin qu'il puisse détecter les appareils VTL. Dans le gestionnaire d'appareils, mettez à jour le pilote du changeur de média. Pour obtenir des instructions, consultez Mise à jour le pilote d'appareil pour votre changeur de média.

Découverte des appareils VTL

Vous devez utiliser les commandes SCSI natives au lieu d'un pilote Windows pour découvrir votre bibliothèque de bandes si votre changeur de média est inconnu. Pour obtenir des instructions détaillées, consultez Bibliothèques de bandes.

Pour découvrir les appareils VTL

1. Dans le logiciel Veeam, sélectionnez Tape infrastructure (Infrastructure de bande). Lorsque la passerelle de bande est connectée, les bandes virtuelles sont indiquées dans l'onglet Backup Infrastructure (Infrastructure de sauvegarde).
2. Développez l'arborescence Bandes pour afficher les lecteurs de bandes et le changeur de média.
3. Développez l'arborescence du changeur de média. Si vos lecteurs de bandes sont mappés au changeur de média, les lecteurs apparaissent sous Lecteurs. Dans le cas contraire, votre bibliothèque de bandes et les lecteurs de bandes apparaissent comme des appareils distincts.

   Si les lecteurs ne sont pas mappés automatiquement, suivez les instructions sur le site Web de Veeam pour mapper les lecteurs.

Importation d'une bande dans Veeam

Vous êtes maintenant prêt à importer des bandes de votre passerelle de bande vers la bibliothèque de l'application de sauvegarde Veeam.

Pour importer une bande dans la bibliothèque Veeam

1. Ouvrez le menu contextuel (clic droit) pour le changeur de média, puis choisissez Importer pour importer les bandes dans les emplacements I/E.
2. Ouvrez le menu contextuel (clic droit) pour le changeur de média, puis choisissez Bibliothèque d'inventaire afin d'identifier les bandes non reconnues. Lorsque vous chargez une nouvelle bande virtuelle dans un lecteur de bandes pour la première fois, la bande n'est pas reconnue par l'application de sauvegarde Veeam. Pour identifier la bande non reconnue, vous faites l'inventaire les bandes de la bibliothèque.

Sauvegarde des données sur une bande dans Veeam

La sauvegarde des données sur une bande est un processus en deux étapes :

1. Vous créez un pool de médias et vous lui ajoutez la bande.
2. Vous écrivez les données sur la bande.

Vous créez pool de médias et vous écrivez des données sur une bande virtuelle en utilisant les mêmes procédures que pour les bandes physiques. Pour obtenir des informations détaillées sur la sauvegarde des données, consultez le document Getting Started with Tapes (Débuter avec les bandes) dans le centre d'assistance de Veeam.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci échouera. Pour terminer la tâche de sauvegarde qui a échoué, vous devez la soumettre à nouveau.

Archivage d'une bande à l'aide de Veeam

Lorsque vous archivez une bande, la passerelle de bande la transfère de la bibliothèque de bandes Veeam vers le stockage hors connexion. Vous commencez l'archivage en éjectant la bande du lecteur de bande vers l'emplacement de stockage, puis en exportant la bande de l'emplacement vers l'archive à l'aide de votre application de sauvegarde, le logiciel Veeam.

Pour archiver une bande dans la bibliothèque Veeam

1. Choisissez Tape infrastructure, puis sélectionnez le pool de médias qui contient la bande que vous voulez archiver.
2. Ouvrez le menu contextuel (clic droit) pour la bande que vous voulez archiver, puis choisissez Ejecter la bande.
3. Pour la zone Ejection de la bande, choisissez Fermer. L'emplacement de la bande passe d'un lecteur de bandes à un emplacement.
4. Ouvrez à nouveau le menu contextuel (clic droit) pour la bande, puis choisissez Exporter. Le statut de la bande passe de Lecteur de bandes à Hors connexion.
5. Pour Exportation de la bande, choisissez Fermer. L'emplacement de la bande passe de Emplacement à Hors connexion.
6. Sur la console Storage Gateway, sélectionnez votre passerelle, puis choisissez Cartouches de bandes VTL et vérifiez le statut de la bande virtuelle que vous archivez.

   La réalisation du processus d'archivage peut prendre du temps. L'état initial de la bande est EN COURS D'ACHEMINEMENT À VTS. Lorsque l'archivage commence, l'état passe à ARCHIVAGE. Une fois l'archivage terminé, la bande éjectée n'est plus répertoriée dans la

bibliothèque de bandes virtuelles (VTL), mais elle est archivée dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

Restauration des données d'une bande archivée dans Veeam

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Récupérez les bandes archivées de l'archive vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez le logiciel Veeam pour restaurer les données. Pour cela, restaurez un fichier du dossier, comme vous le faites lors de la restauration des données à partir de bandes physiques. Pour plus d'informations, consultez Restoring Files from Tape (Restauration des fichiers des bandes) dans le centre d'assistance de Veeam.

Étape suivante

Nettoyage des ressources inutiles

Test de votre configuration à l'aide de Veritas Backup Exec

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les appareils de la bibliothèque de bandes virtuelles (VTL) à l'aide de Veritas Backup Exec. Dans cette rubrique, vous trouverez la documentation de base nécessaire pour effectuer des opérations de sauvegarde et de restauration à l'aide de Backup Exec.

Pour des informations plus détaillées sur l'utilisation de Backup Exec, notamment sur la création de sauvegardes sécurisées, des listes de compatibilité logicielle et matérielle, ainsi que des guides d'administration, consultez le site Web d'assistance de Veritas.

Pour plus d'informations sur les applications de sauvegarde prises en charge, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Configuration du stockage dans Backup Exec
- Importation d'une bande dans Backup Exec
- Ecriture des données sur une bande Backup Exec

- Archivage d'une bande à l'aide de Backup Exec
- Restauration des données d'une bande archivée dans Backup Exec
- Désactivation d'un lecteur de bande dans Backup Exec

Configuration du stockage dans Backup Exec

Une fois que vous avez connecté les appareils de la bibliothèque de bandes virtuelles (VTL) au client Windows, vous configurez le stockage Backup Exec pour identifier vos appareils. Pour plus d'informations sur la connexion des appareils VTL au client Windows, consultez Connexion de vos appareils VTL.

Pour configurer le stockage

1. Démarrez le logiciel Backup Exec, puis choisissez l'icône jaune dans le coin supérieur gauche de la barre d'outils.
2. Choisissez Configuration and Settings (Configuration et paramètresmètres), puis sélectionnez Backup Exec Services (Services Backup Exec) pour ouvrir le Gestionnaire de services Backup Exec.
3. Choisissez Redémarrer tous les services. Backup Exec reconnaît ensuite les appareils VTL (c'est-à-dire, le changeur de média et les lecteurs de bandes). Le processus de redémarrage peut prendre quelques minutes.

   > **Note**
   >
   > Une passerelle de bande fournit 10 lecteurs de bande. Toutefois, votre contrat de licence Backup Exec peut avoir besoin de votre application de sauvegarde pour travailler avec moins de 10 lecteurs de bandes. Dans ce cas, vous devez désactiver les lecteurs de bandes dans la bibliothèque de robots Backup Exec pour laisser uniquement le nombre de lecteurs de bandes autorisé par votre contrat de licence activé. Pour obtenir des instructions, consultez Désactivation d'un lecteur de bande dans Backup Exec .

4. Une fois le redémarrage terminé, fermez le Backup Exec Service Manager.

Importation d'une bande dans Backup Exec

Vous êtes maintenant prêt à importer une bande de votre passerelle vers un emplacement.

1. Choisissez l'onglet Stockage, puis développez l'arborescence Bibliothèque de robots pour afficher les appareils VTL.

   > **Important**
   >
   > Le logiciel Veritas Backup Exec requiert le type de changeur de média de passerelle de bande. Si le type de changeur de média répertorié sous Bibliothèque de robots n'est pas passerelle de bande, vous devez le modifier avant de configurer le stockage dans l'application de sauvegarde. Pour plus d'informations sur la sélection d'un type de changeur de média, consultez Sélection d'un changeur de média après l'activation de la passerelle.

2. Choisissez l'icône Emplacements pour afficher tous les emplacements.

   > **Note**
   >
   > Lorsque vous importez des bandes dans la bibliothèque de robots, les bandes sont stockées dans les emplacements au lieu de lecteurs de bandes. Par conséquent, les lecteurs de bandes peuvent avoir un message indiquant qu'il n'existe aucun média dans les lecteurs (aucun média). Lorsque vous lancez une tâche de sauvegarde ou de restauration, les bandes sont transférées vers les lecteurs de bandes.
   > Vous devez avoir des bandes disponibles dans la bibliothèque de bandes de la passerelle pour importer une bande dans un emplacement de stockage. Pour obtenir des instructions sur la création des bandes, consultez Création de nouvelles bandes virtuelles pour Tape Gateway.

3. Ouvrez le menu contextuel (clic droit) pour afficher un emplacement vide, choisissez Importer, puis sélectionnez Importer le média maintenant. Vous pouvez sélectionner plusieurs emplacements et importer plusieurs bandes au cours d'une seule opération d'importation.
4. Dans la fenêtre Demande de média qui s'affiche, choisissez Afficher les détails.
5. Dans la fenêtre Alerte action : Intervention sur le média, choisissez Répondre OK pour insérer le média dans l'emplacement.

   La bande s'affiche dans l'emplacement que vous avez sélectionné.

> **Note**
>
> Les bandes qui sont importées incluent des bandes vides et des bandes qui ont été extraites de l'archive et transférées sur la passerelle.

Ecriture des données sur une bande Backup Exec

Vous écrivez des données sur une bande virtuelle de la passerelle de bande en utilisant les mêmes procédures et politiques de sauvegarde qu'avec les bandes physiques. Pour des informations détaillées, consultez le Guide d'administration de Backup Exec dans la section de la documentation consacrée au logiciel Backup Exec.

> **Note**
>
> Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci risque d'échouer. Si la tâche de sauvegarde échoue, le statut de la bande dans Veritas Backup Exec passe à Non annexable. Vous pouvez archiver la bande ou continuer à lire les données qu'elle contient. Pour terminer la tâche de sauvegarde qui a échoué, vous devez la soumettre à nouveau sur une nouvelle bande.

Archivage d'une bande à l'aide de Backup Exec

Lorsque vous archivez une bande, la passerelle de bande la transfère de la bibliothèque de bandes virtuelles (VTL) de votre passerelle vers le stockage hors connexion. Vous commencez l'archivage des bandes en exportant la bande à l'aide de votre logiciel Backup Exec.

Pour archiver votre bande

1. Choisissez le menu Stockage, sélectionnez Emplacements, ouvrez le menu contextuel (clic droit) pour l'emplacement à partir duquel vous voulez exporter les bandes, sélectionnez Exporter le média, puis choisissez Exporter le média maintenant. Vous pouvez sélectionner plusieurs emplacements et exporter plusieurs bandes au cours d'une seule opération d'exportation.
2. Dans la fenêtre contextuelle Requête de média, choisissez Afficher les détails, puis choisissez Répondre OK dans la fenêtre Alerte : Intervention sur le média.

Dans la console Storage Gateway, vous pouvez vérifier le statut de la bande vous archivez. Le chargement des données vers AWS peut prendre du temps. Pendant ce temps, la bande exportée figure dans la VTL de la passerelle de bande avec l'état EN COURS D'ACHEMINEMENT A VTS. Lorsque le chargement est terminé et que le processus d'archivage commence, le statut passe à ARCHIVAGE. Une fois l'archivage terminé, la bande éjectée n'est plus répertoriée dans la bibliothèque de bandes virtuelles (VTL), mais elle est archivée dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

3. Sélectionnez votre passerelle, puis choisissez Cartouches de bande VTL et vérifiez que la bande virtuelle n'est plus répertoriée dans votre passerelle.
4. Dans le volet de navigation de la console Storage Gateway, sélectionnez Bandes. Vérifiez que le statut de la bande est ARCHIVÉ.

Restauration des données d'une bande archivée dans Backup Exec

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Extrayez la bande archivée vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez Backup Exec pour restaurer les données. Ce processus est le même que celui de la restauration des données des bandes physiques. Pour des instructions supplémentaires, consultez le Guide d'administration de Backup Exec dans la section de la documentation consacrée au logiciel Backup Exec.

Désactivation d'un lecteur de bande dans Backup Exec

Une passerelle de bande fournit 10 lecteurs de bandes, mais vous pouvez décider d'en utiliser moins. Dans ce cas, vous désactivez les lecteurs de bandes que vous n'utilisez pas.

1. Ouvrez Backup Exec, puis choisissez l'onglet Stockage.
2. Dans l'arborescence Bibliothèque de robots, ouvrez le menu contextuel (clic droit) pour le lecteur de bandes que vous souhaitez désactiver, puis choisissez Désactiver.

Étape suivante

Nettoyage des ressources inutiles

Tester votre configuration à l'aide de Veritas NetBackup

Vous pouvez sauvegarder vos données sur des bandes virtuelles, archiver les bandes et gérer les appareils de votre bibliothèque de bandes virtuelles (VTL) à l'aide de NetBackup Veritas. Dans cette rubrique, vous trouverez une documentation de base sur la configuration de l' NetBackup application pour une passerelle sur bande et sur l'exécution d'une opération de sauvegarde et de restauration.

Pour des informations détaillées sur son utilisation NetBackup, consultez la page Veritas Services and Operations Readiness Tools (SORT) sur le site Web de Veritas.

Pour plus d'informations sur les applications de sauvegarde compatibles, consultez Applications de sauvegarde tierces prises en charge pour une passerelle de bande.

Rubriques

- Configuration des périphériques NetBackup de stockage
- Sauvegarde de données sur une bande
- Archivage de la bande
- Restauration des données de la bande

Configuration des périphériques NetBackup de stockage

Après avoir connecté les appareils de la bibliothèque de bandes virtuelles (VTL) au client Windows, vous configurez le NetBackup stockage Veritas pour qu'il reconnaisse vos appareils. Pour plus d'informations sur la connexion des appareils VTL au client Windows, consultez Connexion de vos appareils VTL.

NetBackup Pour configurer l'utilisation de périphériques de stockage sur votre Tape Gateway

1. Ouvrez la console NetBackup d'administration en tant qu'administrateur.
2. Choisissez Configurer les appareils de stockage pour ouvrir l'assistant de configuration des appareils.
3. Choisissez Suivant. L' NetBackup application détecte votre ordinateur en tant qu'hôte de l'appareil.
4. Dans la colonne Hôtes de l'appareil, sélectionnez l'ordinateur, puis choisissez Suivant. L' NetBackup application analyse votre ordinateur à la recherche d'appareils et découvre tous les appareils.

5. Sur la page Numérisation des hôtes, choisissez Suivant, puis encore Suivant. L' NetBackup application détecte les 10 lecteurs de bande et le changeur de support de votre ordinateur.
6. Dans la fenêtre Dispositifs de sauvegarde, choisissez Suivant.
7. Dans la fenêtre Configuration de glisser et déposer, vérifiez que le changeur de média a bien été sélectionné, puis choisissez Suivant.
8. Dans la boîte de dialogue qui s’affiche, sélectionnez Oui pour enregistrer la configuration sur votre ordinateur. L' NetBackup application met à jour la configuration de l'appareil.
9. Lorsque la mise à jour est terminée, choisissez Next pour mettre les appareils à la disposition de l' NetBackup application.
10. Dans la fenêtre Finished!, choisissez Finish.

Pour vérifier vos appareils dans l' NetBackup application

1. Dans la console d' NetBackup administration, développez le nœud Gestion des médias et des appareils, puis développez le nœud Appareils. Choisissez Lecteurs pour afficher tous les lecteurs de la bande.
2. Dans le nœud Appareils, sélectionnez Robots pour afficher tous vos changeurs de médias. Dans l' NetBackup application, le changeur de média est appelé robot.
3. Dans le volet Tous les robots, ouvrez le menu contextuel (clic droit) pour TLD(0) (c’est-à-dire, votre robot), puis choisissez Inventaire des robots.
4. Dans la fenêtre Inventaire des robots, vérifiez que votre hôte est sélectionné dans la liste Appareil-Hôte située dans la catégorie Sélectionner le robot.
5. Vérifiez que votre robot est sélectionné dans la liste Robot.
6. Dans la fenêtre Inventaire des robots, sélectionnez Mettre à jour la configuration du volume, sélectionnez Aperçu des modifications, sélectionnez Vider le port d’accès au média avant la mise à jour, puis choisissez Commencer.

   Le processus répertorie ensuite votre changeur de support et vos bandes virtuelles dans la base de données de gestion des médias NetBackup d'entreprise (EMM). NetBackup stocke les informations relatives au support, à la configuration du périphérique et à l'état de la bande dans l'EMM.
7. Dans la fenêtre Inventaire des robots, choisissez Oui une fois que l’inventaire est terminé. Si vous choisissez Oui ici, la configuration est mise à jour et les bandes virtuelles trouvées dans les emplacements d’importation/exportation sont transférées dans la bibliothèque de bandes virtuelles.

8. Fermez la fenêtre Inventaire des robots.
9. Dans le nœud Média, développez le nœud Robots et choisissez TLD(0) pour afficher toutes les bandes virtuelles qui sont disponibles pour votre robot (changeur de média).

> **Note**
>
> Si vous avez déjà connecté d'autres appareils à l' NetBackupapplication, il se peut que vous disposiez de plusieurs robots. Veillez à sélectionner le bon robot.

Maintenant que vous avez connecté vos appareils et que vous les avez mis à disposition de l'application de sauvegarde, vous êtes prêt à tester votre passerelle. Pour tester votre passerelle, sauvegardez les données sur les bandes virtuelles que vous avez créé et archivez les bandes.

Sauvegarde de données sur une bande

Vous testez la configuration de la passerelle de bande en sauvegardant les données sur vos bandes virtuelles.

> **Note**
>
> - Vous devez sauvegarder uniquement une petite quantité de données pour cet exercice de mise en route, car des coûts sont associés au stockage, à l'archivage et à la récupération des données. Pour plus d'information sur les tarifs, consultez Tarification sur la page de détails de Storage Gateway.
> - Si votre passerelle de bande redémarre pour une raison quelconque au cours d'une tâche de sauvegarde en cours, celle-ci sera suspendue. La tâche de sauvegarde suspendue reprendra automatiquement lorsque votre passerelle aura fini de redémarrer.

Pour créer un pool de volumes

Un pool de volumes est un ensemble de bandes virtuelles à utiliser pour une sauvegarde.

1. Démarrez la console NetBackup d'administration.
2. Développez le nœud Média, ouvrez le menu contextuel (clic droit) pour Pool de volumes, puis choisissez Nouveau. La boîte de dialogue Nouveau pool de volumes s'affiche.

3. Pour Nom, tapez le nom du pool de volumes.
4. Pour Description, entrez une description du pool de volumes, puis choisissez OK. Le pool de volumes que vous venez de créer est ajouté à la liste de pools de volumes.

   La capture d'écran suivante affiche une liste des pools de volumes.

Pour ajouter des bandes virtuelles à un pool de volumes

1. Développez le nœud Robots et sélectionnez le robot TLD(0) pour afficher les bandes virtuelles que ce robot connaît.

   Si vous avez connecté un robot précédemment, votre robot de passerelle de bande peut avoir un nom différent.
2. Dans la liste de bandes virtuelles, ouvrez le menu contextuel (clic droit) pour la bande que vous voulez ajouter au pool de volumes, puis sélectionnez Modifier pour ouvrir la boîte de dialogue Modifier les volumes.
3. Pour Pool de volumes, choisissez Nouveau pool.
4. Pour Nouveau pool, sélectionnez le pool que vous venez de créer et choisissez OK.

   Vous pouvez vérifier que votre pool de volumes contient la bande virtuelle que vous venez d'ajouter en développant le nœud Média et en choisissant votre pool de volumes.

Pour créer une politique de sauvegarde

La stratégie de sauvegarde spécifie les données à sauvegarder, quand les sauvegarder et le pool de volumes à utiliser.

1. Choisissez votre serveur principal pour revenir à la NetBackup console Veritas.
2. Choisissez Créer une stratégie pour ouvrir la fenêtre Assistant de configuration de stratégie.
3. Sélectionnez Systèmes de fichiers, bases de données, applications, puis choisissez Suivant.
4. Pour Nom de la stratégie, tapez le nom de la stratégie et vérifiez que MS-Windows est sélectionné dans la liste Sélectionner le type de stratégie, puis choisissez Suivant.
5. Dans la fenêtre Liste de clients, choisissez Ajouter, tapez le nom de l'hôte de l'ordinateur dans la colonne Nom, puis choisissez Suivant. Cette étape s'applique à la stratégie que vous définissez pour `localhost` (votre ordinateur client).
6. Dans la fenêtre Fichiers, choisissez Ajouter, puis choisissez l'icône de dossier.

7. Dans la fenêtre Parcourir, recherchez le dossier ou les fichiers que vous souhaitez sauvegarder, choisissez OK, puis sélectionnez Suivant.
8. Dans la fenêtre Types de sauvegarde, acceptez les valeurs par défaut, puis choisissez Suivant.

> **Note**
>
> Si vous souhaitez lancer la sauvegarde vous-même, sélectionnez Sauvegarde utilisateur.

9. Dans la fenêtre Fréquence et conservation, sélectionnez la stratégie de fréquence et de conservation que vous souhaitez appliquer à la sauvegarde. Pour cet exercice, vous pouvez accepter toutes les valeurs par défaut et choisir Next.
10. Dans la fenêtre Commencer, sélectionnez Heures creuses, puis choisissez Suivant. Cette sélection spécifie que votre dossier doit être sauvegardé pendant les heures creuses seulement.
11. Dans l'assistant Configuration de la stratégie, sélectionnez Terminer.

La stratégie exécute les sauvegardes selon la planification. Vous pouvez également effectuer une sauvegarde manuelle à tout moment, ce que nous décrit l'étape suivante.

Pour effectuer une sauvegarde manuelle

1. Dans le volet de navigation de la NetBackup console, développez le nœud NetBackup de gestion.
2. Développez le nœud Politiques.
3. Ouvrez le menu contextuel (clic droit) de la stratégie et choisissez Sauvegarde manuelle.
4. Dans la fenêtre Sauvegarde manuelle, sélectionnez une planification, sélectionnez un client, puis choisissez OK.
5. Dans la boîte de dialogue Sauvegarde manuelle démarrée qui s'affiche, choisissez OK.
6. Dans le volet de navigation, choisissez Moniteur d'activité pour afficher l'état de votre sauvegarde dans la colonne ID de la tâche.

Pour trouver le code-barres de la bande virtuelle sur laquelle NetBackup ont été écrites les données du fichier lors de la sauvegarde, consultez la fenêtre Job Details, comme décrit dans la procédure suivante. Vous avez besoin de ce code à barres dans la procédure de la section suivante, où vous archivez la bande.

Pour trouver le code à barres d'une bande

1. Dans Moniteur d'activité, ouvrez le menu contextuel (clic droit) pour l'identifiant de la tâche de sauvegarde dans la colonne ID de la tâche, puis choisissez Détails.
2. Dans la fenêtre Détails de la tâche, choisissez l'onglet État détaillé.
3. Dans la zone État, recherchez l'ID du média. Par exemple, une entrée du rapport d'état peut se lire comme suit `media id 87A222` : Cet ID vous permet de déterminer sur quelle bande vous avez écrit les données.

Vous avez maintenant déployé une passerelle de bande, créé des bandes virtuelles et sauvegardé vos données. Vous pouvez ensuite archiver les bandes virtuelles et les extraire de l'archive.

Archivage de la bande

Lorsque vous archivez une bande, la passerelle de bande la transfère de la bibliothèque de bandes virtuelles (VTL) de votre passerelle vers l'archive, qui fournit un stockage hors connexion. Vous lancez l'archivage de la bande en éjectant celle-ci à l'aide de votre application de sauvegarde.

Pour archiver une bande virtuelle

1. Dans la console d' NetBackup administration, développez le nœud Gestion des médias et des appareils, puis étendez le nœud Media.
2. Développez Robots, puis choisissez TLD(0).
3. Ouvrez le menu contextuel (clic droit) pour la bande virtuelle que vous souhaitez archiver, puis sélectionnez Ejecter le volume du robot.
4. Dans la fenêtre Ejecter les volumes, assurez-vous que l'ID du média correspond à la bande virtuelle que vous voulez éjecter, puis choisissez Ejecter.
5. Dans la boîte de dialogue, choisissez Oui.

   Une fois l'éjection terminée, le statut de la bande dans la boîte de dialogue Ejecter les volumes indique que l'éjection a réussi.
6. Choisissez Fermer pour fermer la fenêtre Ejecter les volumes.
7. Dans la console Storage Gateway, vérifiez le statut de la bande archivée dans la VTL de la passerelle. Le chargement des données vers AWS peut prendre du temps. Pendant ce temps, la bande éjectée est listée dans la VTL de la passerelle avec l'état EN TRANSIT VERS VTS. Lorsque l'archivage commence, le statut est ARCHIVAGE. Une fois le chargement des données

terminé, la bande éjectée n'est plus répertorié dans la VTL, mais elle est archivée dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

8. Pour vérifier que la bande virtuelle n'est plus répertoriée sur la passerelle, sélectionnez cette dernière, puis choisissez Cartouches de bandes VTL.
9. Dans le volet de navigation de la console Storage Gateway, sélectionnez Bandes. Vérifiez que l'état de votre bande archivée est ARCHIVÉ.

Restauration des données de la bande

La restauration des données archivées est un processus en deux étapes.

Pour restaurer les données d'une bande archivée

1. Extrayez la bande archivée vers une passerelle de bande. Pour obtenir des instructions, consultez Récupération des bandes archivées.
2. Utilisez le logiciel de sauvegarde, d'archivage et de restauration installé avec l' NetBackup application Veritas. Ce processus est le même que celui de la restauration des données des bandes physiques. Pour obtenir des instructions, consultez la section Veritas Services and Operations Readiness Tools (SORT) sur le site web de Veritas.

Étape suivante

Nettoyage des ressources inutiles

Comment procéder ensuite ?

Une fois que votre passerelle de bande est en production, vous pouvez exécuter plusieurs tâches de maintenance, telles que l'ajout et la suppression de bandes, la surveillance et l'optimisation des performances de passerelle, ainsi que le dépannage. Pour accéder à des informations génériques sur ces tâches de gestion, consultez Gestion de votre Tape Gateway.

Vous pouvez effectuer certaines tâches de maintenance de Tape Gateway sur le AWS Management Console, telles que la configuration des limites de débit de bande passante de votre passerelle et la gestion des mises à jour logicielles de la passerelle. Si votre passerelle de bande est déployée sur site, vous pouvez exécuter certaines tâches de maintenance sur la console locale de la passerelle. Cela inclut le routage de votre passerelle de bande via un proxy et sa configuration pour qu'elle utilise

une adresse IP statique. Si vous exécutez votre passerelle en tant qu' EC2 instance Amazon, vous pouvez effectuer des tâches de maintenance spécifiques sur la EC2 console Amazon, telles que l'ajout et la suppression de volumes Amazon EBS. Pour plus d'informations sur la maintenance de votre passerelle de bande, consultez Gestion de votre Tape Gateway.

Si vous avez l'intention de déployer votre passerelle en production, vous devez tenir compte de votre charge de travail réelle pour déterminer la taille des disques. Pour plus d'informations sur la définition de la taille réelle des disques, consultez Gestion des disques locaux pour Storage Gateway. De plus, envisagez un nettoyage si vous n'avez pas l'intention de continuer à utiliser votre passerelle de bande. Le nettoyage vous permet d'éviter des frais. Pour plus d'informations sur le nettoyage, consultez Nettoyage des ressources inutiles.

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 lui permettre de 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 de VPC pour Storage Gateway et obtenez l'ID de point de terminaison de VPC, puis spécifiez cet ID de point de terminaison de VPC lorsque vous créez et activez la passerelle. Pour plus d'informations, consultez Connecter votre passerelle de bande pour AWS .

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

Rubriques

- Création d'une passerelle à l'aide d'un point de terminaison de VPC pour Storage Gateway

Création d'une passerelle à l'aide d'un point de terminaison de VPC pour Storage Gateway

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

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 Enable Private DNS Name (Activer le nom DNS privé) n'est pas sélectionné.
7. Pour Groupe de sécurité, choisissez le groupe de sécurité que vous souhaitez utiliser pour votre VPC. Vous pouvez accepter le groupe de sécurité par défaut. Vérifiez que tous les ports TCP suivants sont autorisés dans votre groupe de sécurité :
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Choisissez 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 ressemble à ceci : `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Maintenant que vous disposez d'un point de terminaison de VPC, vous pouvez créer votre passerelle. Pour plus d'informations, consultez Création de passerelle.

Gestion de votre Tape Gateway

La gestion de votre passerelle inclut des tâches telles que la configuration du stockage en cache et de l'espace tampon de téléchargement, l'utilisation de , de bandes virtuelles et la maintenance générale. Si vous n'avez pas créé de passerelle, consultez Commencer avec AWS Storage Gateway.

Vous trouverez ci-dessous des informations sur la gestion de vos ressources Tape Gateway.

Rubriques

- Modification des informations de base de la passerelle- Découvrez comment 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.
- Gestion de la création automatique de bandes- Découvrez comment configurer Tape Gateway pour créer automatiquement de nouvelles bandes virtuelles afin de maintenir le nombre minimum de bandes disponibles que vous spécifiez.
- Archivage des bandes virtuelles- Découvrez comment configurer l'archivage de vos bandes selon la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive lorsque vous créez une nouvelle bande.
- Déplacement de bandes vers la classe de stockage S3 Glacier Deep Archive- Découvrez comment transférer vos bandes de S3 Glacier Flexible Retrieval vers S3 Glacier Deep Archive pour une conservation des données à long terme et une préservation numérique à très faible coût.
- Récupération des bandes archivées- Découvrez comment accéder aux données stockées sur une bande virtuelle archivée en récupérant d'abord la bande sur votre Tape Gateway.
- Affichage des statistiques d'utilisation des cassettes- Découvrez comment afficher la quantité de données stockées sur une bande à l'aide de la console Storage Gateway.
- Suppression de bandes virtuelles de votre Tape Gateway- Découvrez comment supprimer des bandes virtuelles de votre Tape Gateway à l'aide de la console Storage Gateway.
- Suppression de groupes de bandes personnalisés- Découvrez comment supprimer un pool de bandes personnalisé à l'aide de la console Storage Gateway.
- Désactivation de votre passerelle de bande- Découvrez comment désactiver une passerelle de bande si celle-ci est défaillante et que vous souhaitez récupérer les bandes de la passerelle défaillante vers une autre passerelle.

- Comprendre l'état de la bande- Découvrez les différentes valeurs d'état des bandes indiquées par Storage Gateway pour déterminer si une bande fonctionne normalement ou si un problème nécessite une intervention de votre part.
- Déplacement de vos données vers une nouvelle passerelle- Découvrez comment déplacer des données entre les passerelles au fur et à mesure que vos besoins en données et en performances augmentent, ou si vous recevez une AWS notification vous demandant de migrer votre passerelle.

Modification des informations de base de la passerelle

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.

Gestion de la création automatique de bandes

La passerelle de bande crée automatiquement de nouvelles bandes virtuelles pour conserver le nombre minimal de bandes disponibles que vous configurez. Elle rend ensuite ces nouvelles bandes disponibles pour l'importation par l'application de sauvegarde, afin que vos tâches de sauvegarde puissent s'exécuter sans interruption. La création automatique de bandes élimine le besoin de créer des scripts personnalisés en plus du processus manuel de création de bandes virtuelles.

Pour supprimer une stratégie de création automatique de bandes

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez l'onglet Passerelles.
3. Choisissez la passerelle pour laquelle vous devez gérer la création automatique de bandes.
4. Dans le menu Actions, choisissez Configure tape auto-create (Configurer la création automatique de bandes).
5. Pour supprimer une stratégie de création automatique de bandes sur une passerelle, choisissez Supprimer à droite de la stratégie à supprimer.

   Pour arrêter la création automatique de bandes sur une passerelle, supprimez toutes les politiques de création automatique de bandes pour cette passerelle.

Choisissez Enregistrer les modifications pour confirmer la suppression des politiques de création automatique de bandes pour la passerelle de bande sélectionnée.

> **Note**
>
> La suppression d'une stratégie de création automatique de bandes d'une passerelle ne peut pas être annulée.

Pour modifier les politiques de création automatique de bandes pour une passerelle de bande

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez l'onglet Passerelles.
3. Choisissez la passerelle pour laquelle vous devez gérer la création automatique de bandes.
4. Dans le menu Actions, choisissez Configurer la création automatique des bandes et modifiez les paramètres sur la page qui apparaît.
5. Pour Nombre minimum de bandes, entrez le nombre minimum de bandes virtuelles qui doivent être disponibles sur la passerelle de bande à tout moment. La plage valable pour cette valeur va de 1 à 10.
6. Pour Capacity (Capacité), entrez la taille, en octets, de la capacité de bande virtuelle. La plage valable pour cette valeur va de 100 Gio à 15 Tio.
7. Pour Barcode prefix (Préfixe de code-barres), entrez le préfixe que vous souhaitez ajouter au code à barres de vos bandes virtuelles.

   > **Note**
   >
   > Les bandes virtuelles sont identifiées de manière unique par un code-barres et vous pouvez ajouter un préfixe à ce dernier. Le préfix est facultatif, mais vous pouvez l'utiliser pour faciliter l'identification de vos bandes virtuelles. Le préfixe doit être en majuscules (A-Z) et comporter entre un et quatre caractères.

8. Pour Pool, choisissez Glacier Pool ou Deep Archive Pool. Ce pool représente la classe de stockage dans laquelle vos bandes sont stockées lorsqu'elles sont éjectées par votre logiciel de sauvegarde.

- Choisissez Groupe Glacier si vous souhaitez archiver les bandes dans la classe de stockage S3 Glacier Flexible Retrieval. Lorsque le logiciel de sauvegarde éjecte les bandes, elle sont automatiquement archivées dans S3 Glacier Flexible Retrieval. Vous utilisez S3 Glacier Flexible Retrieval pour des archives plus actives, au sein desquelles vous pouvez récupérer une bande dans un délai compris entre 3 et 5 heures. Pour obtenir des informations détaillées, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.
- Vous choisissez Groupe Deep Archive si vous souhaitez archiver la bande dans S3 Glacier Deep Archive. Lorsque le logiciel de sauvegarde éjecte la bande, celle-ci est automatiquement archivée dans S3 Glacier Deep Archive. Vous utilisez S3 Glacier Deep Archive pour la conservation des données à long terme et l'archivage numérique où les données sont consultées une à deux fois par an. Vous pouvez extraire une bande archivée dans S3 Glacier Deep Archive généralement dans un délai de 12 heures. Pour obtenir des informations détaillées, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.

Si vous archivez des bandes dans S3 Glacier Flexible Retrieval, vous pouvez les déplacer ultérieurement vers S3 Glacier Deep Archive. Pour plus d'informations, consultez Déplacement de bandes vers la classe de stockage S3 Glacier Deep Archive.

9. Vous trouverez des informations au sujet des bandes sur la page de Présentation de la bande. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.

   L'état des bandes virtuelles disponibles est défini initialement sur CRÉATION lorsque les bandes sont créées. Une fois les bandes créées, leur état passe à DISPONIBLE. Pour de plus amples informations, veuillez consulter Comprendre l'état de la bande.

   Pour plus d'informations sur l'activation de la création automatique de bandes, consultez Création automatique des bandes.

Archivage des bandes virtuelles

Vous pouvez archiver vos bandes dans S3 Glacier Flexible Retrieval ou dans S3 Glacier Deep Archive. Lorsque vous créez une bande, vous choisissez le pool d'archives que vous souhaitez utiliser pour archiver votre celle-ci.

Choisissez Groupe Glacier si vous souhaitez archiver la bande dans S3 Glacier Flexible Retrieval. Lorsque le logiciel de sauvegarde éjecte la bande, elle est automatiquement archivée dans S3 Glacier Flexible Retrieval. Vous utilisez S3 Glacier Flexible Retrieval pour des archives plus actives dans lesquelles les données sont régulièrement récupérées et nécessaires en quelques minutes. Pour plus d'informations, consultez Classes de stockage pour l'archivage des objets.

Vous choisissez Groupe Deep Archive si vous souhaitez archiver la bande dans S3 Glacier Deep Archive. Lorsque le logiciel de sauvegarde éjecte la bande, celle-ci est automatiquement archivée dans S3 Glacier Deep Archive. Vous utilisez S3 Glacier Deep Archive pour la conservation des données à long terme et la préservation numérique à très faible coût. Les données contenues dans S3 Glacier Deep Archive ne sont pas récupérées souvent ou sont rarement extraites. Pour plus d'informations, consultez Classes de stockage pour l'archivage des objets.

> **Note**
>
> Toutes les bandes créées avant le 27 mars 2019 sont archivées directement dans S3 Glacier Flexible Retrieval lorsque le logiciel de sauvegarde les éjecte.

Lorsque le logiciel de sauvegarde éjecte une bande, elle est automatiquement archivée dans le pool que vous avez choisi lorsque vous avez créé la bande. Le processus d'éjection d'une bande varie en fonction de votre logiciel de sauvegarde. Avec certains logiciels de sauvegarde, vous devez exporter des bandes après leur éjection, avant que l'archivage puisse commencer. Pour obtenir des informations sur les logiciels de sauvegarde pris en charge, consultez Utilisation d'un logiciel de sauvegarde pour tester la configuration de votre passerelle.

Déplacement de bandes vers la classe de stockage S3 Glacier Deep Archive

Déplacez vos bandes depuis S3 Glacier Flexible Retrieval vers S3 Glacier Deep Archive pour une conservation des données à long terme et une préservation numérique à très faible coût. Vous

utilisez S3 Glacier Deep Archive pour la conservation des données à long terme et l'archivage numérique, où les données sont consultées une à deux fois par an. Pour plus d'informations, consultez Classes de stockage pour l'archivage des objets.

Pour déplacer une bande de S3 Glacier Flexible Retrieval vers S3 Glacier Deep Archive

1. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.
2. Cochez les cases correspondant aux bandes que vous souhaitez déplacer dans S3 Glacier Deep Archive. Vous pouvez voir le groupe auquel cette bande est associée dans la colonne Groupe.
3. Choisissez Affecter à un groupe.
4. Dans la boîte de dialogue Affecter une bande à un groupe, vérifiez les codes barres des bandes que vous déplacez et sélectionnez Affecter.

   > **Note**
   >
   > Si une bande a été éjectée par l'application de sauvegarde et archivée dans S3 Glacier Deep Archive vous ne pouvez pas la redéplacer vers S3 Glacier Flexible Retrieval. Pour le déplacement de vos bandes de S3 Glacier Flexible Retrieval vers S3 Glacier Deep Archive, des frais s'appliquent. De plus, si vous déplacez des bandes de S3 Glacier Flexible Retrieval vers S3 Glacier Deep Archive avant 90 jours, des frais de suppression anticipée vous sont facturés pour S3 Glacier Flexible Retrieval.

5. Une fois la bande déplacée, vous pouvez voir son statut actualisé dans la colonne Groupe de la page de Présentation de la bande.

Récupération des bandes archivées

Pour accéder aux données stockées sur une bande virtuelle archivée, vous devez tout d'abord extraire la bande qui vous intéresse sur la passerelle de bande. Votre passerelle de bande fournit une bibliothèque de bandes virtuelles (VTL) pour chaque passerelle.

Si vous avez plusieurs passerelles de bande dans un Région AWS, vous ne pouvez récupérer une bande que sur une seule passerelle.

La bande récupérée est protégée en écriture, vous pouvez uniquement lire les données sur la bande.

> **Important**
>
> Si vous archivez une bande dans S3 Glacier Flexible Retrieval, vous pouvez la récupérer généralement en 3 à 5 heures. Si vous archivez la bande dans S3 Glacier Deep Archive, vous pouvez la récupérer généralement dans un délai de 12 heures.

> **Note**
>
> L'extraction des bandes de l'archive entraîne des frais. Pour plus d'information sur les tarifs, consultez Tarification Storage Gateway.

Pour récupérer une bande archivée et la transférer sur votre passerelle

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.
3. Choisissez la bande virtuelle que vous souhaitez récupérer dans l'onglet Étagère de bandes virtuelles, puis choisissez Extraire la bande.

   > **Note**
   >
   > Le statut de la bande virtuelle que vous souhaitez extraire doit être ARCHIVÉ.

4. Dans la boîte de dialogue Extraire la bande, pour Code à barres, vérifiez que le code à barres identifie la bande virtuelle que vous souhaitez récupérer.

5. Pour Passerelle, choisissez la passerelle vers laquelle vous souhaitez extraire la bande archivée, puis choisissez Extraire la bande.

Le statut de la bande passe de ARCHIVÉ à RÉCUPÉRATION. À ce stade, vos données sont transférées de l'étagère de bandes virtuelles (soutenue par S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive) vers la bibliothèque de bandes virtuelles (soutenue par Amazon S3). Une fois que toutes les données ont été transférées, le statut de la bande virtuelle dans l'archive passe à RÉCUPÉRÉ.

> **Note**
>
> Les bandes virtuelles récupérées sont en lecture seule.

Affichage des statistiques d'utilisation des cassettes

Lorsque vous écrivez des données sur une bande, vous pouvez consulter la quantité de données stockées sur la bande dans la console de gestion Storage Gateway. L'onglet Détails de chaque bande affiche les informations d'utilisation des bandes.

Pour afficher la quantité de données stockées sur une bande

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.
3. Choisissez la bande qui vous intéresse.
4. La page qui apparaît fournit divers détails et informations sur la bande, notamment les suivants :
   - Taille : capacité totale de la bande sélectionnée.
   - Utilisé : taille des données écrites sur la bande par votre application de sauvegarde.

> **Note**
>
> Cette valeur n'est pas disponible pour les bandes créées avant le 13 mai 2015.

Suppression de bandes virtuelles de votre Tape Gateway

Vous pouvez supprimer des bandes virtuelles de votre passerelle de bande à l'aide de la console Storage Gateway.

> **Note**
>
> Si le statut de la bande que vous souhaitez supprimer de votre passerelle de bande est EXTRAIT, vous devez tout d'abord éjecter la bande à l'aide de votre application de sauvegarde avant de la supprimer. Pour obtenir des instructions sur l'éjection d'une bande à l'aide du NetBackup logiciel Symantec, reportez-vous à la section Archivage de la bande. Une fois que la bande a été éjectée, son état redevient ARCHIVED. Vous pouvez ensuite supprimer la bande.

Faites des copies de vos données avant de supprimer vos bandes. Lorsque vous avez supprimé une bande, vous ne pouvez pas la récupérer.

Pour supprimer une bande virtuelle

> **Warning**
>
> Cette procédure supprime définitivement la bande virtuelle sélectionnée.

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000

bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.

3. Sélectionnez une ou plusieurs bandes à supprimer.
4. Pour Actions, choisissez Supprimer la bande. La boîte de dialogue de confirmation s'affiche.
5. Vérifiez que vous souhaitez bien supprimer les bandes spécifiées, puis tapez le mot supprimer dans le champ de confirmation et choisissez Supprimer.

Une fois que la bande a été supprimée, elle disparaît de la passerelle de bande.

Suppression de groupes de bandes personnalisés

La procédure suivante explique comment supprimer un pool de bandes personnalisé à l'aide de la console Storage Gateway. Pour effectuer cette action par programmation à l'aide de l'API, reportez-vous DeleteTapePoolà la section Storage Gateway API Reference.

Vous ne pouvez supprimer un groupe de bandes personnalisé que s'il n'y a aucune bande archivée dans le groupe et qu'aucune politique de création automatique de bandes n'est attachée au groupe. Si vous devez supprimer les politiques de création automatique de bandes d'un pool de bandes, reportez-vous à la section Gestion de la création automatique de bandes.

Pour supprimer un pool de bandes personnalisé 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 Groupes pour afficher les groupes disponibles.
3. Sélectionnez un ou plusieurs groupes de bandes à supprimer.

   Si le Nombre de bandes pour les groupes de bandes que vous souhaitez supprimer est égal à 0, et si aucune politique de création automatique de bandes n'est associée au groupe de bandes personnalisé, vous pouvez supprimer les groupes.
4. Sélectionnez Delete (Supprimer). La boîte de dialogue de confirmation s'affiche.
5. Vérifiez que vous souhaitez bien supprimer les groupes de bandes spécifiés, puis tapez le mot supprimer dans le champ de confirmation et choisissez Supprimer.

> **Warning**
>
> Cette procédure supprime définitivement les groupes de bandes sélectionnés et ne peut être annulée.

Une fois les groupes de bandes supprimés, ils disparaissent de la librairie de bandes.

Désactivation de votre passerelle de bande

Vous désactivez une passerelle de bande; si celle-ci est défaillante et que vous souhaitez récupérer les bandes de la passerelle défaillante pour les transférer sur une autre passerelle.

Pour récupérer les bandes, vous devez d'abord désactiver la passerelle défaillante. La désactivation d'une passerelle de bande verrouille les bandes virtuelles dans cette passerelle. En d'autres termes, toutes les données que vous pouvez écrire sur ces bandes après avoir désactivé la passerelle ne sont pas envoyées à AWS. Vous pouvez uniquement désactiver une passerelle sur la console Storage Gateway si la passerelle n'est plus connectée à AWS. Si la passerelle est connectée à AWS, vous ne pouvez pas désactiver la Tape Gateway.

Vous désactivez une passerelle de bande dans le cadre de la récupération des données. Pour plus d'informations sur la récupération des bandes, consultez Vous avez besoin de récupérer une bande virtuelle à partir d'une passerelle de bande défaillante.

Pour désactiver la passerelle

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle qui a échoué.
3. Choisissez l'onglet Détails pour que la passerelle affiche le message de désactivation de la passerelle.
4. Choisissez Créer des bandes de récupération.
5. Choisissez Désactiver la passerelle.

Comprendre l'état de la bande

Chaque bande est associée à un état qui vous indique rapidement l'intégrité de la bande. La plupart du temps, l'état indique que la bande fonctionne normalement et qu'aucune action de votre part n'est nécessaire. Dans certains cas, l'état indique un problème avec la bande qui peut exiger une action de votre part. Vous trouverez ci-après des informations pour vous aider à déterminer si vous avez besoin d'intervenir.

Rubriques

- Comprendre les informations sur l'état d'une bande dans une VTL
- Détermination de l'état d'une bande dans une archive

Comprendre les informations sur l'état d'une bande dans une VTL

Le statut de la bande doit être DISPONIBLE pour que vous puissiez lire la bande ou écrire dessus. Le tableau suivant répertorie et décrit les valeurs d'état possibles.

État	Description	Les données de la bande sont stockées dans
CREAtioN	Les bandes virtuelles sont en cours de création. La bande ne peut pas être chargée dans un lecteur de bande car elle est en cours de création.	—
DISPONIBLE	La bande virtuelle a été créée et elle est prête à être chargée dans un lecteur de bandes.	Amazon S3
EN TRANSIT VERS VTS	La bande virtuelle a été éjectée et elle est en cours de chargement pour l'archivage. À ce stade, votre Tape Gateway télécharge des données vers AWS. Si la quantité de données en cours de chargement est faible, l'état n'est pas toujours visible. Une fois le chargement terminé, l'état passe à ARCHIVAGE.	Amazon S3
ARCHIVAGE	La bande virtuelle est transférée par votre passerelle de bande vers l'archive qui est soutenue par S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.	Les données sont en cours de transfert depuis Amazon S3 vers S3

État	Description	Les données de la bande sont stockées dans
	Ce processus se produit une fois le téléchargement des données AWS terminé.	Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
SUPPRESSION	La bande virtuelle est supprimée.	Les données sont en cours de suppression de Amazon S3
SUPPRIMÉ	La bande virtuelle a été supprimée.	—
RECUPERATION	La bande virtuelle est en cours de récupération de l'archive et transférée vers la passerelle de bande. **Note** La bande virtuelle peut être extraite et transférée uniquement vers une passerelle de bande.	Les données sont en cours de déplacement depuis Amazon S3 vers S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive
EXTRAITE	La bande virtuelle est en cours d'extraction de l'archive. La bande extraite est protégée en écriture.	Amazon S3
RECUPEREE	La bande virtuelle est récupérée et elle est en lecture seule. Lorsque votre passerelle de bande n'est pas accessible pour une raison quelconque, vous pouvez récupérer les bandes virtuelles associées à cette passerelle de bande vers une autre passerelle de bande. Pour récupérer les bandes virtuelles, vous devez d'abord désactiver la passerelle de bande inaccessible.	Amazon S3
IRRECUPERABLE	Il est impossible de lire la bande virtuelle ou d'écrire dessus. Ce statut indique une erreur dans votre passerelle de bande.	Amazon S3

Détermination de l'état d'une bande dans une archive

Vous pouvez utiliser la procédure suivante pour déterminer l'état d'une bande virtuelle dans une archive.

Pour déterminer l'état d'une bande virtuelle

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, sélectionnez Bandes.
3. Dans la colonne État de la grille de bibliothèque de bandes, vérifiez l'état de la bande.

   Le statut de la bande s'affiche également dans l'onglet Détails de chaque bande virtuelle.

Vous trouverez ci-dessous une description des valeurs d'état possibles.

État	Description
ARCHIVÉ	La bande virtuelle a été éjectée et elle est chargée dans l'archive.
RECUPERATION	La bande virtuelle est en cours d'extraction de l'archive. **Note** La bande virtuelle peut être extraite et transférée uniquement vers une passerelle de bande.
EXTRAITE	La bande virtuelle a été extraite de l'archive. La bande récupérée est en lecture seule.

Pour plus d'informations sur le fonctionnement des bandes et des appareils VTL, consultez Gestion des bandes dans votre bibliothèque de bandes virtuelle.

Déplacement de vos données vers une nouvelle passerelle

Vous pouvez déplacer des données entre les passerelles au fur et à mesure que vos besoins en données et en performances augmentent, ou si vous recevez une AWS notification vous demandant de migrer votre passerelle. Ce qui suit présente certaines raisons d'effectuer cette tâche :

- Déplacez vos données vers de meilleures plateformes d'hébergement ou de nouvelles EC2 instances Amazon.
- Renouveler le matériel sous-jacent de votre serveur.

Les étapes à suivre pour déplacer vos données vers une nouvelle passerelle dépendent du type de passerelle dont vous disposez.

> **Note**
>
> Les données ne peuvent être déplacées qu'entre les mêmes types de passerelles.

Déplacement de bandes virtuelles dans une nouvelle passerelle de bande

Pour déplacer la bande virtuelle dans une nouvelle passerelle de bande

1. Utilisez votre application de sauvegarde pour sauvegarder toutes vos données sur une bande virtuelle. Attendez que la sauvegarde se termine correctement.
2. Utilisez votre application de sauvegarde pour éjecter votre bande. La bande sera stockée dans l'une des classes de stockage Amazon S3. Les bandes éjectées sont archivées dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive et sont en lecture seule.

   Avant de poursuivre, vérifiez que les bandes éjectées ont été archivées :

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

   b. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour

réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.

c. Dans la colonne État de la liste, vérifiez le statut de la bande.

Le statut de la bande s'affiche également dans l'onglet Détails de chaque bande virtuelle.

Pour plus d'informations sur la façon de déterminer le statut de la bande dans une archive, consultez Détermination de l'état d'une bande dans une archive.

3. À l'aide de votre application de sauvegarde, vérifiez qu'aucune tâche de sauvegarde active n'est envoyée à une passerelle de bande existante avant de l'arrêter. Si des tâches de sauvegarde sont actives, attendez qu'elles soient terminées et éjectez vos bandes (voir étape précédente) avant d'arrêter la passerelle.
4. Effectuez les étapes suivantes pour arrêter la passerelle de bande existante :

a. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez l'ancienne passerelle de bande que vous souhaitez arrêter. L'état de la passerelle est En cours d'exécution.

b. Pour Actions, choisissez Arrêter la passerelle. Vérifiez l'ID de la passerelle dans la boîte de dialogue, puis choisissez Arrêter la passerelle.

Pendant l'arrêt de l'ancienne passerelle de bande, un message indiquant le statut de la passerelle est susceptible de s'afficher. Lorsque la passerelle s'arrête, un message et un bouton Démarrer la passerelle s'affichent dans l'onglet Détails.

Pour en savoir plus sur l'arrêt d'une passerelle, consultez Démarrage et arrêt d'une passerelle de bande.

5. Créez une nouvelle passerelle de bande. Pour obtenir des instructions détaillées, consultez Création d'une passerelle.
6. Procédez comme suit pour créer de nouvelle bandes :

a. Dans le volet de navigation, choisissez l'onglet Passerelles.

b. Choisissez Créer une bande pour ouvrir la boîte de dialogue Créer une bande.

c. Pour Passerelle, choisissez une passerelle. La bande est créée pour cette passerelle.

d. Pour Number of tapes (Nombre de bandes), choisissez le nombre de bandes que vous souhaitez créer. Pour plus d'informations sur les limites des bandes, consultez AWS Storage Gateway quotas.

À ce stade, vous pouvez également configurer la création automatique de bandes. Pour plus d'informations, consultez Création automatique de bandes.

e. Pour Capacity (Capacité), entrez la taille de la bande virtuelle que vous souhaitez créer. La taille des bandes doit être supérieure à 100 Gio. Pour en savoir plus sur les limites de capacité, consultez AWS Storage Gateway quotas.

f. Pour Barcode prefix (Préfixe de code-barres), entrez le préfixe que vous souhaitez ajouter au code à barres de vos bandes virtuelles.

> **Note**
>
> Les bandes virtuelles sont identifiées de façon unique par un code à barres. Vous pouvez ajouter un préfixe au code-barres. Le préfix est facultatif, mais vous pouvez l'utiliser pour faciliter l'identification de vos bandes virtuelles. Le préfixe doit être en majuscules (A-Z) et comporter entre un et quatre caractères.

g. Pour Pool, choisissez Glacier Pool ou Deep Archive Pool. Ce pool représente la classe de stockage dans laquelle votre bande sera stockée lorsqu'elle sera éjectée par votre logiciel de sauvegarde.

   Choisissez Groupe Glacier si vous souhaitez archiver la bande dans S3 Glacier Flexible Retrieval. Lorsque le logiciel de sauvegarde éjecte la bande, elle est automatiquement archivée dans S3 Glacier Flexible Retrieval. Vous utilisez S3 Glacier Flexible Retrieval pour des archives plus actives, au sein desquelles vous pouvez récupérer une bande dans un délai compris entre 3 et 5 heures. Pour plus d'informations, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.

   Choisissez Groupe Deep Archive si vous souhaitez archiver la bande dans S3 Glacier Deep Archive. Lorsque le logiciel de sauvegarde éjecte la bande, celle-ci est automatiquement archivée dans S3 Glacier Deep Archive. Vous utilisez S3 Glacier Deep Archive pour la conservation des données à long terme et l'archivage numérique, où les données sont consultées une à deux fois par an. Vous pouvez extraire une bande archivée dans S3 Glacier Deep Archive généralement dans un délai de 12 heures. Pour plus d'informations, consultez Classes de stockage pour l'archivage d'objets dans le Guide de l'utilisateur Amazon Simple Storage Service.

Si vous archivez une bande dans S3 Glacier Flexible Retrieval, vous pouvez la déplacer vers S3 Glacier Deep Archive ultérieurement. Pour plus d'informations, consultez Déplacement de bandes vers la classe de stockage S3 Glacier Deep Archive.

> **Note**
>
> Les bandes créées avant le 27 mars 2019 sont archivées directement dans S3 Glacier Flexible Retrieval lorsque le logiciel de sauvegarde les éjecte.

h. (Facultatif) Pour Balises, entrez une clé et une valeur pour ajouter une balise à votre bande. Une balise est une paire clé-valeur sensible à la casse qui vous aide à gérer, filtrer et rechercher vos bandes.

i. Choisissez Créer des bandes.

7. Utilisez votre application de sauvegarde pour démarrer une tâche de sauvegarde et sauvegardez vos données sur la nouvelle bande.

8. (Facultatif) Si votre bande est archivée et que vous devez restaurer des données à partir de celle-ci, récupérez-la sur la nouvelle passerelle de bande. La bande sera en mode lecture seule. Pour en savoir plus sur la récupération de bandes archivées, consultez Récupération des bandes archivées.

> **Note**
>
> Des frais de données sortantes peuvent s'appliquer.

a. Dans le volet de navigation, sélectionnez Bibliothèque de bandes > Bandes pour afficher vos bandes. Par défaut, cette liste affiche jusqu'à 1 000 bandes à la fois, mais les recherches que vous effectuez s'appliquent à toutes vos bandes. Vous pouvez utiliser la barre de recherche pour trouver des bandes répondant à des critères spécifiques ou pour réduire la liste à moins de 1 000 bandes. Lorsque votre liste contient 1 000 bandes ou moins, vous pouvez les trier par ordre croissant ou décroissant selon différentes propriétés.

b. Choisissez la bande virtuelle que vous voulez récupérer. Pour Actions, choisissez Récupérer la bande.

> **Note**
>
> Le statut de la bande virtuelle que vous souhaitez récupérer doit être `ARCHIVED`.

c. Dans la boîte de dialogue Extraire la bande, pour Code à barres, vérifiez que le code à barres identifie la bande virtuelle que vous souhaitez récupérer.

d. Dans Passerelle, choisissez la nouvelle passerelle de bande vers laquelle vous souhaitez extraire la bande archivée, puis choisissez Récupérer la bande.

Lorsque vous avez confirmé que votre nouvelle passerelle de bande fonctionne correctement, vous pouvez supprimer l'ancienne passerelle de bande.

> **Important**
>
> Avant de supprimer une passerelle, veillez à ce qu'aucune application ne soit en train d'écrire sur les volumes de la passerelle. Si vous supprimez une passerelle alors qu'elle est en cours d'utilisation, une perte de données peut se produire.

9. Effectuez les étapes suivantes pour supprimer l'ancienne passerelle de bande :

> **Warning**
>
> Lorsqu'une passerelle est supprimée, il n'y a plus aucun moyen de la récupérer.

a. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle que vous souhaitez supprimer.

b. Pour Actions, choisissez Delete stack (Supprimer la pile).

Dans la boîte de dialogue de confirmation qui s'affiche, assurez-vous que l'ID de passerelle indiqué indique l'ancienne passerelle de bande que vous souhaitez supprimer, entrez **`delete`** dans le champ de confirmation, puis choisissez Supprimer.

c. Supprimez la machine virtuelle. Pour plus d'informations sur la façon de supprimer une machine virtuelle, consultez la documentation de votre hyperviseur.

Surveillance de Storage Gateway

Cette section décrit comment surveiller une Storage Gateway, y compris la surveillance des ressources associées à la passerelle, à l'aide d'Amazon CloudWatch. Vous pouvez surveiller la mémoire tampon de chargement et le stockage en cache de la passerelle. Vous utilisez la console Storage Gateway pour afficher les métriques et les alarmes de votre passerelle. Par exemple, vous pouvez afficher le nombre d'octets utilisés pour les opérations de lecture et d'écriture, le temps consacré à celles-ci et le temps nécessaire pour récupérer les données à partir du cloud Amazon Web Services. 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. Elles vous permettent d'accéder aux informations d'historique et d'obtenir un meilleur point de vue sur les performances de votre passerelle et des volumes. 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.

Pour obtenir des informations spécifiques à la surveillance d'une passerelle de bande et de ses ressources associées, consultez la section Surveillance de votre passerelle de bande.

Rubriques

- Présentation des métriques de la passerelle
- Surveillance du tampon de chargement
- Surveillance du stockage de cache
- Comprendre les CloudWatch alarmes
- Création d' CloudWatch alarmes recommandées pour votre passerelle
- Création d'une CloudWatch alarme personnalisée pour votre passerelle
- Surveillance de votre passerelle de bande

Présentation des métriques de la passerelle

Dans le cadre de cette rubrique, nous définissons les métriques de passerelle comme des métriques limitées à la passerelle, c'est-à-dire qu'elles mesurent quelque chose à propos de la passerelle. Dans

la mesure où une passerelle contient un ou plusieurs volumes, une métrique propre à la passerelle représente tous les volumes de la passerelle. Par exemple, la métrique `CloudBytesUploaded` correspond au nombre total d'octets que la passerelle a envoyés au cloud au cours de la période de génération du rapport. Cette métrique inclut l'activité de tous les volumes de la passerelle.

Lorsque vous travaillez avec les données des métriques de la passerelle, vous spécifiez l'identification unique de la passerelle dont vous souhaitez consulter les métriques. Dans cette optique, vous spécifiez les valeurs `GatewayId` et `GatewayName`. Si vous souhaitez utiliser une métrique de passerelle, vous spécifiez la dimension de la passerelle dans l'espace de noms des métriques, ce qui permet de faire la distinction entre une métrique de passerelle et une métrique de volume. Pour plus d'informations, consultez Utilisation d'Amazon CloudWatch Metrics.

> **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.

Métrique	Description	
`AvailabilityNotifications`	Nombre de notifications d'intégrité liées à la disponibilité et générées par la passerelle. Utilisez cette métrique avec la statistique `Sum` pour observer si la passerelle rencontre des événements liés à la disponibilité. Pour plus de détails sur les événements, consultez le groupe de CloudWatch journaux que vous avez configuré. Unité : nombre	

Métrique	Description
`CacheHitPercent`	Pourcentage des accès en lecture à l'application fourni par la mémoire cache. L'exemple est pris à la fin de la période de génération de rapport. Unité : 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. Utilisez cette métrique avec la `Sum` statistique. Idéalement, cette métrique devrait rester faible. Unité : pourcentage
`CacheUsed`	Nombre total d'octets utilisés pour le stockage du cache de la passerelle. L'exemple est pris à la fin de la période de génération de rapport. Unité : octets
`IoWaitPercent`	Pourcentage de temps pendant lequel la passerelle attend une réponse du disque local. Unité : pourcentage

Métrique	Description	
`MemTotalBytes`	Quantité de RAM allouée à la machine virtuelle de la passerelle, en octets. Unité : octets	
`MemUsedBytes`	Quantité de RAM actuellement en cours d'utilisation par la machine virtuelle de la passerelle, en octets. Unité : octets	
`QueuedWrites`	Normalement, cette valeur représente le nombre d'octets stockés localement en attente d'écriture AWS, mais elle reflète également le processus de synchronisation qui se produit entre les données locales et les données du cloud lors du « bootstrap », qui a lieu chaque fois qu'une passerelle redémarre. Unité : octets	
`TotalCacheSize`	Taille totale du cache en octets. L'exemple est pris à la fin de la période de génération de rapport. Unité : octets	

Métrique	Description
`UploadBufferPercentUsed`	Utilisation en pourcentage de la mémoire tampon de chargement de la passerelle. L'exemple est pris à la fin de la période de génération de rapport. Unité : pourcentage
`UploadBufferUsed`	Nombre total d'octets utilisés dans la mémoire tampon de chargement de la passerelle. L'exemple est pris à la fin de la période de génération de rapport. Unité : octets
`UserCpuPercent`	Pourcentage de temps CPU consacré au traitement de la passerelle, en moyenne pour tous les cœurs. Unité : pourcentage

Dimensions des métriques de Storage Gateway

L'espace de CloudWatch noms du service Storage Gateway est`AWS/StorageGateway`. Les données sont disponibles automatiquement toutes les 5 minutes sans coût aucun.

Dimension	Description
`GatewayId` , `GatewayName`	Ces dimensions filtrent les données demandées sur la base des métriques spécifiques à la passerelle. Vous pouvez identifier une passerelle à utiliser en fonction de la valeur de `GatewayId` ou de `GatewayName` . Si le nom de votre passerelle a été

Dimension	Description
	modifié pendant l'intervalle de temps dont vous souhaitez examiner les métriques, utilisez le `GatewayId` . Le débit et la latence des données d'une passerelle sont basés sur tous les volumes de la passerelle. Pour obtenir des informations sur l'utilisation des métriques de passerelle, consultez Mesure des performances entre votre passerelle et AWS.

Surveillance du tampon de chargement

Vous trouverez ci-après des informations sur la surveillance du tampon de chargement d'une passerelle et sur la création d'une alarme afin que vous receviez une notification lorsque le tampon dépasse un seuil défini. Grâce à cette approche, vous pouvez ajouter un stockage de tampon à une passerelle avant qu'elle ne se remplisse complètement et que votre application de stockage ne cesse les sauvegardes dans AWS.

Vous surveillez le tampon de chargement de la même manière dans les architectures de passerelles de bande et de volume en cache. Pour plus d'informations, consultez Fonctionnement d'une passerelle de bande.

> **Note**
>
> Les métriques `WorkingStoragePercentUsed`, `WorkingStorageUsed` et `WorkingStorageFree` représentent le tampon de chargement pour les volumes stockés uniquement avant le lancement de la fonctionnalité des volumes mis en cache dans Storage Gateway. Utilisez maintenant les métriques équivalentes du tampon de chargement `UploadBufferPercentUsed`, `UploadBufferUsed` et `UploadBufferFree`. Ces métriques s'appliquent aux deux architectures de la passerelle.

Elément intéressant	Comment le mesurer
Utilisation du tampon de chargement	Utilisez les métriques `UploadBufferPercentUsed` , `UploadBufferUsed` et `UploadBufferFree` avec la statistique `Average`. Par

Elément intéressant	Comment le mesurer
	exemple, utilisez `UploadBufferUsed` avec la statistique `Average` pour analyser l'utilisation du stockage sur une période de temps.

Pour mesurer le pourcentage du tampon de chargement utilisé

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez la dimension StorageGateway: Gateway Metrics et recherchez la passerelle avec laquelle vous souhaitez travailler.
3. Choisissez la métrique `UploadBufferPercentUsed`.
4. Pour Plage de temps, choisissez une valeur.
5. Choisissez la statistique `Average`.
6. Pour Période, choisissez une valeur de 5 minutes afin qu'elle corresponde au temps par défaut du rapport.

L'ensemble de points de données obtenu pendant la période contient le pourcentage utilisé du tampon de chargement.

La procédure suivante vous permet de créer une alarme à l'aide de la CloudWatch console. Pour en savoir plus sur les alarmes et les seuils, consultez la section Création d' CloudWatch alarmes dans le guide de CloudWatch l'utilisateur Amazon.

Pour définir une alarme de seuil supérieur pour le tampon de chargement de la passerelle

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Create Alarm (Créer une alarme) pour lancer l'assistant de création d'alarmes.
3. Spécifiez une métrique pour votre alarme :
    a. Sur la page Sélectionner une métrique de l'assistant de création d'alarme GatewayId, choisissez la GatewayName dimension AWS/StorageGateway:, puis recherchez la passerelle avec laquelle vous souhaitez travailler.
    b. Choisissez la métrique `UploadBufferPercentUsed`. Utilisez la statistique `Average` et une période de 5 minutes.
    c. Choisissez Continuer.
4. Définissez le nom, la description et le seuil de l'alarme :

a. Sur la page Define Alarm (Définir une alarme) de l'assistant de création d'alarmes, identifiez votre alarme en lui donnant un nom et une descriptions dans les zones Name (Nom) et Description.

b. Définissez le seuil de l'alarme.

c. Choisissez Continuer.

5. Configurez une action d'e-mail pour l'alarme :

a. Sur la page Configure Actions (Configurer des actions) de l'assistant de création d'alarmes, choisissez Alarm (Alarme) pour Alarm State (État de l'alarme).

b. Pour Rubrique, sélectionnez Choisir ou créer une rubrique d'e-mail.

La création d'une rubrique d'e-mail signifie que vous configurez une rubrique Amazon SNS. Pour plus d'informations sur Amazon SNS, consultez Configurer Amazon SNS dans le guide de l'utilisateur Amazon CloudWatch .

c. Dans Rubrique, entrez un nom descriptif pour la rubrique.

d. Sélectionnez Ajouter une action.

e. Choisissez Continuer.

6. Passez en revue les paramètres de l'alarme, puis créez cette dernière :

a. Sur la page Review (Révision) de l'assistant de création d'alarmes, vérifiez la définition de l'alarme, la métrique et les actions associées à effectuer (par exemple, l'envoi d'une notification par e-mail).

b. Après avoir examiné le récapitulatif de l'alarme, choisissez Enregistrer l'alarme.

7. Validez votre abonnement à la rubrique d'alarme :

a. Ouvrez l'e-mail Amazon SNS envoyé à l'adresse e-mail que vous avez spécifiée lors de la création de la rubrique.

b. Validez votre abonnement en cliquant sur le lien de l'e-mail.

Une confirmation d'abonnement s'affiche.

Surveillance du stockage de cache

Vous trouverez ci-après des informations sur la surveillance du stockage de cache d'une passerelle et sur la création d'une alarme afin que vous receviez une notification lorsque les paramètres du cache dépassent les seuils spécifiés. A l'aide de cette alarme, vous savez quand ajouter du stockage de cache à une passerelle.

Vous surveillez uniquement le stockage de cache dans l'architecture de volumes mis en cache. Pour plus d'informations, consultez Fonctionnement d'une passerelle de bande.

Elément intéressant	Comment le mesurer
Utilisation totale du cache	Utilisez les métriques `CachePercentUsed` et `TotalCacheSize` avec la statistique `Average`. Par exemple, utilisez `CachePercentUsed` avec la statistique `Average` pour analyser l'utilisation du cache sur une période de temps. La métrique `TotalCacheSize` change uniquement lorsque vous ajoutez le cache à la passerelle.
Pourcentage de demandes de lectures servies depuis le cache	Utilisez la métrique `CacheHitPercent` avec la statistique `Average`. En règle générale, il est préférable que la métrique `CacheHitPercent` reste élevée.
Pourcentage du cache qui est sale, c'est-à-dire qu'il contient du contenu qui n'a pas été chargé vers AWS	Utilisez la métrique `CachePercentDirty` avec la statistique `Average`. En règle générale, il est préférable que la métrique `CachePercentDirty` soit faible.

Pour mesurer le pourcentage d'un cache corrompu pour une passerelle et tous ses volumes

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez la dimension StorageGateway: Gateway Metrics et recherchez la passerelle avec laquelle vous souhaitez travailler.

3. Choisissez la métrique `CachePercentDirty`.
4. Pour Plage de temps, choisissez une valeur.
5. Choisissez la statistique `Average`.
6. Pour Période, choisissez une valeur de 5 minutes afin qu'elle corresponde au temps par défaut du rapport.

Le jeu de points de données obtenu pendant la période contient le pourcentage de cache qui est corrompu pendant les 5 minutes.

Pour mesurer le pourcentage du cache corrompu pour un volume

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez la dimension StorageGateway: Volume Metrics et recherchez le volume avec lequel vous souhaitez travailler.
3. Choisissez la métrique `CachePercentDirty`.
4. Pour Plage de temps, choisissez une valeur.
5. Choisissez la statistique `Average`.
6. Pour Période, choisissez une valeur de 5 minutes afin qu'elle corresponde au temps par défaut du rapport.

Le jeu de points de données obtenu pendant la période contient le pourcentage de cache qui est corrompu pendant les 5 minutes.

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 une passerelle de bande, consultez Comprendre les métriques de passerelle et Comprendre les métriques de bande virtuelle. Pour chaque alarme, vous spécifiez les conditions qui déclencheront son état 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
- Notifications d'intégrité : `HealthNotifications` >= 1 pour 1 point de données en 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 sur les plateformes VMware hôtes avec le mode HA activé, nous recommandons également cette CloudWatch alarme supplémentaire :

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

Le tableau suivant décrit l'état d'une alarme.

État	Description
OK	La métrique ou l'expression se trouve dans le seuil défini.

État	Description
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 Création d'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 Configuration de votre passerelle de bande. Si vous souhaitez ajouter ou mettre à jour les CloudWatch alarmes recommandées pour une passerelle existante, suivez la procédure ci-dessous.

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, choisissez Gateways, puis choisissez la passerelle pour laquelle vous souhaitez créer des CloudWatch alarmes recommandées.
3. Sur la page de 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.

Création d'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 ALARME quand 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 bande

Les rubriques de cette section décrivent les procédures et les informations conceptuelles relatives à la surveillance de votre Tape Gateway. Vous pouvez surveiller les bandes virtuelles, le stockage en cache et la mémoire tampon de téléchargement associés à votre Tape Gateway. Vous pouvez utiliser le AWS Management Console pour afficher les métriques de votre Tape Gateway. Avec les métriques, vous pouvez suivre l'intégrité de la passerelle de bande et configurer des alarmes pour vous avertir lorsqu'une ou plusieurs métriques dépassent un seuil défini.

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir des informations sur l'état de votre Tape Gateway 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.

Storage Gateway fournit CloudWatch des métriques sans frais supplémentaires. Les métriques de Storage Gateway sont enregistrées pendant une période de deux semaines. À l'aide de ces métriques, vous pouvez accéder aux informations d'historique et d'obtenir un meilleur point de vue sur les performances de votre passerelle de bande et des bandes virtuelles. Pour obtenir des informations détaillées à ce sujet CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Le débit des données, la latence des données et les opérations par seconde sont des mesures que vous pouvez utiliser pour comprendre les performances de vos applications de stockage avec Tape Gateway. Lorsque vous utilisez la statistique d'agrégation correcte, ces valeurs peuvent être mesurées en utilisant les métriques Storage Gateway qui disponibles.

Rubriques

- Obtenir les journaux de santé de Tape Gateway à l'aide de groupes de CloudWatch journaux
- Utilisation d'Amazon CloudWatch Metrics
- Comprendre les métriques des bandes virtuelles
- Mesurer les performances entre votre Tape Gateway et AWS

Obtenir les journaux de santé de Tape Gateway à l'aide de groupes de CloudWatch journaux

Vous pouvez utiliser Amazon CloudWatch Logs pour obtenir des informations sur l'état de votre Tape Gateway 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.

Supposons, par exemple, que votre passerelle soit déployée dans un cluster activé avec VMware HA et que vous ayez besoin de connaître les éventuelles erreurs. Vous pouvez configurer un groupe de CloudWatch journaux pour surveiller votre passerelle et être averti lorsque celle-ci rencontre une erreur. Vous pouvez configurer le groupe lorsque vous activez la passerelle ou une fois que la passerelle est activée et opérationnelle. Pour plus d'informations sur la configuration d'un groupe de CloudWatch journaux lors de l'activation d'une passerelle, consultez la section Configurer votre passerelle sur bande. 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 obtenir des informations sur la façon de résoudre et corriger ces types d'erreurs, consultez Dépannage des problèmes de bandes virtuelles.

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 fichiers

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 passerelle ou dans l'onglet Détails, sous Health logs et Not Enabled, choisissez Configurer le groupe de journaux pour ouvrir la boîte de CustomerGatewayNamedialogue Modifier.
4. Pour le Groupe de journaux sur l'intégrité de la passerelle, choisissez l'une des options suivantes :

   - Désactivez la journalisation si vous ne souhaitez pas surveiller votre passerelle à l'aide de groupes de CloudWatch journaux.
   - 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.
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 CloudWatch Logs. La page des détails du groupe de journaux s'ouvre dans la CloudWatch console.

Voici un exemple de message d'événement Tape Gateway envoyé à CloudWatch. Cet exemple montre un message `TapeStatusTransition`.

```
{
"severity": "INFO",
"source": "FZTT16FCF5",
"type": "TapeStatusTransition",
"gateway": "sgw-C51DFEAC",
"timestamp": "1581553463831",
"newStatus": "RETRIEVED"
}
```

Utilisation d'Amazon CloudWatch Metrics

Vous pouvez obtenir des données de surveillance pour votre Tape Gateway à l'aide de l'API AWS Management Console ou de l' CloudWatch API. La console affiche un ensemble de graphiques basés sur les données brutes obtenues avec l'API CloudWatch . L' CloudWatch API peut également être utilisée via l'un des kits de développement AWS logiciel Amazon (SDKs) ou les outils d' 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 choisissez pour travailler avec les métriques, vous devez spécifier les informations suivantes :

- La dimension de métrique à utiliser. Une dimension est une paire nom-valeur qui vous aide à identifier une métrique de façon unique. Les dimensions de Storage Gateway sont `GatewayId` et `GatewayName`. Dans la console CloudWatch , vous pouvez utiliser l'affichage `Gateway Metrics` pour sélectionner facilement les dimensions propres aux bandes et 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 noms Amazon CloudWatch	Dimension	Description
`AWS/StorageGateway`	`GatewayId`, `GatewayName`	Ces dimensions filtrent les données des métriques qui décrivent des aspects de la passerelle de bande. Vous pouvez identifier une passerelle de bande à utiliser en spécifiant les dimensions `GatewayId` et `GatewayName`. Le débit et les données de latence d'une passerelle de bande reposent sur toutes les bandes virtuelles dans la passerelle de bande. Les données sont disponibles automatiquement toutes les 5 minutes sans coût aucun.

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

- Affichage des métriques disponibles
- Obtention des statistiques d'une métrique
- Création d'alarmes CloudWatch

Comprendre les métriques des bandes virtuelles

Vous trouverez, ci-après, des informations sur les métriques de Storage Gateway qui couvrent les bandes virtuelles. Chaque bande est associée à un ensemble de métriques.

Certaines métriques spécifiques aux bandes peuvent porter le même nom que certaines métriques spécifiques à la passerelle. Ces métriques représentent les mêmes types de mesures, mais s'appliquent à une bande plutôt qu'à une passerelle. Avant de commencer le travail, indiquez si vous souhaitez utiliser une métrique de passerelle ou une métrique de bande. Lorsque vous utilisez des métriques de bandes, spécifiez l'ID de la bande pour laquelle vous souhaitez afficher les métriques. Pour plus d'informations, consultez Utilisation d'Amazon CloudWatch Metrics.

> **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 de Storage Gateway que vous pouvez utiliser pour obtenir des informations sur vos bandes.

Métrique	Description
`CachePercentDirty`	Contribution de la bande pour le pourcentage global de cache de la passerelle qui n'est pas conservé dans AWS. L'exemple est pris à la fin de la période de génération de rapport. Utilisez la métrique `CachePercentDirty` de la passerelle pour afficher le pourcentage global de cache de la passerelle qui n'est pas conservé dans AWS. Pour de plus amples informations, veuillez consulter Présentation des métriques de la passerelle. Unités : pourcentage
`CloudTraffic`	Quantité d'octets chargés et téléchargés depuis le cloud vers la bande. Unité : Octets
`IoWaitPercent`	Pourcentage d' IoWait unités allouées actuellement utilisées par la bande. Unités : pourcentage
`HealthNotification`	Nombre de notifications d'intégrité envoyées par la bande. Unités : nombre

Métrique	Description
`MemUsedBytes`	Pourcentage de mémoire allouée actuellement utilisé par la bande. Unités : octets
`MemTotalBytes`	Pourcentage de mémoire totale actuellement utilisé par la bande. Unités : octets
`ReadBytes`	Nombre total d'octets lus depuis vos applications sur site au cours de la période de génération 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
`UserCpuPercent`	Pourcentage d'unités de calcul CPU allouées pour l'utilisateur qui sont actuellement utilisées par la bande. Unités : pourcentage
`WriteBytes`	Nombre total d'octets écrits dans vos applications sur site au cours de la période de génération de rapport. Utilisez cette métrique avec la statistique `Sum` pour mesurer le débit et avec la statistique `Samples` pour mesurer les IOPS. Unités : octets

Mesurer les performances entre votre Tape Gateway et AWS

Le débit des données, la latence des données et les opérations par seconde sont les trois mesures que vous pouvez utiliser pour comprendre la façon dont s'exécute le stockage d'application qui utilise votre passerelle de bande. Lorsque vous utilisez la statistique d'agrégation correcte, ces valeurs peuvent être mesurées en utilisant les métriques Storage Gateway qui disponibles.

Une statistique est l'agrégation d'une métrique sur une période de temps donnée. Lorsque vous affichez les valeurs d'une métrique dans CloudWatch, utilisez la `Average` statistique pour la latence des données (millisecondes) et pour les opérations d'entrée/sortie `Samples` par seconde (IOPS). Pour plus d'informations, consultez la section Statistiques du guide de CloudWatch l'utilisateur Amazon.

Le tableau suivant récapitule les métriques et la statistique correspondante que vous pouvez utiliser pour mesurer le débit, la latence et l'IOPS entre votre passerelle de bande et AWS.

Elément intéressant	Comment le mesurer
Latence	Utilisez les métriques `ReadTime` et `WriteTime` avec la statistique `Average` CloudWatch . Par exemple, la valeur `Average` de la métrique `ReadTime` vous donne la latence par opération sur l'échantillon de période.
Débit vers AWS	Utilisez les `CloudBytesUploaded` métriques `CloudBytesDownloaded` et avec les `Sum` CloudWatch statistiques. Par exemple, la `Sum` valeur de la `CloudBytesDownloaded` métrique sur une période d'échantillonnage de 5 minutes divisée par 300 secondes vous donne le débit entre AWS le Tape Gateway et le débit en octets par seconde.
Latence des données vers AWS	Utilisez la métrique `CloudDownloadLatency` avec la statistique `Average`. Par exemple, la statistique `Average` de la métrique `CloudDownloadLatency` vous donne la latence par opération.

Pour mesurer le débit de données de téléchargement depuis une passerelle sur bande vers AWS

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Sélectionnez l'onglet Métriques.

3. Choisissez la dimension StorageGateway: Gateway Metrics et recherchez la passerelle Tape Gateway avec laquelle vous souhaitez travailler.
4. Choisissez la métrique `CloudBytesUploaded`.
5. Pour Plage de temps, choisissez une valeur.
6. Choisissez la statistique `Sum`.
7. Pour Période, choisissez une valeur de 5 minutes ou plus.
8. Dans l'ensemble de points de données classés de façon chronologique obtenu, divisez chaque point de données par la période (en secondes) afin d'obtenir le débit pour l'échantillon de période. Par exemple, si le débit entre Tape Gateway et AWS est de 555 544 576 octets pour un point de données donné et que la période est de 300 secondes, le débit approximatif serait de 1,85 mégaoctet par seconde.

Pour mesurer la latence des données entre une passerelle sur bande et AWS

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Sélectionnez l'onglet Métriques.
3. Choisissez la GatewayMetrics dimension StorageGateway: et recherchez la passerelle Tape Gateway avec laquelle vous souhaitez travailler.
4. Choisissez la métrique `CloudDownloadLatency`.
5. Pour Plage de temps, choisissez une valeur.
6. Choisissez la statistique `Average`.
7. Pour Période, choisissez une valeur de 5 minutes afin qu'elle corresponde au temps par défaut du rapport.

L'ensemble de points de données classés chronologiquement obtenu contient la latence en millisecondes.

Pour définir une alarme de seuil supérieur pour le débit d'une passerelle de bande à AWS

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Create Alarm (Créer une alarme) pour lancer l'assistant de création d'alarmes.
3. Choisissez la dimension StorageGateway: Gateway Metrics et recherchez la passerelle Tape Gateway avec laquelle vous souhaitez travailler.
4. Choisissez la métrique `CloudBytesUploaded`.

5. Configurez l'alarme en définissant l'état de l'alarme lorsque la métrique `CloudBytesUploaded` est supérieure ou égale à une valeur spécifiée pendant une durée spécifiée. Par exemple, vous pouvez définir un état d'alarme lorsque la métrique `CloudBytesUploaded` est supérieure à 10 Mo pendant 60 minutes.
6. Configurez les actions mettre en œuvre pour l'état de l'alarme. Par exemple, vous pouvez faire en sorte qu'une notification vous soit envoyée par e-mail.
7. Sélectionnez Create Alarm (Créer une alerte).

Pour définir une alarme de seuil supérieur pour lire les données depuis AWS

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Create Alarm (Créer une alarme) pour lancer l'assistant de création d'alarmes.
3. Choisissez la dimension StorageGateway: Gateway Metrics et recherchez la passerelle Tape Gateway avec laquelle vous souhaitez travailler.
4. Choisissez la métrique `CloudDownloadLatency`.
5. Configurez l'alarme en définissant l'état de l'alarme lorsque la métrique `CloudDownloadLatency` est supérieure ou égale à une valeur spécifiée pendant une durée spécifiée. Par exemple, vous pouvez définir un état d'alarme lorsque `CloudDownloadLatency` est supérieure à 60 000 millisecondes pendant plus de 2 heures.
6. Configurez les actions mettre en œuvre pour l'état de l'alarme. Par exemple, vous pouvez faire en sorte qu'une notification vous soit envoyée par e-mail.
7. Sélectionnez Create Alarm (Créer une alerte).

Maintenance de votre passerelle

La maintenance de votre Tape Gateway inclut des tâches telles que le dimensionnement et la configuration des disques locaux pour le stockage en cache et l'espace tampon de téléchargement, la gestion des mises à jour et la définition d'un calendrier de mise à jour, la gestion de l'utilisation de la bande passante et l'arrêt ou la suppression de votre passerelle et des ressources associées si nécessaire. Ces tâches sont communes à tous les types de passerelle. Si vous n'avez pas créé de passerelle, consultez Création de votre passerelle.

Rubriques

- Gestion des disques locaux pour Storage Gateway- Apprenez à évaluer les exigences en matière de taille de disque, à augmenter la capacité de cache et à gérer les disques locaux que vous allouez à votre Tape Gateway pour la mise en mémoire tampon et le stockage.
- Gestion de la bande passante pour votre passerelle de bande- Découvrez comment limiter le débit de téléchargement depuis votre passerelle AWS afin de contrôler la quantité de bande passante réseau utilisée par la passerelle.
- 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 Tape Gateway .
- Arrêt de la machine virtuelle de la 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.
- 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 disques locaux pour Storage Gateway

La machine virtuelle de la passerelle utilise les disques locaux que vous allouez sur site pour le tampon et le stockage. Les passerelles créées sur les EC2 instances Amazon utilisent les volumes Amazon EBS comme disques locaux.

Rubriques

- Déterminer la quantité de stockage du disque local

- Configuration d'un stockage supplémentaire de tampon de chargement et de cache

Déterminer la quantité de stockage du disque local

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

- Les passerelles de bande requièrent au moins deux disques. L'un sera utilisé en tant que cache et l'autre en tant que tampon de chargement.

Le tableau suivant recommande des tailles pour le stockage du disque local associé à la passerelle déployée. Vous pouvez ajouter ultérieurement plus de stockage local une fois que vous avez configuré la passerelle et en fonction de l'augmentation de vos demandes de charge de travail.

Stockage local	Description
Tampon de chargement	Le tampon de chargement fournit une zone de transit pour les données avant que la passerell e ne charge les données sur Amazon S3. Votre passerelle charge ces données de tampon via une connexion chiffrée SSL (Secure Sockets Layer) à AWS.
Stockage de cache	Le stockage de cache fait office de stockage sur site durable des données en attente de chargement sur Amazon S3 à partir du tampon de chargement. Lorsque votre application effectue des E/S sur un volume ou une bande, la passerell e enregistre les données sur le stockage de cache pour l'accès à faible latence. Lorsque votre application demande les données

Stockage local	Description	
	d'une volume ou d'une bande, la passerelle recherche d'abord les données dans le stockage de cache avant de télécharger les données d' AWS.	

> **Note**
>
> Lorsque vous allouez des disques, nous vous recommandons vivement de ne pas allouer des disques locaux pour le stockage de tampon de chargement et de cache s'ils utilisent la même ressource physique (le même disque). 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 mettez en service un disque local (par exemple, pour utiliser comme stockage de cache ou tampon de chargement), vous avez la possibilité de 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 le stockage de cache et une autre pour le tampon de chargement. Une banque de données qui est basée sur un seul disque physique sous-jacent peut entraîner des performances médiocres dans certains cas si elle est utilisée pour soutenir le stockage de cache et le tampon de chargement. Cela est également vrai si la sauvegarde est une configuration RAID moins performante, telle que. RAID1

Après la configuration initiale et le déploiement de votre passerelle, vous pouvez ajuster le stockage local en ajoutant ou supprimant des disques pour un tampon de chargement. Vous pouvez également ajouter des disques pour le stockage de cache.

Détermination de la taille de tampon de chargement à allouer

Vous pouvez déterminer la taille du tampon de chargement à allouer en utilisant une formule de tampon de chargement. Nous vous recommandons vivement d'allouer au moins 150 Gio de tampon de chargement. Si la formule retourne une valeur inférieure à 150 Gio, utilisez 150 Gio comme

volume à allouer au tampon de chargement. Vous pouvez configurer jusqu'à 2 Tio de capacité de tampon de chargement pour chaque passerelle.

> **Note**
>
> Pour les passerelles de bande, lorsque le tampon de chargement atteint sa capacité, vos applications peuvent continuer à lire et écrire des données sur vos volumes de stockage. Cependant, Tape Gateway n'écrit aucune donnée de votre volume dans sa mémoire tampon de téléchargement et n'y télécharge aucune de ces données AWS tant que Storage Gateway n'a pas synchronisé les données stockées localement avec la copie des données stockées dans AWS. Cette synchronisation se produit lorsque les volumes ont le statut AMORÇAGE.

Afin d'estimer la quantité de tampon de chargement à allouer, vous pouvez déterminer les taux de données attendus entrants et sortants et les intégrer à la formule suivante.

Taux de données entrantes

Ce taux fait référence au débit de l'application, le taux auquel vos applications sur site écrivent des données sur votre passerelle pendant une période donnée.

Taux de données sortantes

Ce taux fait référence au débit du réseau, le taux auquel votre passerelle est capable de charger les données sur AWS. Ce taux dépend de la vitesse et de l'utilisation du réseau, ainsi que de l'activation de la limitation de bande passante. Ce taux doit être réglé pour la compression. Lors du téléchargement de données vers AWS, la passerelle applique une compression des données dans la mesure du possible. Par exemple, si vos données d'application sont uniquement du texte, vous pouvez obtenir un rapport de compression efficace d'environ 2:1. Toutefois, si vous écrivez des vidéos, la passerelle ne sera peut-être pas en mesure d'obtenir une compression des données et pourra nécessiter davantage de tampon de chargement pour la passerelle.

Nous vous recommandons fortement d'allouer au moins 150 Gio d'espace tampon de chargement si l'une des conditions suivantes est remplie :

- Votre taux d'entrée est plus élevé que le taux de sortie.
- La formule renvoie une valeur inférieure à 150 Gio.

Par exemple, supposons que vos applications métier écrivent des données de texte sur votre passerelle à un taux de 40 Mo par seconde pendant 12 heures par jour et que le débit de votre réseau soit de 12 Mo par seconde. En supposant un facteur de compression de 2:1 pour les données de texte, vous devez allouer environ 690 Gio d'espace pour le tampon de chargement.

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

Vous pouvez utiliser cette approximation au départ afin de déterminer la taille du disque que vous souhaitez allouer à la passerelle comme espace de tampon de chargement. Ajoutez plus d'espace de tampon de chargement en fonction des besoins à l'aide de la console Storage Gateway. Vous pouvez également utiliser les métriques CloudWatch opérationnelles d'Amazon pour surveiller l'utilisation de la mémoire tampon de téléchargement et déterminer les besoins de stockage supplémentaires. Pour plus d'informations sur les métriques et la configuration des alarmes, consultez Surveillance du tampon de chargement.

Détermination de la taille du stockage de cache à allouer

Votre passerelle utilise son stockage de cache pour fournir un accès à faible latence aux données récemment consultées. Le stockage de cache fait office de stockage sur site durable des données en attente de chargement sur Amazon S3 à partir du tampon de chargement. En général, vous dimensionnez le stockage de cache à 1,1 fois la taille du tampon de chargement. Pour plus d'informations sur l'estimation de la taille du stockage de cache, consultez Détermination de la taille de tampon de chargement à allouer.

Vous pouvez d'abord utiliser cette approximation pour mettre en service les disques du stockage de cache. 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 Surveillance du stockage de cache.

Configuration d'un stockage supplémentaire de tampon de chargement et de cache

Les besoins de votre application évoluant, vous pouvez accroître la capacité du tampon de chargement ou du stockage de 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 un cache ou une mémoire tampon de téléchargement à une passerelle existante, vous devez créer de nouveaux disques sur l'hyperviseur hôte de la passerelle ou sur l' EC2 instance Amazon. Ne supprimez pas ou ne modifiez pas la taille des disques existants qui ont déjà été alloués en tant que cache ou tampon de chargement.

Pour configurer le stockage supplémentaire de tampon de chargement ou de cache pour la passerelle

1. Provisionnez un ou plusieurs nouveaux disques sur votre passerelle, votre hyperviseur hôte ou votre EC2 instance Amazon. Pour obtenir des informations sur la façon d'allouer un disque dans un hyperviseur, consultez la documentation de votre hyperviseur. Pour plus d'informations sur le provisionnement de volumes Amazon EBS pour une EC2 instance Amazon, consultez les volumes Amazon EBS dans le guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Linux. Lors des étapes suivantes, vous allez configurer ce disque en tant que stockage de tampon de chargement ou de 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.
6. Dans la section Configurer le stockage, identifiez les disques que vous avez alloués. Si vos disques n'apparaissent pas, cliquez sur l'icône d'actualisation pour actualiser la liste. Pour chaque disque, choisissez TAMPON DE CHARGEMENT ou STOCKAGE DE CACHE dans le menu déroulant Alloué à.

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

Gestion de la bande passante pour votre passerelle de bande

Vous pouvez limiter (ou limiter) le débit de téléchargement depuis la passerelle vers votre passerelle AWS ou le débit de téléchargement depuis celle-ci AWS . La limitation de bande passante vous permet de contrôler la quantité de bande passante réseau utilisée par votre passerelle. Par défaut, une passerelle activée n'a pas de limites de taux pour les chargements ou téléchargements.

Vous pouvez spécifier la limite de débit à l' AWS Management Console aide de ou par programmation à l'aide de l'API Storage Gateway (voir UpdateBandwidthRateLimit) ou d'un kit de développement AWS logiciel (SDK). En limitant la bande passante par programme, vous pouvez modifier les limites automatiquement tout au long de la journée, par exemple en planifiant des tâches pour modifier la bande passante.

Vous pouvez également définir une limitation de bande passante basée sur une planification pour votre passerelle. Vous planifiez la régulation de la bande passante en définissant un ou plusieurs bandwidth-rate-limit intervalles. Pour de plus amples informations, veuillez consulter Limitation de bande passante basée sur une planification à l'aide de la console Storage Gateway.

La configuration d'un paramètre unique pour la limitation de la bande passante est l'équivalent fonctionnel de la définition d'un calendrier avec un bandwidth-rate-limit intervalle unique défini pour Everyday, avec une heure de début **`00:00`** et une heure de fin de. `23:59`

> **Note**
>
> Les informations de cette section sont spécifiques aux passerelles de bande et de volume. Pour gérer la bande passante d'une passerelle de fichiers Amazon S3, consultez Gestion de la bande passante pour votre passerelle de fichiers Amazon S3. Les limites de bande passante ne sont actuellement pas prises en charge pour Amazon FSx File Gateway.

Rubriques

- Modification de la limitation de bande passante à l'aide de la console Storage Gateway
- Limitation de bande passante basée sur une planification à l'aide de la console Storage Gateway
- Mise à jour des limites de bande passante de la passerelle à l'aide du AWS SDK pour Java

- Mise à jour des limites de bande passante de la passerelle à l'aide du AWS SDK pour .NET
- Mise à jour des limites de bande passante de la passerelle à l'aide du AWS Tools for Windows PowerShell

Modification de la limitation de bande passante à l'aide de la console Storage Gateway

La procédure suivante montre comment modifier la limitation de bande passante d'une passerelle à partir de la console Storage Gateway.

Pour modifier une limitation de bande passante de passerelle à l'aide de la console

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation gauche, choisissez Passerelles, puis sélectionnez la passerelle que vous souhaitez gérer.
3. Pour Actions, choisissez Modifier la limite de bande passante.
4. Dans la boîte de dialogue Modifier les limites de taux, entrez les nouvelles valeurs de limites, puis choisissez Enregistrer. Vos modifications apparaissent dans l'onglet Détails de la passerelle.

Limitation de bande passante basée sur une planification à l'aide de la console Storage Gateway

La procédure suivante montre comment modifier la limitation de bande passante d'une passerelle à partir de la console Storage Gateway.

Pour ajouter ou modifier une planification de limitation de la bande passante de la passerelle

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation gauche, choisissez Passerelles, puis sélectionnez la passerelle que vous souhaitez gérer.
3. Pour Actions, choisissez Modifier la limite de taux de bande passante.

Le bandwidth-rate-limit calendrier de la passerelle est affiché dans la boîte de dialogue Modifier le calendrier de limite de débit de bande passante. Par défaut, un nouveau bandwidth-rate-limit calendrier de passerelle est vide.

4. Dans la boîte de dialogue Modifier le calendrier de limite de bande passante, choisissez Ajouter un nouvel élément pour ajouter un nouvel bandwidth-rate-limit intervalle. Entrez les informations suivantes pour chaque bandwidth-rate-limit intervalle :

   - Jours de la semaine : vous pouvez créer un bandwidth-rate-limit intervalle pour les jours de semaine (du lundi au vendredi), pour les week-ends (samedi et dimanche), pour chaque jour de la semaine ou pour un ou plusieurs jours spécifiques de la semaine.
   - Heure de début : entrez l'heure de début de l'intervalle de bande passante dans le fuseau horaire local de la passerelle, en utilisant le format HH:MM.

     > **Note**
     >
     > Votre bandwidth-rate-limit intervalle commence au début de la minute que vous spécifiez ici.

   - Heure de fin — Entrez l'heure de fin de l' bandwidth-rate-limitintervalle dans le fuseau horaire local de la passerelle, en utilisant le format HH:MM.

     > **Important**
     >
     > L' bandwidth-rate-limitintervalle se termine à la fin de la minute spécifiée ici. Pour planifier un intervalle se terminant au bout d'une heure, entrez **`59`**.
     > Pour planifier des intervalles continus consécutifs, en effectuant la transition au début de l'heure, sans interruption entre les intervalles, entrez **`59`** pour la minute de fin du premier intervalle. Saisissez **`00`** pour la minute de début de l'intervalle suivant.

   - Taux de téléchargement : entrez la limite de taux de téléchargement, en kilobits par seconde (Kbits/s), ou sélectionnez Aucune limite pour désactiver la limitation de bande passante pour le téléchargement. La valeur minimale pour le taux de téléchargement est 100 Kbits/s.
   - Taux de chargement : entrez la limite du taux de téléchargement, en Kbits/s, ou sélectionnez Aucune limite pour désactiver la limitation de bande passante pour le téléchargement. La valeur minimale pour le taux de chargement est 50 Kbits/s.

Pour modifier vos bandwidth-rate-limit intervalles, vous pouvez saisir des valeurs révisées pour les paramètres des intervalles.

Pour supprimer vos bandwidth-rate-limit intervalles, vous pouvez choisir Supprimer à droite de l'intervalle à supprimer.

Une fois que vos modifications sont terminées, sélectionnez Enregistrer.

5. Continuez à ajouter bandwidth-rate-limit des intervalles en choisissant Ajouter un nouvel article et en saisissant le jour, les heures de début et de fin, ainsi que les limites de taux de téléchargement et de chargement.

> **Important**
>
> Bandwidth-rate-limitles intervalles ne peuvent pas se chevaucher. L'heure de début d'un intervalle doit être postérieure à l'heure de fin d'un intervalle précédent et antérieure à l'heure de début d'un intervalle suivant.

6. Après avoir saisi tous les bandwidth-rate-limit intervalles, choisissez Enregistrer les modifications pour enregistrer votre bandwidth-rate-limit planning.

Lorsque le bandwidth-rate-limit calendrier est correctement mis à jour, vous pouvez voir les limites de taux de téléchargement et de téléversement actuelles dans le panneau Détails de la passerelle.

Mise à jour des limites de bande passante de la passerelle à l'aide du AWS SDK pour Java

En mettant à jour les limites de bande passante par programme, vous pouvez ajuster vos limites automatiquement sur une période donnée, par exemple en utilisant des tâches planifiées. L'exemple suivant montre comment mettre à jour les limites de taux de bande passante à l'aide de AWS SDK pour Java. Pour utiliser l'exemple de code, vous devez maîtriser l'exécution d'une application de console Java. Pour plus d'informations, consultez Mise en route dans le Manuel du développeur AWS SDK pour Java .

Example : Mise à jour des limites de bande passante de la passerelle à l'aide du AWS SDK pour Java

L'exemple de code Java suivant met à jour les limites de taux de bande passante d'une passerelle. Pour utiliser ce code d'exemple, vous devez fournir le point de terminaison du service, le nom Amazon Resource Name (ARN) de la passerelle, ainsi que les limites de chargement et de téléchargement. Pour obtenir la liste des points de terminaison de AWS service que vous pouvez utiliser avec Storage Gateway, consultez la section AWS Storage Gateway Endpoints and Quotas dans le. Références générales AWS

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;


public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

    // Rates
    static long uploadRate = 51200;  // Bits per second, minimum 51200
    static long downloadRate = 102400;   // Bits per second, minimum 102400

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

        // Create a Storage Gateway client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

 UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
        sgClient.setEndpoint(serviceURL);

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);
```

```
    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

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

Mise à jour des limites de bande passante de la passerelle à l'aide du AWS SDK pour .NET

En mettant à jour les limites de bande passante par programme, vous pouvez ajuster vos limites automatiquement sur une période donnée, par exemple en utilisant des tâches planifiées. L'exemple suivant montre comment mettre à jour les limites de taux de bande passante à l'aide d' AWS SDK pour .NET. Pour utiliser l'exemple de code, vous devez maîtriser l'exécution d'une application de console .NET. Pour plus d'informations, consultez Mise en route dans le Manuel du développeur AWS SDK pour .NET .

Example : Mise à jour des limites de bande passante de la passerelle à l'aide du AWS SDK pour .NET

L'exemple de code C# suivant met à jour les limites de taux de bande passante d'une passerelle. Pour utiliser ce code d'exemple, vous devez fournir le point de terminaison du service, le nom Amazon Resource Name (ARN) de la passerelle, ainsi que les limites de chargement et de téléchargement. Pour obtenir la liste des points de terminaison de AWS service que vous pouvez utiliser avec Storage Gateway, consultez la section AWS Storage Gateway Endpoints and Quotas dans le. Références générales AWS

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Amazon.StorageGateway;
using Amazon.StorageGateway.Model;

namespace AWSStorageGateway
{
    class UpdateBandwidthExample
    {
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

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

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

        // Rates
        static long uploadRate = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

        public static void Main(string[] args)
        {
            // Create a Storage Gateway client
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = serviceURL;
            sgClient = new AmazonStorageGatewayClient(sgConfig);

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);
```

```
            Console.WriteLine("\nTo continue, press Enter.");
            Console.Read();
        }

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
 sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
 updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
 returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
 second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

Mise à jour des limites de bande passante de la passerelle à l'aide du AWS Tools for Windows PowerShell

En mettant à jour les limites de bande passante par programme, vous pouvez ajuster les limites automatiquement sur une période donnée, par exemple en utilisant des tâches planifiées. L'exemple suivant montre comment mettre à jour les limites de taux de bande passante à l'aide de AWS Tools for Windows PowerShell. Pour utiliser l'exemple de code, vous devez être familiarisé avec l'exécution

d'un PowerShell script. Pour plus d'informations, consultez Démarrer dans le Guide de l'utilisateur Outils AWS pour PowerShell .

Example : Mise à jour des limites de bande passante de la passerelle à l'aide du AWS Tools for Windows PowerShell

L'exemple de PowerShell script suivant met à jour les limites de bande passante d'une passerelle. Pour utiliser ce script d'exemple, vous devez fournir le nom Amazon Resource Name (ARN) de la passerelle, ainsi que les limites de chargement et de téléchargement.

```
<#
.DESCRIPTION
    Update Gateway bandwidth limits.

.NOTES
    PREREQUISITES:
    1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and region stored in session using Initialize-AWSDefault.
    For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html


.EXAMPLE
    powershell.exe .\SG_UpdateBandwidth.ps1
#>

$UploadBandwidthRate = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

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 EC2 instance Amazon dans le AWS 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 de la 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.

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 des mises à jour de maintenance mensuelles. Les mises à jour de maintenance mensuelles peuvent 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. 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 notes de version du logiciel Tape Gateway Appliance .

Les mises à jour de maintenance mensuelles 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. Vous pouvez réduire au minimum le risque de perturbation de vos applications provoqué par le redémarrage de la passerelle en augmentant les délais d'attente de votre initiateur iSCSI. Pour plus d'informations sur l'augmentation des délais de l'initiateur iSCSI pour Windows et Linux, consultez Personnalisation des paramètres iSCSI Windows et Personnalisation de vos paramètres iSCSI Linux.

Lorsque vous déployez et activez votre passerelle, un calendrier de maintenance hebdomadaire 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 mensuelles, mais nous vous recommandons de les laisser activées.

> **Note**
>
> Des mises à jour urgentes seront parfois 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 AWS Health Dashboard. Pour de plus amples informations, veuillez consulter AWS Health Dashboard. 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 applique automatiquement ces mises à jour conformément au calendrier de la fenêtre de maintenance configuré. Pour plus d'informations, voir .

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, procédez comme suit :

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 n'est pas possible de configurer le calendrier de maintenance pour 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.

Arrêt de la machine virtuelle de la passerelle

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

> **Important**
>
> Si vous arrêtez et démarrez une EC2 passerelle Amazon qui utilise un stockage éphémère, la passerelle sera définitivement hors ligne. 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 EC2 instance.

> **Note**
>
> Si vous arrêtez la passerelle tandis que votre logiciel de sauvegarde écrit sur une bande ou lit des données sur celle-ci, la tâche d'écriture ou de lecture est susceptible d'échouer. Avant d'arrêter la passerelle, vous devez vérifier votre logiciel de sauvegarde et la planification de sauvegarde pour toutes les tâches en cours.

- Console locale de la machine virtuelle de la passerelle : consultez Connexion à la console locale Tape Gateway.
- API Storage Gateway : voir ShutdownGateway

Démarrage et arrêt d'une passerelle de bande

Pour arrêter une passerelle de bande

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle à arrêter. L'état de la passerelle est En cours d'exécution.
3. Dans le menu Actions, choisissez Stop gateway (Arrêter la passerelle) et vérifiez l'ID de la passerelle dans la boîte de dialogue, puis choisissez Arrêter la passerelle (Stop gateway).

   Pendant l'arrêt de la passerelle, un message indiquant l'état de la passerelle est susceptible de s'afficher. Lorsque la passerelle s'arrête, un message et un bouton Démarrer la passerelle s'affichent dans l'onglet Détails.

Lorsque vous arrêtez votre passerelle, les ressources de stockage ne sont pas accessibles tant que vous ne démarrez pas votre stockage. Si la passerelle téléchargeait des données lorsqu'elle a été arrêtée, le chargement reprendra lorsque vous démarrerez la passerelle.

Pour démarrer une passerelle de bande

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle à démarrer. L'état de la passerelle est Fermeture.
3. Sélectionnez Détails et choisissez Démarrer la passerelle.

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 sur la console de AWS Storage Gateway gestion et sa connexion iSCSI à l'initiateur est fermée. La procédure de suppression d'une passerelle est identique pour tous les types de passerelle. Toutefois, en fonction du type de passerelle que vous souhaitez supprimer et de l'hôte sur lequel il est déployé, vous suivez les instructions de suppression des ressources associées.

> **Note**
>
> Lorsque vous supprimez une passerelle de bande, toutes les bandes actuellement en `AVAILABLE` état sont également supprimées et toutes les données qu'elles contiennent sont perdues. Si vous souhaitez conserver les données des bandes utilisées par une passerelle que vous souhaitez supprimer, vous devez archiver les bandes avant de supprimer la passerelle. Pour plus d'informations, consultez Archivage des bandes virtuelles.

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.

Rubriques

- Suppression de la passerelle à l'aide de la console Storage Gateway

- Suppression de ressources à partir d'une passerelle déployée sur site
- Suppression de ressources d'une passerelle déployée sur une EC2 instance Amazon

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 EC2 instance Amazon, l'instance continue d'exister 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.

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 les bandes virtuelles, les instantanés Amazon Elastic Block Store (Amazon EBS) et EC2 les instances Amazon persistent. Vous continuerez à être facturé pour ces ressources. Vous pouvez choisir de supprimer les EC2 instances Amazon et les instantanés Amazon EBS en annulant votre abonnement Amazon. EC2 Si vous souhaitez conserver votre EC2 abonnement Amazon, vous pouvez supprimer vos instantanés Amazon EBS à l'aide de la console Amazon EC2.

Suppression de ressources à partir d'une passerelle déployée sur site

Vous pouvez utiliser les instructions suivantes pour supprimer les ressources à partir d'une passerelle déployée sur site.

Suppression de ressources à partir d'une passerelle de bande déployée sur une machine virtuelle

Lorsque vous supprimez une passerelle ou une bibliothèque de bandes virtuelles, vous effectuez des étapes de nettoyage supplémentaires avant et après la suppression de la passerelle. Ces étapes supplémentaires vous aident à supprimer les ressources dont vous n'avez pas besoin pour éviter de continuer à les payer.

Si la passerelle de bande à supprimer est déployée sur une machine virtuelle (VM), nous vous recommandons de procéder comme suit pour nettoyer les ressources.

> **Important**
>
> Avant de supprimer une passerelle de bande, vous devez annuler toutes les opérations de récupération de bandes et éjecter toutes les bandes récupérées.
> Une fois que vous avez supprimé la passerelle de bande, vous devez supprimer toutes les ressources associées à la passerelle de bande dont vous n'avez pas besoin afin d'éviter de payer pour ces ressources.

Lorsque vous supprimez une passerelle de bande, vous pouvez rencontrer l'un des deux scénarios suivants.

- La passerelle de bande est connectée à AWS : si la passerelle de bande est connectée à la passerelle AWS et que vous la supprimez, les cibles iSCSI associées à la passerelle (c'est-à-dire les lecteurs de bandes virtuels et le changeur de média) ne seront plus disponibles.
- La passerelle de bande n'est pas connectée à AWS : si la passerelle de bande n'est pas connectée AWS, par exemple si la machine virtuelle sous-jacente est désactivée ou si votre réseau est en panne, vous ne pouvez pas supprimer la passerelle. Si vous essayez de le faire, lorsque votre environnement fonctionnera à nouveau, vous pouvez disposer d'une passerelle de bande qui s'exécute sur site avec des cibles iSCSI disponibles. Cependant, aucune donnée Tape Gateway ne sera chargée vers, ni téléchargée depuis, AWS.

Si la passerelle de bande à supprimer ne fonctionne pas, vous devez tout d'abord la désactiver avant de la supprimer comme décrit ci-après :

- Pour supprimer les bandes ayant le statut RECUPEREE à partir de la bibliothèque, éjectez la bande à l'aide de votre logiciel de sauvegarde. Pour obtenir des instructions, reportez-vous à Archivage de la bande.

Après avoir désactivé la passerelle de bande et supprimé les bandes, vous pouvez supprimer la passerelle de bande. Pour plus d'informations sur la suppression d'une passerelle, consultez Suppression de la passerelle à l'aide de la console Storage Gateway.

Si vous avez des bandes archivées, ces bandes restent et vous continuez à payer pour leur stockage jusqu'à ce que vous les supprimiez. Pour des instructions sur la suppression des bandes d'une archive, consultez Suppression de bandes virtuelles de votre Tape Gateway.

> **Important**
>
> 90 jours de stockage minimum vous sont facturés pour les bandes virtuelles dans une archive. Si vous extrayez une bande virtuelle qui a été stockée dans l'archive pendant moins de 90 jours, vous êtes toujours facturé pour le stockage de 90 jours.

Suppression de ressources d'une passerelle déployée sur une EC2 instance Amazon

Si vous souhaitez supprimer une passerelle que vous avez déployée sur une EC2 instance Amazon, nous vous recommandons de nettoyer les AWS ressources utilisées avec la passerelle, en particulier l' EC2 instance Amazon, tous les volumes Amazon EBS, ainsi que les bandes si vous avez déployé une passerelle sur bande. Vous éviterez ainsi des coûts d'utilisation imprévus.

Suppression des ressources de votre passerelle de bande déployée sur Amazon EC2

Si vous avez déployé une passerelle de bande, nous vous invitons à procéder comme suit pour supprimer votre passerelle, puis nettoyer ses ressources :

1. Supprimez toutes les bandes virtuelles que vous avez récupérées dans votre passerelle de bande. Pour plus d'informations, consultez Suppression de bandes virtuelles de votre Tape Gateway.
2. Supprimez toutes les bandes virtuelles de la bibliothèque de bandes. Pour plus d'informations, consultez Suppression de bandes virtuelles de votre Tape Gateway.
3. Supprimez la passerelle de bande. Pour de plus amples informations, veuillez consulter Suppression de la passerelle à l'aide de la console Storage Gateway.
4. Mettez fin à toutes les EC2 instances Amazon et supprimez tous les volumes Amazon EBS. Pour plus d'informations, consultez Nettoyez votre instance et votre volume dans le guide de EC2 l'utilisateur Amazon.
5. Supprimez toutes les bandes virtuelles archivées. Pour plus d'informations, consultez Suppression de bandes virtuelles de votre Tape Gateway.

> **Important**
>
> 90 jours de stockage minimum vous sont facturés pour les bandes virtuelles dans l’archive. Si vous extrayez une bande virtuelle qui a été stockée dans l’archive pendant moins de 90 jours, vous êtes toujours facturé pour le stockage de 90 jours.

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. La console locale s'exécute directement sur la plate-forme hôte de virtualisation qui héberge votre dispositif de passerelle. Pour les passerelles sur site, vous accédez à la console locale via votre hôte de VMware virtualisation KVM Hyper-V ou Linux. Pour les EC2 passerelles Amazon, vous accédez à la console en vous connectant à l' EC2instance Amazon via SSH. 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 des tâches sur la console locale de 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 EC2 locale Amazon- Apprenez à vous connecter à la console locale pour effectuer des tâches de configuration de base et avancées pour une EC2 passerelle Amazon, 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'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 Tape 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 Tape 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 Tape 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 des tâches sur la console locale de machine virtuelle

Pour une passerelle de que vous déployez sur site, vous pouvez effectuer les tâches de maintenance suivantes à l'aide de la console locale de passerelle à laquelle vous accédez depuis la plate-forme hôte de votre 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 Tape Gateway- Découvrez comment vous connecter à la console locale de la passerelle où vous pouvez configurer les paramètres réseau de la passerelle et modifier le mot de passe par défaut.
- Configuration d'un SOCKS5 proxy pour votre passerelle sur site- Découvrez comment configurer Storage Gateway pour acheminer tout le trafic des AWS terminaux via un serveur proxy Socket Secure version 5 (SOCKS5).

- Configuration de votre passerelle réseau- Découvrez comment configurer votre passerelle pour utiliser le protocole DHCP ou attribuer une adresse IP statique.
- Test de votre connexion de passerelle à Internet- Découvrez comment utiliser la console locale de la passerelle pour tester la connexion entre la passerelle et Internet.
- Exécution de commandes de passerelle de stockage dans la console locale pour une passerelle locale- Découvrez comment exécuter des commandes de console locales qui vous permettent d'effectuer des tâches supplémentaires telles que l'enregistrement de tables de routage, la connexion à Support, etc.
- 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 disponibles pour votre appliance de passerelle.

Connexion à la console locale Tape 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, utilisez les informations d'identification par défaut pour vous connecter. Ces informations d'identification par défaut vous donnent accès aux menus, dans lesquels vous pouvez configurer les paramètres réseau de la passerelle et changer le mot de passe de la console locale. Storage Gateway vous permet de définir votre propre mot de passe depuis la AWS Storage Gateway console au lieu de le modifier depuis la console locale. Vous n'avez pas besoin de connaître le mot de passe par défaut pour définir un nouveau mot de passe. Pour plus d'informations, consultez Définition du mot de passe de la console locale à partir de la console Storage Gateway.

Pour vous connecter à la console locale de la passerelle

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

  Sinon, utilisez vos informations d'identification pour vous connecter.

  > **Note**
  >
  > Nous vous recommandons de 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 de commandes de passerelle de stockage dans la console locale pour une passerelle locale. Vous pouvez également définir votre propre mot de passe depuis la AWS Storage Gateway console. Pour de plus amples informations, veuillez consulter Définition du mot de passe de la console locale à partir de la console Storage Gateway.

> **Important**
>
> Pour les anciennes versions de la passerelle de volume ou de bande, le nom d'utilisateur est `sguser` et le mot de passe est `sgpassword`. Si vous réinitialisez votre mot de passe et que votre passerelle est mise à jour vers une version plus récente, votre nom d'utilisateur passera à admin mais le mot de passe sera conservé.

Définition du mot de passe de la console locale à partir de la console Storage Gateway

Lorsque vous vous connectez à la console locale pour la première fois, vous vous connectez à la machine virtuelle avec les informations d'identification par défaut. Le nom d'utilisateur est `admin` et le mot de passe est `password`. Nous vous recommandons de définir toujours un nouveau mot de passe immédiatement après avoir créé votre nouvelle passerelle. Vous pouvez définir ce mot de passe à partir de la console AWS Storage Gateway au lieu de la console locale si vous le souhaitez. Vous n'avez pas besoin de connaître le mot de passe par défaut pour définir un nouveau mot de passe.

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

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez la passerelle pour laquelle vous souhaitez définir un nouveau mot de passe.
3. Pour Actions, choisissez Set Local Console Password (Définir le mot de passe de la console locale).
4. Dans la boîte de dialogue Définir le mot de passe de la console locale, tapez un nouveau mot de passe, confirmez-le, puis choisissez Enregistrer. Votre nouveau mot de passe remplace le mot de passe par défaut. Storage Gateway n'enregistre pas le mot de passe mais le transmet en toute sécurité à la machine virtuelle.

> **Note**
>
> Le mot de passe peut être constitué de n'importe quel caractère sur le clavier et peut comporter de 1 à 512 caractères.

Configuration d'un SOCKS5 proxy pour votre passerelle sur site

Les passerelles de volume et les passerelles de bande prennent en charge la configuration d'un proxy Socket Secure version 5 (SOCKS5) entre votre passerelle sur site et. AWS

> **Note**
>
> La seule configuration de proxy prise en charge est SOCKS5.

Si votre passerelle doit utiliser un serveur proxy pour communiquer avec Internet, vous devez configurer les paramètres de proxy SOCKS de votre passerelle. Pour cela, spécifiez un numéro de port et une adresse IP pour l'hôte exécutant le proxy. Ensuite, Storage Gateway achemine tout le trafic via le serveur proxy. Pour plus d'informations sur les exigences en matière de réseau pour votre passerelle, consultez Exigences pour le réseau et le pare-feu.

La procédure suivante vous montre comment configurer un proxy SOCKS pour une passerelle de volume et une passerelle de bande.

Pour configurer un SOCKS5 proxy pour les passerelles de volume et de bande

1. Connectez-vous à la console locale de la passerelle.
   - 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.
   - KVM – Pour plus d'informations, consultez Accès à la console locale de la passerelle avec Linux KVM.
2. Dans le menu principal AWS Storage Gateway - Configuration, entrez le chiffre correspondant pour sélectionner Configuration de proxy SOCKS.

3. Dans le menu Configuration du proxy SOCKS de AWS Storage Gateway, entrez le chiffre correspondant pour effectuer l'une des tâches suivantes :

Pour exécuter cette tâche	Procédez comme suit
Configurer un proxy SOCKS	Saisissez le chiffre correspondant pour sélectionner Configurer le proxy SOCKS. Vous devez fournir un nom d'hôte et un port pour finaliser la configuration.
Afficher la configuration actuelle du proxy SOCKS	Saisissez le chiffre correspondant pour sélectionner Afficher la configuration de proxy SOCKS. Si aucun proxy SOCKS n'est configuré, le message `SOCKS Proxy not configured` s'affiche. Si un proxy SOCKS est configuré, le nom d'hôte et le port du proxy s'affichent.
Supprimer une configuration de proxy SOCKS	Saisissez le chiffre correspondant pour sélectionner Supprimer la configuration de proxy SOCKS. Le message `SOCKS Proxy Configuration Removed` s'affiche.

4. Redémarrez votre machine virtuelle pour appliquer votre configuration HTTP.

Configuration de votre passerelle réseau

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.

   - 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.
   - KVM – Pour plus d'informations, consultez Accès à la console locale de la passerelle avec Linux KVM.

2. Dans le menu principal de AWS Storage Gateway - Configuration, entrez le chiffre correspondant pour sélectionner Configuration de réseau.
3. Dans le menu Configuration de réseau AWS Storage Gateway, effectuez l'une des tâches suivantes :

Pour exécuter cette tâche	Procédez comme suit
Décrire la carte réseau	Saisissez le chiffre correspondant pour sélectionner Décrire la carte. La liste des noms de cartes s'affiche et vous êtes invité à saisir un nom de carte, 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 DHCP activé

Pour exécuter cette tâche	Procédez comme suit
	Vous utilisez les noms de cartes répertoriés ici lorsque vous configurez une adresse IP statique ou que vous définissez la carte par défaut de votre passerelle.
Configurer 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 plus d'informations, consultez Arrêt de la machine virtuelle de la passerelle. Si votre passerelle utilise plusieurs interfaces réseau, vous devez définir toutes les interfaces

Pour exécuter cette tâche	Procédez comme suit
	activées pour utiliser DHCP ou des adresses IP statiques. Par exemple, supposons que votre machine virtuelle 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 utiliseront 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.

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 la machine virtuelle de la passerelle.
Définir la carte de routage par défaut de la passerelle	Saisissez le chiffre correspondant pour sélectionner Définir la carte par défaut. Les cartes disponibles pour votre passerelle sont affichées et vous êtes invité à sélectionner l'une des cartes, par exemple **`eth0`**.
Afficher la configuration DNS de la passerelle	Saisissez le chiffre correspondant pour sélectionner Afficher la configuration DNS. Les adresses IP des serveurs de noms DNS principaux et secondaires s'affichent.

Pour exécuter cette tâche	Procédez comme suit
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 votre connexion de passerelle à Internet

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

Pour tester la connexion de la passerelle à Internet

1. Connectez-vous à la console locale de la passerelle.
   - 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.
   - KVM – Pour plus d'informations, consultez Accès à la console locale de la passerelle avec Linux KVM.
2. Dans le menu principal de AWS Storage Gateway - Configuration, entrez le chiffre correspondant pour sélectionner Tester la connectivité de 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.

Exécution de commandes de passerelle de stockage dans la console locale pour une passerelle 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 :

Command	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, consultez Configuration de votre réseau de passerelle.
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, consultez Configuration de votre réseau de passerelle.
iptables	Outil d'administration pour le filtrage des IPv4 paquets et le NAT.

Command	Fonction
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.
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.
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@amaz on.com, il est probable qu'une applicati on effectue une inspection SSL. Dans ce cas, nous recommandons de contourner l'inspection SSL pour l'appliance Storage Gateway.
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.

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

Message	Description
	passerelle ne fonctionne pas correctement. Storage Gateway affiche un message qui décrit les résultats de la vérification de la ressource.

La console affiche également le nombre d'erreurs et d'avertissements en regard de l'option de menu de contrôle de la ressource.

Exécution de tâches sur la console EC2 locale Amazon

Certaines tâches de maintenance de Storage Gateway nécessitent que vous vous connectiez à la console locale de la passerelle pour une passerelle que vous avez déployée sur une EC2 instance Amazon. Vous pouvez accéder à la console locale de la passerelle sur votre EC2 instance Amazon à l'aide d'un client Secure Shell (SSH). Les rubriques de cette section décrivent comment se connecter à la console locale de la passerelle et effectuer des tâches de maintenance.

Rubriques

- Connexion à votre console locale Amazon EC2 Gateway- Découvrez comment vous connecter et vous connecter à la console locale de passerelle de votre EC2 instance Amazon à l'aide d'un client Secure Shell (SSH).
- Routage de votre passerelle déployée EC2 via un proxy HTTP- Découvrez comment configurer Storage Gateway pour acheminer tout le trafic AWS des terminaux via un serveur proxy Socket Secure version 5 (SOCKS5) vers votre instance Amazon EC2 Gateway.
- Test de la connectivité réseau des passerelles- Découvrez comment utiliser la console locale de la passerelle pour tester la connectivité réseau entre votre passerelle et diverses ressources réseau.
- Affichage de l'état des ressources système de la passerelle- Découvrez comment utiliser la console locale de passerelle pour vérifier les cœurs de processeur virtuels, la taille du volume racine et la RAM disponibles pour votre appliance de passerelle.
- Exécution des commandes Storage Gateway sur la console locale- Découvrez comment exécuter des commandes de console locales qui vous permettent d'effectuer des tâches supplémentaires telles que l'enregistrement de tables de routage, la connexion à Support, etc.

Connexion à votre console locale Amazon EC2 Gateway

Vous pouvez vous connecter à votre EC2 instance Amazon à l'aide d'un client Secure Shell (SSH). Pour obtenir des informations détaillées, consultez Connect to Your Instance dans le guide de EC2 l'utilisateur Amazon. Pour ce type de connexion, vous aurez besoin de la paire de clés SSH que vous avez spécifiée lorsque vous avez lancé l'instance. Pour plus d'informations sur les paires de EC2 clés Amazon, consultez Amazon EC2 Key Pairs dans le guide de EC2 l'utilisateur Amazon.

Pour se connecter à la console locale de la passerelle

1. Connectez-vous à votre console locale. Si vous vous connectez à votre EC2 instance depuis un ordinateur Windows, connectez-vous en tant qu'administrateur.
2. Une fois connecté, le menu principal Configuration d'AWS Storage Gateway s'affiche, à partir duquel vous pouvez effectuer diverses tâches.

Pour en savoir plus sur cette tâche	Consultez cette rubrique
Configurer un proxy SOCKS pour la passerelle	Routage de votre passerelle déployée EC2 via un proxy HTTP
Tester la connectivité réseau	Test de la connectivité réseau des passerelles
Exécuter les commandes de console Storage Gateway	Exécution des commandes Storage Gateway sur la console locale
Consulter le contrôle d'une ressource système	Affichage de l'état des ressources système de la passerelle.

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

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

Routage de votre passerelle déployée EC2 via un proxy HTTP

Storage Gateway prend en charge la configuration d'un proxy Socket Secure version 5 (SOCKS5) entre votre 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, consultez Connexion à votre console locale Amazon EC2 Gateway.
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 des passerelles

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, consultez Connexion à votre console locale Amazon EC2 Gateway.
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 obtenir des instructions, consultez Connexion à votre console locale Amazon EC2 Gateway.
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.

Exécution des commandes Storage Gateway sur la console locale

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, consultez Connexion à votre console locale Amazon EC2 Gateway.
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 :

Command	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.
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.
iptables	Outil d'administration pour le filtrage des IPv4 paquets et le NAT.

Command	Fonction
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.
save-iptables	Conservez les tableaux IP.
save-routing-table	Enregistrez l'entrée de table de routage récemment ajoutée.
sslcheck	Vérifiez la validité du protocole SSL pour le dépannage du réseau.
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 le nom de la commande suivi de l'option `-h`, par exemple : `sslcheck -h`.

Performances et optimisation pour Tape Gateway

Cette section décrit les performances de Storage Gateway.

Rubriques

- Recommandations en matière de performances pour les passerelles de bande
- Optimisation des performances de la passerelle

Recommandations en matière de performances pour les passerelles de bande

Dans cette section, vous trouverez des recommandations de configuration à des fins de mise en service du matériel pour la machine virtuelle de votre passerelle de bande. Les tailles et types d' EC2 instances Amazon répertoriés dans le tableau sont des exemples et sont fournis à titre de référence.

Configuration	Débit d'écriture Gbit/s	Lecture à partir du cache débit G bit/s	Lire depuis le cloud d'Amazon Web Services, débit en Gbit/s
Plateforme hôte : EC2 instance Amazon — c5.4xlarge CPU : 16 vCPU | RAM : 32 Go Disque racine : 80 Go, SSD io1, 4 000 IOPS Disque cache : RAID rayé (2 x 500 Go, disque SSD io1 EBS, 25000) IOPs Disque tampon de télécharg ement : 450 Go, disque SSD io1, 2000 IOPs	2.3	4.0	2.2

Configuration	Débit d'écriture Gbit/s	Lecture à partir du cache débit G bit/s	Lire depuis le cloud d'Amazon Web Services, débit en Gbit/s
Bande passante réseau vers le cloud : 10 Gbit/s			
Plateforme hôte : Appliance matérielle Storage Gateway Disque de cache : 2,5 To Disque tampon de chargement : 2 To Bande passante réseau vers le cloud : 10 Gbit/s	2.3	8,8	3.8
Plateforme hôte : Amazon EC2instance — c5d.9xlarge CPU : 36 vCPU | RAM : 72 Go Disque racine : 80 Go, SSD io1, 4 000 IOPS Disque cache : disque de 900 Go NVMe Disque tampon de télécharg ement : NVMe disque de 900 Go Bande passante réseau vers le cloud : 10 Gbit/s	5.2	11.6	5.2

Configuration	Débit d'écriture Gbit/s	Lecture à partir du cache débit G bit/s	Lire depuis le cloud d'Amazon Web Services, débit en Gbit/s
Plateforme hôte : Amazon EC2instance — c5d.metal CPU : 96 vCPU | RAM : 192 Go Disque racine : 80 Go, SSD io1, 4 000 IOPS Disque cache : RAID rayé (2 NVMe disques de 900 Go) Disque tampon de télécharg ement : NVMe disque de 900 Go Bande passante réseau vers le cloud : 10 Gbit/s	5.2	11.6	7.2

Note

Cette performance a été obtenue en utilisant simultanément une taille de bloc de 1 Mo et dix lecteurs de bandes.

Les EC2 configurations présentées dans le tableau ci-dessus sont uniquement destinées à être représentatives des performances que vous pourriez atteindre sur vos propres serveurs physiques dotés de ressources similaires. Par exemple, les EC2 configurations utilisant un RAID par bandes ont été effectuées par le biais d'un mécanisme spécial qui n'est généralement pas pris en charge par notre passerelle sur EC2. Pour obtenir des performances similaires, vous devez plutôt utiliser un contrôleur RAID matériel connecté au serveur sur site exécutant votre passerelle.

Vos performances peuvent varier en fonction de la configuration de votre plateforme hôte et de la bande passante réseau.

Pour améliorer les performances en écriture et en lecture de votre passerelle de bande, consultez Optimiser les paramètres iSCSI, Utiliser une taille de bloc supérieure pour les lecteurs de bandes et Optimisation des performances des lecteurs de bandes virtuelles dans le logiciel de sauvegarde.

Optimisation des performances de la passerelle

Configuration recommandée du serveur de passerelle

Pour optimiser les performances de votre passerelle, Storage Gateway recommande la configuration de passerelle suivante pour le serveur hôte de votre passerelle :

- Au moins 64 cœurs de CPU physiques dédiés
- Pour une passerelle de bande, votre matériel doit dédier les quantités de RAM suivantes :
  - Au moins 16 Gio de RAM réservée pour les passerelles avec une taille de cache maximale de 16 Tio
  - Au moins 32 Gio de RAM réservée pour les passerelles avec une taille de cache maximale de 16 à 32 Tio
  - Au moins 48 Gio de RAM réservée pour les passerelles avec une taille de cache maximale de 32 à 64 Tio

> **Note**
>
> Pour optimiser les performances de la passerelle, vous devez allouer au moins 32 Gio de RAM.

- Disque 1, à utiliser comme cache de passerelle comme suit :
  - RAID rayé (réseau redondant de disques indépendants) composé de NVMe SSDs.
- Disque 2, à utiliser comme tampon de chargement de passerelle comme suit :
  - RAID rayé composé de NVMe SSDs.
- Disque 3, à utiliser comme tampon de chargement de passerelle comme suit :
  - RAID rayé composé de NVMe SSDs.
- 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 VMXnet3 ajoutez-en un (10 Gbit/s) à utiliser pour vous connecter AWS.

Ajouter des ressources à la passerelle

Les goulots d'étranglement suivants peuvent réduire les performances de votre Tape Gateway en deçà du débit soutenu maximal théorique (votre bande passante vers le cloud) : AWS

- Nombre de cœurs de CPU
- Débit du disque de cache/tampon de chargement
- Quantité totale de RAM
- Bande passante réseau pour AWS
- Bande passante du réseau entre l'initiateur et la passerelle

Cette section décrit les étapes à suivre pour optimiser les performances de votre passerelle. Ces recommandations reposent sur l'ajout de ressources à votre passerelle ou à votre serveur d'application.

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

Le débit des disques de cache et de tampon de chargement peut limiter les performances de chargement et de téléchargement de votre passerelle. Si les performances de votre passerelle sont nettement inférieures aux attentes, envisagez d'améliorer le débit des disques de cache et de tampon de chargement en effectuant les actions suivantes :

- Utilisation d'un RAID agrégé par bandes tel que le RAID 10 pour améliorer le débit des disques, idéalement avec un contrôleur RAID matériel.

> **Note**
>
> Les configurations RAID (réseau redondant de disques indépendants), ou plus spécifiquement les configurations RAID agrégées par bandes, comme le RAID 10, consistent à diviser un jeu de données en blocs et à répartir les blocs de données sur plusieurs périphériques de stockage. Le niveau RAID que vous utilisez influe sur la

vitesse exacte et la tolérance aux pannes que vous pouvez atteindre. En répartissant les charges de travail d'E/S sur plusieurs disques, le débit global du périphérique RAID est bien supérieur à celui de n'importe quel disque unique.

- Utilisation de disques hautes performances attachés directement

  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. Les performances améliorées des disques entraînent généralement un débit plus élevé et un nombre plus élevé d'opérations d'entrée/sortie par seconde (IOPS).

  Pour mesurer le débit, utilisez les `WriteBytes` métriques `ReadBytes` et avec les CloudWatch statistiques `Samples` Amazon. 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. Pour plus d'informations sur les métriques de passerelle, consultez Mesurer les performances entre votre Tape Gateway et AWS.

  > **Note**
  >
  > CloudWatch les métriques ne sont pas disponibles pour toutes les passerelles. Pour obtenir des informations sur les métriques de passerelle, consultez Surveillance de Storage Gateway.

Ajouter d'autres disques tampons de chargement

Pour obtenir un débit d'écriture plus élevé, ajoutez au moins deux disques tampons de chargement. Lorsque des données sont écrites sur la passerelle, elles sont écrites et stockées localement sur les disques tampons de chargement. Ensuite, les données locales stockées sont lues de manière asynchrone à partir des disques à traiter et charger sur AWS. L'ajout de disques tampons de chargement supplémentaires peut réduire le nombre d'opérations d'E/S simultanées effectuées sur chaque disque individuel. Cela peut entraîner une augmentation du débit d'écriture vers la passerelle.

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

Lorsque vous mettez en service les disques d’une passerelle, nous vous recommandons vivement de ne pas mettre en service des disques locaux pour le stockage de tampon de chargement et de cache qui utilisent la même ressource de stockage physique sous-jacente (c’est-à-dire, le même disque). 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 ou RAID 6, peut entraîner des performances médiocres.

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 chaque processeur virtuel attribué à la machine virtuelle de la passerelle est soutenus par un cœur de CPU dédié. 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 la passerelle de gérer, en parallèle, le stockage des données de votre application vers votre stockage local et le chargement de ces données vers Amazon S3. 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.

Augmentez la bande passante entre votre passerelle et le cloud AWS

L'augmentation de votre bande passante à destination et en provenance AWS augmentera le taux maximal d'entrée de données vers votre passerelle et de sortie vers AWS le cloud. Cela peut

améliorer les performances de votre passerelle si la vitesse du réseau est le facteur limitant dans la configuration de votre passerelle, plutôt que d'autres facteurs tels que des disques lents ou une faible bande passante de connexion entre la passerelle et l'initiateur.

La bande passante réseau à destination et en provenance AWS définit les performances moyennes maximales théoriques de votre Tape Gateway lors de charges de travail prolongées.

- La vitesse moyenne à laquelle vous pouvez écrire des données sur votre passerelle de bande sur de longs intervalles ne dépassera pas votre bande passante de chargement vers AWS.
- La vitesse moyenne à laquelle vous pouvez lire les données depuis votre Tape Gateway sur de longs intervalles ne dépassera pas votre bande passante de téléchargement AWS.

> **Note**
>
> Les performances de votre passerelle observées seront probablement inférieures à la bande passante de votre réseau en raison d'autres facteurs limitatifs répertoriés ici, tels que le débit du disque de cache/tampon de chargement, le nombre de cœurs de CPU, la quantité totale de RAM ou la bande passante entre votre initiateur et la passerelle. De plus, le fonctionnement normal de votre passerelle implique de nombreuses mesures prises pour protéger vos données, ce qui peut entraîner une baisse des performances observées par rapport à la bande passante du réseau.

Optimiser les paramètres iSCSI

Vous pouvez optimiser les paramètres iSCSI sur votre initiateur iSCSI pour obtenir des performances d'E/S supérieures. Nous vous recommandons de choisir 256 Ko pour `MaxReceiveDataSegmentLength` et `FirstBurstLength`, et 1 Mo pour `MaxBurstLength`. Pour plus d'informations sur la configuration des paramètres iSCSI, consultez Personnalisation des paramètres iSCSI.

> **Note**
>
> Ces paramètres recommandés peuvent participer à obtenir de meilleures performances globales. Toutefois, les paramètres iSCSI spécifiques nécessaires pour optimiser les performances varient en fonction du logiciel de sauvegarde que vous utilisez. Pour plus de détails, consultez la documentation de votre logiciel de sauvegarde.

Utiliser une taille de bloc supérieure pour les lecteurs de bandes

Pour une passerelle de bande, la taille de bloc par défaut pour un lecteur de bande est de 64 Ko. Cependant, vous pouvez augmenter la taille de bloc jusqu'à 1 Mo afin d'améliorer les performances d'E/S.

La taille de bloc choisie dépend de la taille de bloc maximale prise en charge par votre logiciel de sauvegarde. Nous vous recommandons de définir la taille de bloc des lecteurs de bandes dans votre logiciel de sauvegarde sur une taille aussi importante que possible. Toutefois, cette taille de bloc ne doit pas être supérieure à 1 Mo, c'est-à-dier la taille maximale prise en charge par la passerelle.

Les passerelles de bande négocient la taille de bloc des lecteurs de bandes virtuelles afin que cela corresponde automatiquement à ce qui est défini sur le logiciel de sauvegarde. Lorsque vous augmentez la taille de bloc sur le logiciel de sauvegarde, nous vous recommandons de vérifier également les paramètres afin de vous assurer que l'hôte initiateur prend en charge la nouvelle taille du bloc. Pour plus d'informations, consultez la documentation de votre logiciel de sauvegarde. Pour plus d'informations sur les performances de passerelles spécifiques, consultez Performances et optimisation pour Tape Gateway.

Optimisation des performances des lecteurs de bandes virtuelles dans le logiciel de sauvegarde

Votre logiciel de sauvegarde peut sauvegarder des données sur un maximum de 10 lecteurs de bandes virtuelles sur une passerelle de bande en même temps. Nous vous recommandons de configurer les tâches de sauvegarde dans votre logiciel de sauvegarde de façon à utiliser au moins 4 lecteurs de bandes virtuelles simultanément sur la passerelle de bande. Vous pouvez obtenir un meilleur débit d'écriture lorsque le logiciel de sauvegarde sauvegarde les données sur plusieurs bandes virtuelles en même temps.

En règle générale, vous pouvez obtenir un débit maximal plus élevé en utilisant (en lecture ou en écriture) un plus grand nombre de bandes virtuelles en même temps. En utilisant davantage de lecteurs de bande, vous permettez à votre passerelle de traiter un plus grand nombre de demandes simultanément, ce qui peut améliorer les performances.

Ajouter des ressources à votre environnement d'application

Augmenter la bande passante entre le serveur d'application et la passerelle

La connexion entre votre initiateur iSCSI et votre passerelle peut limiter les performances de chargement et de téléchargement. Si les performances de votre passerelle sont nettement inférieures aux attentes et que vous avez déjà augmenté votre nombre de cœurs de CPU et votre débit de disque, pensez à prendre les mesures suivantes :

- Mise à niveau de vos câbles réseau pour augmenter la bande passante entre l'initiateur et la passerelle.
- Utilisation d'autant de lecteurs de bande simultanément que possible. L'iSCSI ne prend pas en charge la mise en file d'attente de plusieurs demandes pour la même cible, ce qui signifie que plus vous utilisez de lecteurs de bande, plus votre passerelle peut traiter de demandes simultanément. Cela vous permettra d'utiliser plus pleinement la bande passante entre votre passerelle et l'initiateur, augmentant ainsi le débit apparent de votre 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 métriques `ReadBytes` et `WriteBytes` de la passerelle afin de mesurer le débit total des données. Pour plus d'informations sur ces métriques, consultez Mesurer les performances entre votre Tape Gateway et AWS.

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 charge d'E/S.

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 cela 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 cloud Amazon Web Services. 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.

Rubriques

- Protection des données dans AWS Storage Gateway
- Identity and Access Management pour AWS Storage Gateway
- Validation de conformité pour AWS Storage Gateway
- Résilience dans AWS Storage Gateway
- Sécurité de l'infrastructure dans AWS Storage Gateway
- AWS Bonnes pratiques en matière de sécurité
- Connexion et surveillance dans AWS 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 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 AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS 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

Storage Gateway utilise SSL/TLS (Secure Socket Layers/Transport Layer Security (Layer Security) pour chiffrer les données transférées entre votre dispositif de passerelle et le AWS stockage. Par défaut, Storage Gateway utilise des clés de chiffrement gérées par Amazon S3 (SSE-S3) pour chiffrer côté serveur toutes les données stockées dans Amazon S3. Vous pouvez utiliser l'API Storage Gateway pour configurer votre passerelle afin de chiffrer les données stockées dans le cloud à l'aide du chiffrement côté serveur avec des clés AWS Key Management Service (SSE-KMS).

> **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 .

Chiffrement d'un partage de fichiers

Pour un partage de fichiers, vous pouvez configurer votre passerelle pour chiffrer vos objets à l'aide de clés gérées par AWS KMS, à l'aide de SSE-KMS. Pour plus d'informations sur l'utilisation de l'API Storage Gateway pour chiffrer les données écrites sur un partage de fichiers, voir Create NFSFile Share dans le guide de référence des AWS Storage Gateway API.

Chiffrement d'un volume

Pour les volumes mis en cache et stockés, vous pouvez configurer votre passerelle pour chiffrer les données de volume stockées dans le cloud à l'aide de clés AWS KMS gérées à l'aide de l'API Storage Gateway. Vous pouvez définir l'une des clés gérées comme la clé KMS. La clé que vous utilisez pour chiffrer votre volume ne peut pas être modifié une fois que le volume est créé. Pour plus d'informations sur l'utilisation de l'API Storage Gateway pour chiffrer des données écrites sur un volume mis en cache ou stocké, consultez CreateCachediSCSIVolumeou consultez le Guide de CreateStorediSCSIVolumeréférence des AWS Storage Gateway API.

Chiffrement d'une bande

Pour une bande virtuelle, vous pouvez configurer votre passerelle pour chiffrer les données sur bande stockées dans le cloud à l'aide de clés AWS KMS gérées à l'aide de l'API Storage Gateway. Vous pouvez définir l'une des clés gérées comme la clé KMS. La clé que vous utilisez pour chiffrer vos données de bande ne peut pas être modifiée une fois que la bande est créée. Pour plus d'informations sur l'utilisation de l'API Storage Gateway pour chiffrer des données écrites sur une bande virtuelle, reportez-vous CreateTapesà la section AWS Storage Gateway API Reference.

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. En d'autres termes, les données sont chiffrées dans Amazon S3.
- 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 .
- Si vous supprimez ou désactivez votre AWS AWS KMS clé ou si vous révoquez le jeton d'autorisation, vous ne pouvez pas accéder aux données du volume ou de la bande. Pour plus d'informations, consultez Suppression des clés KMS dans le Guide du développeur AWS Key Management Service .
- Si vous créez un instantané à partir d'un volume chiffré par KMS, l'instantané est chiffré. Si vous créez un instantané à partir d'un volume chiffré par KMS, l'instantané est chiffré.
- Si vous créez un nouveau volume à partir d'un instantané chiffré par KMS, le volume est chiffré. Vous pouvez spécifier une autre clé KMS pour le nouveau volume.

> **Note**
>
> Storage Gateway ne prend actuellement pas en charge la création d'un volume non chiffré à partir d'un point de récupération d'un volume chiffré par KMS ou d'un instantané chiffré par KMS.

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

Identity and Access Management pour AWS Storage Gateway

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. 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 des accès à l'aide de politiques
- Comment AWS Storage Gateway fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour Storage Gateway
- Résolution des problèmes AWS d'identité et d'accès à Storage Gateway

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans AWS SGW.

Utilisateur du service : si vous utilisez le service AWS SGW pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités AWS SGW pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS SGW, consultez Résolution des problèmes AWS d'identité et d'accès à Storage Gateway.

Administrateur du service — Si vous êtes responsable des ressources de la AWS SGW dans votre entreprise, vous avez probablement un accès complet à la AWS SGW. C'est à vous de déterminer à quelles fonctionnalités et ressources AWS SGW les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AWS SGW, consultez. Comment AWS Storage Gateway fonctionne avec IAM

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS SGW. Pour consulter

des exemples de politiques basées sur l'identité AWS SGW que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Storage Gateway

Authentification par des identités

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

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est

appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, 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 au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour 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 au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas,

vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser 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.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser

un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

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.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

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.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou

rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique 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. 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

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.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder

à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez 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. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. 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

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. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie

de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. 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. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

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

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. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

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

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` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition AWS SGW, consultez 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

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 des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

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

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. 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.

Sessions d'accès transmises pour AWS SGW

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions 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 aux services : 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

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources AWS SGW. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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 AWS 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, un utilisateur doit 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 ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

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.

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. Parmi eux figurent SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR, et 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— 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.

An Région AWS est un emplacement physique dans le monde entier où les centres de données sont regroupés en cluster. 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 mondiale, Storage Gateway propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données :

- Utilisez VMware vSphere High Availability (VMware HA) pour protéger les charges de travail de stockage contre les défaillances matérielles, d'hyperviseurs ou de réseau. Pour de plus amples informations, veuillez consulter Utilisation de VMware vSphere High Availability avec Storage Gateway.
- Archivez des bandes virtuelles dans S3 Glacier Flexible Retrieval. Pour plus d'informations, consultez Archivage des bandes virtuelles.

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 le livre blanc Amazon Web Services : Overview of Security Processes.

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 .

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 dans 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 d' CloudTrail événements vers un compartiment Amazon S3, y compris des 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 compte Amazon Web Services lorsque vous créez le compte. Lorsqu'une activité se produit dans Storage Gateway, elle est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte Amazon Web

Services. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements dans votre compte Amazon Web Services, y compris les événements pour Storage Gateway, créez un journal de suivi. 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 de suivi consigne les événements de toutes les régions dans la partition AWS , et il livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour 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 AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la 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 de passerelle

Vous trouverez ci-dessous des informations sur les meilleures pratiques et les problèmes de résolution des problèmes liés aux passerelles, aux plateformes hôtes, aux bandes virtuelles, à la haute disponibilité, à la restauration des données et à la sécurité. 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 de connexion à la passerelle- Découvrez comment diagnostiquer les problèmes susceptibles de faire apparaître votre passerelle hors ligne dans la console Storage Gateway.
- Résolution des problèmes : erreur interne lors de l'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.
- Dépannage des problèmes de 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.
- Dépannage de configuration 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 liés à EC2 la passerelle Amazon- Trouvez des informations sur les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec des passerelles déployées sur Amazon EC2.
- Résolution des problèmes des appliances matérielles- Découvrez comment résoudre les problèmes que vous pourriez rencontrer avec l'appliance matérielle Storage Gateway.
- Dépannage des problèmes de bandes virtuelles- Découvrez les mesures que vous pouvez prendre si vous rencontrez des problèmes inattendus avec vos bandes virtuelles.
- Résolution des 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 : problèmes de connexion à la passerelle

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 au [réseau et au pare-feu Exigences relatives](#) 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 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 celle-ci et la rendre inaccessible. 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, veillez à prendre des mesures pour récupérer vos données. Pour plus d'informations, consultez Meilleures pratiques pour récupérer 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 :

1. Arrêtez la passerelle.
2. Réinitialisez le disque de cache.
3. Reconfigurez le disque pour le stockage en cache.
4. Redémarrez la passerelle.

Pour plus d'informations sur le dépannage d'un disque cache endommagé pour une passerelle de bande, voir Vous devez récupérer une bande virtuelle à partir d'un disque de cache défectueux.

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) ou à l'instance Amazon Elastic Compute Cloud (Amazon EC2) de la passerelle 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 la marche à suivre 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 EC2 instance Amazon, 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 connexion de votre passerelle à Internet .

> **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 de passerelle Synchronisation de l'heure de votre machine virtuelle passerelle

L'option System Time Management n'est pas disponible sur les passerelles hébergées sur des EC2 instances Amazon. Pour vous assurer qu'Amazon EC2 Gateway peut correctement synchroniser l'heure, vérifiez que l' EC2 instance Amazon peut se connecter à la liste de pool 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

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 sur 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 d'un point de terminaison pour Storage Gateway.

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 de passerelle Synchronisation de l'heure de votre machine virtuelle passerelle

L'option System Time Management n'est pas disponible sur les passerelles hébergées sur des EC2 instances Amazon. Pour vous assurer qu'Amazon EC2 Gateway peut correctement synchroniser l'heure, vérifiez que l' EC2 instance Amazon peut se connecter à la liste de pool 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 est EC2 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 volet 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.

Dépannage des problèmes de 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 de les activer pour résoudre les problèmes liés Support à votre passerelle.

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. Si vous avez toujours du mal à trouver l'adresse IP de la passerell e : • 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. • SSL certifie l'un validation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign ou l'autre des certificats. • 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 terminais on de service. Pour plus d'informations sur les exigences de réseau et de pare-feu, consultez Exigences pour le réseau et le pare-feu.
L'activation de votre passerelle échoue lorsque vous cliquez sur le bouton	• Vérifiez que la machine virtuelle de la passerelle est accessible en faisant un ping de la machine virtuelle à partir du client.

Problème	Action à exécuter
Passer à l'activation dans la console de gestion Storage Gateway.	• 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 Configuration d'un SOCKS5 proxy pour votre passerelle sur site. • 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. Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux • 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. • SSL certifie l'un validation/inspection should not be activated. Storage Gateway utilizes mutual TLS authentication which would fail if any 3rd party application tries to intercept/sign ou l'autre des certificats. • Vérifiez que votre machine virtuelle dispose d'au moins 7,5 Go de RAM. L'attribution de la passerelle échoue s'il y a moins de 7,5 Go de RAM. Pour plus d'informations, consultez Exigences relatives à la configuration de Tape Gateway.

Problème	Action à exécuter
Vous devez supprimer un disque alloué en tant qu'espace de tampon de chargement. Par exemple, vous devrez peut-être réduire la quantité d'espace du tampon de chargemen t d'une passerelle ou remplacer un disque utilisé comme tampon de chargement qui a échoué.	Pour plus d'informations sur la suppression d'un disque alloué comme espace de tampon de chargement, consultez Suppression de disques de votre passerelle.
Vous avez besoin d'amélior er 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 adaptateu r 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 AWS 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 Mesurer les performan ces entre votre Tape Gateway et AWS. 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 la machine virtuelle de la 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 votre connexion de passerelle à Internet.
	• Vérifiez la configuration de la carte réseau de votre passerelle et veillez à ce que toutes les interfaces qui doivent être activées pour la passerelle le soient réellement. Pour afficher la configura tion de la carte réseau de votre passerelle, suivez les instructi ons de Configuration de votre passerelle réseau et sélectionnez l'option d'affichage de la configuration du réseau de la 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 provenanc e de votre passerelle AWS, voir Mesurer les performances entre votre Tape Gateway et AWS.

Problème	Action à exécuter
Vous rencontrez des problèmes d'importation (déploiement) de Storage Gateway sur Microsoft Hyper-V.	Consultez Dépannage de configuration de Microsoft Hyper-V, qui traite des problèmes les plus courants de déploiement d'une passerelle sur Microsoft Hyper-V.
Vous recevez un message 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.

Permettre Support de 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'activation Support pour accéder à votre passerelle afin de vous aider à résoudre les problèmes liés à la passerelle. Par défaut, Support l'accès à votre passerelle est désactivé. Vous fournissez cet accès par le biais de 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 autoriser Support l'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. Entrez **`exit`** pour vous déconnecter de la console de passerelle.
8. Suivez les invites pour quitter la console locale.

Dépannage de configuration 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'importe r 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 identific ateur. 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 Tape 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 Tape 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 Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux.
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 liés à EC2 la passerelle Amazon

Dans les sections suivantes, vous trouverez les problèmes courants que vous pourriez rencontrer lors de l'utilisation de votre passerelle déployée sur Amazon EC2. Pour plus d'informations sur la différence entre une passerelle sur site et une passerelle déployée sur Amazon EC2, consultezDéployez une EC2 instance Amazon personnalisée pour Tape Gateway.

Rubriques

- L'activation de votre passerelle ne se produit pas au bout de quelques instants
- Vous ne trouvez pas votre instance de EC2 passerelle dans la liste des instances
- Vous avez créé un volume Amazon EBS mais vous ne parvenez pas à l'associer à votre instance de EC2 passerelle
- Vous obtenez un message indiquant qu'aucun disque n'est disponible lorsque vous essayez d'ajouter des volumes de stockage
- Vous souhaitez supprimer un disque alloué comme espace de tampon de chargement pour réduire l'espace du tampon de chargement
- Le débit à destination ou en provenance de votre EC2 passerelle tombe à zéro
- Vous souhaitez aider Support à résoudre les problèmes liés à votre passerelle EC2

- Vous souhaitez vous connecter à votre instance de passerelle à l'aide de la console EC2 série Amazon

L'activation de votre passerelle ne se produit pas au bout de quelques instants

Vérifiez les points suivants dans la EC2 console Amazon :

- Le port 80 est activé 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 Ajouter une règle de groupe de sécurité dans le guide de EC2 l'utilisateur Amazon.
- L'instance de passerelle est marquée comme étant en cours d'exécution. Dans la EC2 console Amazon, la valeur State de l'instance doit être RUNNING.
- Assurez-vous que votre type d' EC2 instance Amazon répond aux exigences minimales, comme décrit dansBesoins de stockage.

Après avoir corrigé le problème, essayez à nouveau d'activer la passerelle. Pour ce faire, ouvrez la console Storage Gateway, choisissez Deploy a new Gateway on Amazon EC2, puis saisissez à nouveau l'adresse IP de l'instance.

Vous ne trouvez pas votre instance de EC2 passerelle 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 avez créé un volume Amazon EBS mais vous ne parvenez pas à l'associer à votre instance de EC2 passerelle

Vérifiez que le volume Amazon EBS en question est dans la même zone de disponibilité que l'instance de passerelle. S'il y a une différence dans les zones de disponibilité, créez un nouveau volume Amazon EBS dans la même zone de disponibilité que votre instance.

Vous obtenez un message indiquant qu'aucun disque n'est disponible lorsque vous essayez d'ajouter des volumes de stockage

Pour une passerelle nouvellement activée, aucun volume de stockage n'est défini. Avant de pouvoir définir le volume de stockage, vous devez allouer des disques locaux à la passerelle. Ceux-ci seront utilisés comme stockage de tampon de chargement et de cache. Pour une passerelle déployée sur Amazon EC2, les disques locaux sont des volumes Amazon EBS attachés à l'instance. Ce message d'erreur se produit généralement si aucun volume Amazon EBS n'est définie pour l'instance.

Vérifiez les appareils de bloc définis pour l'instance qui exécute la passerelle. S'il y a seulement deux appareils de bloc (les appareils par défaut fournis avec l'AMI), vous devez ajouter du stockage. Pour plus d'informations sur la procédure à utiliser, consultez Déployez une EC2 instance Amazon personnalisée pour Tape Gateway. Après avoir attaché deux ou plusieurs volumes Amazon EBS, essayez de créer le stockage de volume sur la passerelle.

Vous souhaitez supprimer un disque alloué comme espace de tampon de chargement pour réduire l'espace du tampon de chargement

Suivez les étapes de Détermination de la taille de tampon de chargement à allouer.

Le débit à destination ou en provenance de votre EC2 passerelle tombe à zéro

Vérifiez que l'instance de passerelle est en cours d'exécution. Si l'instance démarre en raison d'un redémarrage, par exemple, attendez que le redémarrage soit terminé.

Vérifiez également que l'IP de la passerelle IP n'a pas changé. Si l'instance a été arrêtée, puis redémarrée, son adresse IP a peut-être changé. Dans ce cas, vous devez activer une nouvelle 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 AWS, voir Mesurer les performances entre votre Tape Gateway et AWS.

Vous souhaitez aider Support à résoudre les problèmes liés à votre passerelle EC2

Storage Gateway fournit une console locale que vous pouvez utiliser pour effectuer plusieurs tâches de maintenance, notamment l'activation Support pour accéder à votre passerelle afin de vous aider à résoudre les problèmes liés à la passerelle. Par défaut, Support l'accès à votre passerelle est désactivé. Vous fournissez cet accès via la console EC2 locale Amazon. Vous vous connectez à la console EC2 locale Amazon via un 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 la façon d'ajouter une règle de groupe de sécurité, consultez les groupes EC2 de sécurité Amazon dans le guide de EC2 l'utilisateur Amazon.

Pour autoriser la Support connexion à votre passerelle, vous devez d'abord vous connecter à la console locale de l' EC2 instance Amazon, accéder à la console de Storage Gateway, puis fournir l'accès.

Pour activer Support l'accès à une passerelle déployée sur une EC2 instance Amazon

1. Connectez-vous à la console locale de votre EC2 instance Amazon. Pour obtenir des instructions, rendez-vous sur Connect to your instance dans le guide de EC2 l'utilisateur Amazon.

   Vous pouvez utiliser la commande suivante pour vous connecter à la console locale de l' EC2 instance.

   ```
   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 EC2 clés que vous avez utilisée pour lancer l' EC2 instance Amazon. Pour plus d'informations, consultez la section Extraction de la clé publique de votre paire de clés dans le guide de l' EC2 utilisateur Amazon.
> *INSTANCE-PUBLIC-DNS-NAME*Il s'agit du nom DNS (Domain Name System) public de votre EC2 instance Amazon sur laquelle s'exécute votre passerelle. Vous obtenez ce nom DNS public en sélectionnant l' EC2instance Amazon dans la EC2 console et en cliquant 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 tant que vous ne vous Support êtes pas informé que la session d'assistance 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.

Vous souhaitez vous connecter à votre instance de passerelle à l'aide de la console EC2 série Amazon

Vous pouvez utiliser la console EC2 série Amazon pour résoudre les 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 d'Amazon Elastic Compute Cloud.

Résolution des problèmes des appliances matérielles

Les rubriques suivantes présentent les problèmes rencontrés lors de l'utilisation de l'appliance matérielle Storage Gateway et les suggestions en matière de dépannage.

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 effectuer une réinitialisation d'usine sur votre appareil, contactez l'équipe de l'appliance matérielle Storage Gateway pour obtenir de l'aide, comme décrit dans la section support ci-après.

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 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.

Dépannage des problèmes de bandes virtuelles

Vous trouverez ci-après des informations sur les actions à mettre en œuvre si vous rencontrez des problèmes inattendus avec les bandes virtuelles.

Rubriques

- Récupération d'une bibliothèque de bandes virtuelles à partir d'une passerelle irrécupérable
- Résolution des problèmes de bandes irrécupérables
- Notifications d'intégrité relatives à la haute disponibilité

Récupération d'une bibliothèque de bandes virtuelles à partir d'une passerelle irrécupérable

Bien que cela soit rare, votre passerelle de bande peut rencontrer une défaillance irrécupérable. Une défaillance de ce type peut se produire dans votre hôte hyperviseur, la passerelle elle-même ou les disques de cache. En cas de défaillance, vous pouvez récupérer vos bandes en suivant les instructions de dépannage de cette section.

Rubriques

- Vous avez besoin de récupérer une bande virtuelle à partir d'une passerelle de bande défaillante
- Vous avez besoin de récupérer une bande virtuelle à partir d'un disque de cache défectueux

Vous avez besoin de récupérer une bande virtuelle à partir d'une passerelle de bande défaillante

Si votre Tape Gateway ou l'hôte de l'hyperviseur rencontre une défaillance irréparable, vous pouvez récupérer toutes les données qui ont déjà été téléchargées AWS vers une autre passerelle de bande.

Notez que les données écrites sur une bande peuvent ne pas être complètement chargées tant que cette bande n'a pas été archivée correctement dans VTS. Les données contenues sur les bandes récupérées sur une autre passerelle de cette façon peuvent être incomplètes ou vides. Nous recommandons de réaliser un inventaire de toutes les bandes récupérées afin de vérifier qu'elles contiennent le contenu attendu.

Pour récupérer une bande sur une autre passerelle de bande

1. Identifiez une passerelle de bande existante en état de marche qui jouera le rôle de passerelle cible de récupération. Si vous n'avez pas de passerelle de bande sur laquelle récupérer les bandes, créez une nouvelle passerelle de bande. Pour obtenir des informations sur la création d'une passerelle, consultez Création de passerelle.
2. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
3. Dans le volet de navigation, sélectionnez Passerelles, puis choisissez la passerelle de bande à partir de laquelle vous souhaitez récupérer des bandes.
4. Cliquez sur l'onglet Détails. Un message de récupération de bande s'affiche dans l'onglet.
5. Choisissez Créer des bandes de récupération pour désactiver la passerelle.
6. Dans la boîte de dialogue qui s'affiche, sélectionnez Désactiver la passerelle.

   Ce processus arrête de façon permanente le fonctionnement normal de votre passerelle de bande et expose les points de récupération disponibles. Pour obtenir des instructions, consultez Désactiver votre passerelle de bande.
7. Sur les bandes affichées par la passerelle désactivée, choisissez la bande virtuelle et le point de récupération que vous souhaitez récupérer. Une bande virtuelle peut avoir plusieurs points de récupération.
8. Pour commencer la récupération des bandes voulues sur la passerelle de bande cible, choisissez Créer une bande de récupération.
9. Dans la boîte de dialogue Créer une bande de récupération, vérifiez le code à barres de la bande virtuelle que vous souhaitez récupérer.

10. Pour Passerelle, choisissez la passerelle de bande sur laquelle vous souhaitez transférer la bande virtuelle récupérée.
11. Choisissez Créer une bande de récupération.
12. Supprimez la passerelle de bande défaillante afin de ne pas être facturé. Pour obtenir des instructions, consultez Suppression de votre passerelle et suppression des ressources associées.

Storage Gateway déplace la bande de la passerelle de bande défaillante vers la passerelle de bande que vous avez spécifiée. La passerelle de bande marque le statut de la bande comme RÉCUPÉRÉ.

Vous avez besoin de récupérer une bande virtuelle à partir d'un disque de cache défectueux

Si le cache de votre disque rencontre une erreur, la passerelle empêche les opérations de lecture et d'écriture sur les bandes virtuelles de la passerelle. Par exemple, une erreur peut se produire lorsqu'un disque est corrompu ou supprimé de la passerelle. La console Storage Gateway affiche un message concernant l'erreur.

Dans le message d'erreur, Storage Gateway vous invite à choisir une des deux actions qui peuvent récupérer vos bandes :

- Arrêter et ajouter à nouveau des disques : adoptez cette approche si le disque contient des données intactes et qu'il a été retiré. Par exemple, si l'erreur s'est produite parce qu'un disque a été supprimé accidentellement de votre hôte, mais que le disque et les données sont intactes, vous pouvez ajouter à nouveau le disque. Pour ce faire, consultez la procédure mentionnée plus loin dans cette rubrique.
- Réinitialiser le disque de cache : Adoptez cette approche si le disque de cache est corrompu ou n'est pas accessible. Si l'erreur de disque rend le disque de cache inaccessible, inutilisable ou corrompu, vous pouvez réinitialiser le disque. Si vous réinitialisez le disque de cache, les bandes ayant des données propres (c'est-à-dire, les bandes pour lesquelles les données du disque de cache et d'Amazon S3 sont synchronisées) continueront d'être disponibles pour l'utilisation. Cependant, les bandes ayant des données qui ne sont pas synchronisées avec Amazon S3 sont automatiquement récupérées. L'état de ces bandes est défini sur RECUPEREE, mais les bandes seront en lecture seule. Pour plus d'informations sur la suppression d'un disque de votre hôte, consultez Détermination de la taille de tampon de chargement à allouer.

> **Important**
>
> Si le disque de cache que vous réinitialisez contient des données qui n'ont pas encore été chargées sur Amazon S3, ces données peuvent être perdues. Une fois que vous avez réinitialisé les disques de cache, aucun disque de cache configuré ne reste sur la passerelle. Vous devez donc configurer au moins un nouveau disque de cache pour que la passerelle fonctionne correctement.

Pour réinitialiser le disque de cache, consultez la procédure mentionnée plus loin dans cette rubrique.

Pour arrêter et ajouter à nouveau un disque

1. Arrêtez la passerelle. Pour plus d'informations sur l'arrêt d'une passerelle, consultez Arrêt de la machine virtuelle de la passerelle.
2. Ajoutez le disque à votre hôte et veillez à ce que le nombre de nœuds de disque du disque n'ait pas changé. Pour plus d'informations sur la façon d'ajouter un disque, consultez Détermination de la taille de tampon de chargement à allouer.
3. Redémarrez la passerelle. Pour plus d'informations sur le redémarrage d'une passerelle, consultez Arrêt de la machine virtuelle de la passerelle.

Après le redémarrage de la passerelle, vous pouvez vérifier l'état des disques du cache. L'état d'un disque peut avoir les valeurs suivantes :

- présent : le disque est disponible pour l'utilisation.
- manquant : le disque n'est plus connecté à la passerelle.
- décalage : le nœud de disque est occupé par un disque qui a des métadonnées incorrectes ou le contenu du disque est corrompu.

Pour réinitialiser et reconfigurer un disque de cache

1. Dans le message d'erreur Une erreur de disque s'est produite illustré précédemment, choisissez Réinitialiser le disque de cache.

2. Sur la page Configurer la passerelle, configurez le disque du stockage de cache. Pour obtenir des informations sur la façon de faire, consultez Configurer votre passerelle de bande.
3. Une fois que vous avez configuré le stockage de cache, arrêtez et redémarrez la passerelle comme décrit dans la procédure précédente.

La passerelle doit récupérer après le redémarrage. Vous pouvez ensuite vérifier l'état du cache du disque.

Pour vérifier l'état d'un disque de cache

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, choisissez Passerelles, puis sélectionnez votre passerelle.
3. Sur Actions, choisissez Configurer le stockage local pour afficher la boîte de dialogue Configurer le stockage local. Cette boîte de dialogue affiche tous les disques locaux de la passerelle.

L'état du nœud du disque de cache s'affiche à côté du disque.

> **Note**
>
> Si vous n'effectuez pas le processus de récupération, la passerelle affiche une bannière qui vous invite à configurer le stockage local.

Résolution des problèmes de bandes irrécupérables

Si la bande virtuelle échoue de façon inattendue, Storage Gateway définit le statut de la bande ayant échoué sur IRRÉCUPÉRABLE. L'action mise en œuvre varie selon les circonstances. Vous trouverez ci-après des informations sur certains problèmes potentiels et sur leur dépannage.

Vous devez récupérer des données à partir d'une bande IRRECUPERABLE

Si vous avez une bande virtuelle avec l'état IRRECUPERABLE et que vous devez l'utiliser, effectuez l'une des actions suivantes :

- Activez une nouvelle passerelle de bande si aucune n'est activée. Pour plus d'informations, consultez Création d'une passerelle.

- Désactivez la passerelle de bande qui contient la bande irrécupérable et récupérez celle-ci à partir d'un point de récupération vers la nouvelle passerelle de bande. Pour plus d'informations, consultez Vous avez besoin de récupérer une bande virtuelle à partir d'une passerelle de bande défaillante.

> **Note**
>
> Vous devez reconfigurer l'application de sauvegarde et l'initiateur iSCSI afin d'utiliser la nouvelle passerelle de bande. Pour plus d'informations, consultez Connexion de vos appareils VTL.

Bande inutile à l'état IRRECOVERABLE qui n'est pas archivée

Si vous avez une bande virtuelle dont l'état est IRRECOVERABLE, que vous n'en avez pas besoin et qu'elle n'a jamais été archivée, vous devez la supprimer. Pour plus d'informations, consultez Suppression de bandes virtuelles de votre Tape Gateway.

Un disque de cache de votre passerelle rencontre une défaillance

Si un ou plusieurs disque de cache rencontrent une erreur, la passerelle empêche les opérations de lecture et d'écriture sur les bandes virtuelles et les volumes. Pour reprendre le fonctionnement normal, reconfigurez votre passerelle comme décrit ci-dessous :

- Si le disque de cache est inaccessible ou inutilisable, supprimez-le de la configuration de votre passerelle.
- Si le disque de cache est toujours accessible et utilisable, reconnectez-le à votre passerelle.

> **Note**
>
> Si vous effacez un disque de cache, les bandes ou les volumes ayant des données propres (c'est-à-dire, pour lesquels les données du disque de cache et d'Amazon S3 sont synchronisées) continueront d'être disponibles lorsque la passerelle retourne à un fonctionnement normal. Par exemple, si votre passerelle possède trois disques de cache et que vous en supprimez deux, les bandes ou volumes propres auront le statut DISPONIBLE. Les autres bandes et volumes auront le statut IRRÉCUPÉRABLE.
> Si vous utilisez des disques éphémères comme disques de cache pour votre passerelle ou si vous montez vos disques de cache sur un lecteur éphémère, vos disques de cache seront

perdus lorsque vous fermerez la passerelle. L'arrêt de la passerelle lorsque votre disque de cache et Amazon S3 ne sont pas synchronisés peut entraîner une perte de données. Par conséquent, nous vous déconseillons d'utiliser des lecteurs ou des disques éphémères.

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 de haute disponibilité.

Résolution des 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 lancer 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 Tape Gateway

Cette section contient les rubriques suivantes, qui fournissent des informations sur les meilleures pratiques relatives à l'utilisation des passerelles, des disques locaux, des instantanés 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 de passerelle.

Rubriques

- Bonnes pratiques : récupération de vos données
- Nettoyage des 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 restauration d'une machine virtuelle de passerelle à partir d'un instantané créé par votre hyperviseur ou de votre Amazon EC2 Amazon Machine Image (AMI). 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.

Rubriques

- Récupération après l'arrêt inattendu d'une machine virtuelle
- Récupération de vos données provenant d'une passerelle ou d'une machine virtuelle défaillante
- Récupération des données d'une bande irrécupérable
- Récupération des données d'un disque de cache défaillant

- Récupération de vos données à partir d'un centre de données inaccessible

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 votre connexion de passerelle à Internet.
- Pour les configurations de bandes, lorsque votre passerelle devient accessible, vos bandes prennent le statut AMORÇAGE. Cette fonctionnalité garantit que vos données stockées localement continuent d'être synchronisées avec AWS. Pour plus d'informations sur cet état, consultez Comprendre l'état de la bande.
- Si votre passerelle fonctionne mal et si des problèmes se produisent avec vos volumes ou bandes suite à un arrêt inattendu, vous pouvez récupérer vos données. Pour obtenir des informations sur la récupération de vos données, consultez les sections suivantes qui s'appliquent à votre scénario.

Récupération de vos données provenant d'une passerelle ou d'une machine virtuelle défaillante

Si votre passerelle de bande ou l'hôte hyperviseur rencontre une défaillance irrécupérable, vous pouvez mettre en œuvre les actions suivantes pour récupérer les bandes sur la passerelle de bande défectueuse et les transférer sur une autre passerelle de bande :

1. Identifiez la passerelle de bande à utiliser comme cible de récupération ou créez-en une nouvelle.
2. Désactivez la passerelle défaillante.
3. Créez des bandes de récupération pour chaque bande à récupérer et spécifiez la passerelle de bande cible.
4. Supprimez la passerelle de bande défaillante.

Pour obtenir des informations détaillées sur la récupération des bandes d'une passerelle de bande défaillante à transférer sur une autre passerelle de bande, consultez Vous avez besoin de récupérer une bande virtuelle à partir d'une passerelle de bande défaillante.

Récupération des données d'une bande irrécupérable

Si votre bande rencontre une défaillance et que son état est IRRECUPERABLE, nous vous recommandons d'utiliser l'une des options suivantes pour récupérer vos données ou résoudre la défaillance selon le cas de figure :

- Si vous avez besoin des données de la bande irrécupérable, vous pouvez récupérer la bande et la transférer sur une nouvelle passerelle.
- Si vous n'avez pas besoin des données de la bande et si celle-ci n'a jamais été archivée, vous pouvez simplement supprimer la bande de la passerelle de bande.

  Pour des informations détaillées sur la récupération de vos données ou la résolution d'une défaillance si votre bande est IRRECUPERABLE, consultez Résolution des problèmes de bandes irrécupérables.

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.
- Si le disque de cache est corrompu ou inaccessible, fermez la passerelle, réinitialisez le disque de cache, reconfigurez le disque pour le stockage de cache, puis redémarrez la passerelle.

Pour plus d'informations, consultez Vous avez besoin de récupérer une bande virtuelle à partir d'un disque de cache défectueux.

Récupération de vos données à partir d'un centre de données inaccessible

Si votre passerelle ou votre centre de données devient inaccessible pour une quelconque raison, vous pouvez récupérer vos données sur une autre passerelle dans un autre centre de données ou les récupérer sur une passerelle hébergée sur une EC2 instance Amazon. Si vous n'avez pas accès à un autre centre de données, nous vous recommandons de créer la passerelle sur une EC2

instance Amazon. 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 bande dans un centre de données inaccessible

1. Créez et activez une nouvelle Tape Gateway sur un EC2 hôte Amazon. Pour de plus amples informations, veuillez consulter Déployez une EC2 instance Amazon personnalisée pour Tape Gateway.
2. Restaurez les bandes de la passerelle source du centre de données vers la nouvelle passerelle que vous avez créée sur Amazon. EC2 Pour plus d'informations, consultezRécupération d'une bibliothèque de bandes virtuelles à partir d'une passerelle irrécupérable.

   Vos cassettes doivent être protégées jusqu'à la nouvelle EC2 passerelle Amazon.

Nettoyage des ressources inutiles

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

Si vous avez l'intention de continuer à utiliser votre passerelle de bande, consultez des informations supplémentaires dans Comment procéder ensuite ?

Pour nettoyer les ressources dont vous n'avez pas besoin

1. Supprimez les bandes de l'archive et de la bibliothèque de bandes virtuelles (VTL) de votre passerelle. Pour plus d'informations, consultez Suppression de votre passerelle et suppression des ressources associées.

   a. Archivez les bandes ayant l'état RECUPERE dans la VTL de la passerelle. Pour obtenir des instructions, consultez Archivage des bandes.
   b. Supprimez les bandes restantes de la VTL de la passerelle. Pour obtenir des instructions, consultez Suppression de bandes virtuelles de votre Tape Gateway.
   c. Supprimez les bandes de l'archive. Pour obtenir des instructions, consultez Suppression de bandes virtuelles de votre Tape Gateway.
2. À que vous ne prévoyiez de poursuivre l'utilisation de la passerelle de bande, supprimez-la. Pour obtenir des instructions, consultez Suppression de votre passerelle et suppression des ressources associées.

3. Supprimez la machine virtuelle Storage Gateway de votre hôte sur site. Si vous avez créé votre passerelle sur une EC2 instance Amazon, mettez fin à l'instance.

Ressources Storage Gateway supplémentaires

Cette section décrit les AWS logiciels, outils et ressources tiers qui peuvent vous aider à configurer ou à gérer votre passerelle, ainsi que les quotas de Storage Gateway.

Rubriques

- Déploiement et configuration de l'hôte de la machine virtuelle de passerelle- Découvrez comment déployer et configurer un hôte de machine virtuelle pour votre passerelle.
- Utilisation des ressources de stockage Tape Gateway- Découvrez les procédures relatives aux ressources de stockage Tape Gateway, telles que le retrait de disques locaux, la gestion des volumes Amazon EBS, l'utilisation de périphériques de bibliothèque de bandes virtuelles et la gestion des bandes de votre bibliothèque de bandes virtuelle.
- Obtention d'une clé d'activation pour votre passerelle- Découvrez où trouver la clé d'activation que vous devez fournir lorsque vous déployez une nouvelle passerelle.
- Connexion aux initiateurs iSCSI- Apprenez à travailler avec des volumes ou des périphériques VTL (Virtual Tape Library) exposés en tant que cibles iSCSI (Internet Small Computer System Interface).
- Utilisation AWS Direct Connect avec Storage Gateway- Découvrez comment créer une connexion réseau dédiée entre votre passerelle sur site et le AWS cloud.
- 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 de Storage Gateway IDs- Découvrez comment AWS identifier les ressources et les sous-ressources créées par Storage Gateway.
- Balisage des ressources Storage Gateway- Apprenez à utiliser les balises de métadonnées pour classer vos ressources et en faciliter la gestion.
- Utilisation de composants open source pour Storage Gateway- Découvrez les outils et licences tiers utilisés pour fournir les fonctionnalités de Storage Gateway.
- AWS Storage Gateway quotas- Découvrez les limites et les quotas de Tape Gateway, y compris les limites maximales relatives à la taille et à la quantité de bande, ainsi que les recommandations relatives à la taille des disques locaux.

Déploiement et configuration de l'hôte de la machine virtuelle de passerelle

Les rubriques de cette section décrivent comment configurer et gérer l'hôte de la machine virtuelle pour votre appliance Storage Gateway, y compris les appliances sur site exécutées sur VMware Hyper-V ou Linux KVM, et les appliances exécutées sur des EC2 instances Amazon dans le cloud. AWS

Rubriques

- Déployer un EC2 hôte Amazon par défaut pour Tape Gateway- Découvrez comment déployer et activer une passerelle de sur une instance Amazon Elastic Compute Cloud (Amazon EC2) en utilisant les spécifications par défaut.
- Déployez une EC2 instance Amazon personnalisée pour Tape Gateway- Découvrez comment déployer et activer une passerelle de sur une instance Amazon Elastic Compute Cloud (Amazon EC2) à l'aide de paramètres personnalisés.
- Modifier les options de métadonnées de l' EC2 instance Amazon- Découvrez comment configurer votre instance Amazon EC2 Gateway pour accepter les demandes de métadonnées entrantes qui utilisent la version 1 de l'IMDS (IMDSv1) ou pour exiger que toutes les demandes de métadonnées utilisent la version 2 de l'IMDS (IMDSv2).
- Synchroniser l'heure de la machine virtuelle avec l'heure de l'hôte KVM Hyper-V ou Linux- Découvrez comment afficher et synchroniser l'heure d'une machine virtuelle de passerelle KVM Hyper-V ou Linux sur site avec un serveur NTP (Network Time Protocol).
- Synchroniser l'heure de la machine virtuelle avec VMware celle de l'hôte- Découvrez comment vérifier l'heure d'hôte d'une machine virtuelle VMware passerelle et, si nécessaire, régler l'heure et configurer l'hôte pour qu'il synchronise automatiquement son heure avec un serveur NTP (Network Time Protocol).
- Configuration de la paravirtualisation sur un hôte VMware - Découvrez comment configurer la plate-forme VMware hôte de votre appliance Storage Gateway afin d'utiliser des contrôleurs iSCSI (Internet Small Computer System Interface Protocol) paravirtuels.
- Configuration des adaptateurs réseau pour votre passerelle- Découvrez comment reconfigurer votre passerelle pour utiliser l'adaptateur réseau VMXNET3 (10 GbE) ou pour utiliser plusieurs adaptateurs réseau afin qu'elle soit accessible à partir de plusieurs adresses IP.
- Utilisation de VMware vSphere High Availability avec Storage Gateway- Découvrez comment protéger vos charges de travail de stockage contre les pannes matérielles, d'hyperviseurs ou

de réseau en configurant Storage Gateway pour qu'il fonctionne avec VMware vSphere High Availability.

Déployer un EC2 hôte Amazon par défaut pour Tape Gateway

Cette rubrique décrit les étapes à suivre pour déployer un EC2 hôte Amazon en utilisant les spécifications par défaut.

Vous pouvez déployer et activer une passerelle de sur une instance Amazon Elastic Compute Cloud (Amazon EC2). L'Amazon Machine Image (AMI) de AWS Storage Gateway est disponible en tant qu'AMI de 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 Amazon EC2instance, 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' EC2 instance Amazon, consultez Déploiement d'une EC2 instance Amazon pour héberger votre passerelle de bande .
2. Sélectionnez Launch instance pour ouvrir le modèle d'AMI AWS Storage Gateway dans la EC2 console Amazon 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 EC2 instance Amazon avec la configuration par défaut.

   L' EC2 instance Amazon créée par Use default settings possède les spécifications par défaut suivantes :

   - Type d'instance : m5.xlarge
   - Paramètres réseau
     - Pour le VPC, sélectionnez le VPC dans lequel vous souhaitez exécuter votre EC2 instance.
     - Pour Sous-réseau, spécifiez le sous-réseau dans lequel votre EC2 instance doit être lancée.

> **Note**
>
> Les sous-réseaux VPC apparaîtront dans le menu déroulant uniquement si le paramètre d'attribution automatique des IPv4 adresses publiques est activé depuis la console de gestion VPC.

- Attribuer automatiquement une adresse IP publique : Activé

Un groupe EC2 de sécurité est créé et associé à l' EC2 instance. 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 EC2 instance ne sera accessible que via les autres ports depuis le VPC sélectionné.
> Les cibles iSCSI de votre passerelle ne sont accessibles qu'à partir des hôtes du même VPC que la passerelle. Si les cibles iSCSI 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' EC2instance Amazon, en sélectionnant Sécurité, en 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				
3260	TCP	iSCSI				

- Configurer le stockage

Paramètres par défaut	Volume racine de l'AMI	Cache du volume 2	Cache du volume 3			
Nom du périphérique		'/dev/sdb'	'/dev/sdb'			
Size	80 Gio	165 Gio	150 Gio			
Type de volume	gp3	gp3	gp3			
IOPS	3000	3000	3000			
Supprimer à la résiliation	Oui	Oui	Oui			
Chiffré	Non	Non	Non			
Débit	125	125	125			

Déployez une EC2 instance Amazon personnalisée pour Tape Gateway

Vous pouvez déployer et activer une passerelle de 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.
> Tape 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-CLASSIC-2.9.0
```

Pour déployer une EC2 instance Amazon afin d'héberger votre Tape Gateway

1. Commencez à configurer une nouvelle passerelle à l'aide de la console Storage Gateway. Pour obtenir des instructions, consultez Configuration d'une passerelle de bande. 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' EC2 instance Amazon qui hébergera votre Tape Gateway .
2. Choisissez Launch instance pour ouvrir le modèle d' AWS Storage Gateway AMI dans la EC2 console Amazon, où vous pouvez configurer des paramètres supplémentaires.

   Utilisez Quicklaunch pour lancer l' EC2 instance Amazon 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 Nom, entrez le nom de l' EC2 instance Amazon. Une fois l'instance déployée, vous pouvez rechercher ce nom pour trouver votre instance sur les pages de liste de la EC2 console Amazon.
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 plus d'informations, consultez Exigences relatives aux types d' EC2 instances Amazon.

   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' EC2 utilisateur Amazon.

   > **Note**
   >
   > Certains types d'instances, notamment i3 EC2, utilisent des disques NVMe SSD. Ceux-ci peuvent entraîner des problèmes lorsque vous démarrez ou arrêtez une passerelle de bande. Vous pouvez, par exemple, 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 le 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 EC2 instance Amazon 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 une passerelle de bande , consultez Exigences relatives 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**
>
> La passerelle de bande nécessite que le port TCP 80 soit ouvert pour le trafic entrant et pour un accès HTTP unique lors de l'activation de la passerelle. Après activation, vous pouvez fermer ce port.
> De plus, vous devez ouvrir le port TCP 3260 pour l'accès iSCSI.

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 165 Gio pour le stockage en cache, et au moins un volume Amazon EBS d'une capacité d'au moins 150 Gio pour la mémoire tampon de téléchargement, 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 Launch instance pour lancer votre nouvelle instance Amazon EC2 Gateway avec les paramètres configurés.
13. Pour vérifier que votre nouvelle instance a été lancée avec succès, accédez à la page Instances de la EC2 console Amazon 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' IPv4adresse publique depuis la section Récapitulatif de l'instance, puis revenez à la page Set up gateway de la console Storage Gateway pour reprendre la configuration de votre Tape Gateway .

Vous pouvez déterminer l'ID AMI à utiliser pour lancer une passerelle de Tape Gateway 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 Configuration d'une passerelle de bande. Lorsque vous atteignez la section des 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 EC2 console Amazon.

Vous êtes redirigé vers la page AMI de la EC2 communauté, 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/VTL/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/VTL/
latest
```

La commande de l'interface de ligne de commande renvoie un résultat semblable à ce qui suit :

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/VTL/
latest",
        "Name": "/aws/service/storagegateway/ami/VTL/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Modifier les options de métadonnées de l' EC2 instance Amazon

Le service de métadonnées d'instance (IMDS) est un composant sur instance qui fournit un accès sécurisé aux métadonnées des EC2 instances Amazon. 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'en avoir besoin IMDSv2 pour toutes les EC2 instances Amazon 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 de la paravirtualisation sur un hôte VMware

La procédure suivante décrit comment configurer la plate-forme VMware hôte de votre appliance Storage Gateway afin qu'elle utilise des contrôleurs iSCSI (Internet Small Computer System Interface Protocol) paravirtuels. Les contrôleurs iSCSI paravirtuels sont des contrôleurs de stockage hautes performances qui peuvent améliorer le débit et réduire l'utilisation du processeur. Ces contrôleurs sont parfaitement adaptés aux environnements de stockage à hautes performances. Lorsque vous configurez les contrôleurs iSCSI de cette façon, la machine virtuelle Storage Gateway fonctionne avec le système d'exploitation hôte pour permettre à la console de passerelle d'identifier les disques virtuels que vous ajoutez à votre machine virtuelle.

> **Note**
>
> Vous devez effectuer cette étape pour éviter les problèmes liés à l'identification de ces disques lorsque vous les configurez dans la console de passerelle.

Pour configurer votre plate-forme VMware hôte afin d'utiliser des contrôleurs paravirtualisés

1. Dans le client VMware vSphere, cliquez avec le bouton droit sur le nom de votre machine virtuelle de passerelle dans le volet de navigation situé sur le côté gauche de la fenêtre de l'application pour ouvrir le menu contextuel, puis choisissez Modifier les paramètres.
2. Dans la boîte de dialogue Propriétés de la machine virtuelle, choisissez l'onglet Matériel.
3. Dans l'onglet Matériel, sélectionnez Contrôleur SCSI 0, puis Change Type.
4. Dans la boîte de dialogue Modifier le type de contrôleur SCSI, sélectionnez le type de contrôleur VMware SCSI paravirtuel, puis cliquez sur OK pour enregistrer la configuration.

Configuration des adaptateurs réseau pour votre passerelle

Par défaut, Storage Gateway est configuré pour utiliser le type d'adaptateur réseau E1000, mais vous pouvez reconfigurer votre passerelle pour utiliser l'adaptateur réseau VMXNET3 (10 GbE). Vous pouvez également configurer Storage Gateway de façon à ce que plusieurs adresses IP puissent y accéder. Pour cela, configurez votre passerelle de façon à utiliser plusieurs cartes réseau.

Rubriques

- Configuration de votre passerelle pour utiliser l'adaptateur VMXNET3 réseau
- Configuration de votre passerelle pour plusieurs NICs

Configuration de votre passerelle pour utiliser l'adaptateur VMXNET3 réseau

Storage Gateway prend en charge le type d'adaptateur réseau E1000 à la fois sur les hôtes hyperviseurs Microsoft Hyper-V VMware ESXi et sur les hôtes. Toutefois, le type d'adaptateur réseau VMXNET3 (10 GbE) n'est pris en charge que dans VMware ESXi l'hyperviseur. Si votre passerelle est hébergée sur un VMware ESXi hyperviseur, vous pouvez la reconfigurer pour utiliser le type d'adaptateur VMXNET3 (10 GbE). Pour plus d'informations sur ces adaptateurs, voir Choisir un adaptateur réseau pour votre machine virtuelle sur le site Web de Broadcom (VMware).

> **Important**
>
> Pour effectuer une sélection VMXNET3, le type de système d'exploitation client doit être Autre Linux64.

Voici les étapes à suivre pour configurer votre passerelle afin qu'elle utilise l' VMXNET3adaptateur :

1. Supprimez la carte E1000 par défaut.
2. Ajoutez l' VMXNET3 adaptateur.
3. Redémarrez la passerelle.
4. Configurez la carte pour le réseau.

Voici des détails sur chaque étape.

Pour supprimer l'adaptateur E1000 par défaut et configurer votre passerelle pour qu'elle utilise l'VMXNET3 adaptateur

1. Dans VMware, ouvrez le menu contextuel (clic droit) de votre passerelle et choisissez Modifier les paramètres.
2. Dans la fenêtre Propriétés de la machine virtuelle, choisissez l'onglet Matériel.
3. Pour Matériel, choisissez Carte réseau. Notez que la carte actuelle est E1000 dans la section Type de carte. Vous allez remplacer cet adaptateur par l' VMXNET3 adaptateur.
4. Sélectionnez la carte réseau E1000, puis choisissez Supprimer. Dans cet exemple, la carte réseau E1000 est Carte réseau 1.

   > **Note**
   >
   > Bien que vous puissiez exécuter le E1000 et les adaptateurs VMXNET3 réseau sur votre passerelle en même temps, nous vous déconseillons de le faire car cela peut entraîner des problèmes de réseau.

5. Choisissez Ajouter pour ouvrir l'assistant Ajouter du matériel.
6. Choisissez Carte Ethernet, puis sélectionnez Suivant.
7. Dans l'assistant Type de réseau, sélectionnez **VMXNET3** pour Type de carte, puis choisissez Suivant.

8. Dans l'assistant des propriétés de la machine virtuelle, vérifiez dans la section Type d'adaptateur que l'adaptateur actuel est défini sur VMXNET3, puis cliquez sur OK.
9. Dans le VMware VSphere client, arrêtez votre passerelle.
10. Dans le VMware VSphere client, redémarrez votre passerelle.

Après le redémarrage de votre passerelle, reconfigurez la carte que vous venez d'ajouter pour vous assurer que la connectivité réseau à Internet est établie.

Pour configurer la carte pour le réseau

1. Dans le VSphere client, choisissez l'onglet Console pour démarrer la console locale. Utilisez les informations d'identification de connexion par défaut pour vous connecter à la console locale de la passerelle pour cette tâche de configuration. Pour obtenir des informations sur la façon de se connecter à l'aide des informations d'identification par défaut, consultez Connexion à la console locale à l'aide des informations d'identification par défaut.
2. À l'invite, entrez le chiffre correspondant pour sélectionner Configuration réseau.
3. A l'invite, entrez le chiffre correspondant pour sélectionner pour sélectionner Tout réinitialiser sur DHCP, puis entrez **y** (pour confirmer) à l'invite pour que toutes les cartes utilisent le protocole de configuration d'hôte dynamique (DHCP). Toutes les cartes disponibles sont définies pour utiliser le protocole DHCP.

   Si votre passerelle a déjà été activée, vous devez l'arrêter et la redémarrer à partir de la console de gestion Storage Gateway. Après le redémarrage de la passerelle, vous devez tester la connectivité réseau à Internet. Pour obtenir des informations sur la façon de tester la connectivité réseau, consultez Test de votre connexion passerelle à Internet.

Configuration de votre passerelle pour plusieurs NICs

Si vous configurez votre passerelle pour utiliser plusieurs adaptateurs réseau (NICs), plusieurs adresses IP peuvent y accéder. Cela peut être utile dans les cas suivants :

- Optimisation du débit : vous pouvez optimiser le débit vers une passerelle lorsque les cartes réseau sont 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 de réseau : l'environnement de l'application peut nécessiter que vous conserviez les cibles iSCSI et les initiateurs qui se connectent à elles dans un réseau isolé 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). A l'exception de cette carte, les initiateurs doivent être dans le même sous-réseau que la carte qui contient les cibles iSCSI à laquelle 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 iSCSI pour cette cible et le AWS trafic passeront par le même adaptateur.

Lorsque vous configurez une carte pour qu'elle se connecte à la console Storage Gateway, puis que vous ajoutez une deuxième carte, Storage Gateway configure automatiquement la table de routage pour qu'elle utilise la deuxième carte comme route préférée. Pour obtenir des instructions sur la façon de configurer plusieurs cartes, consultez les sections suivantes.

- Configuration de plusieurs adaptateurs réseau sur un VMware ESXi hôte
- Configuration de plusieurs adaptateurs réseau sur un hôte Microsoft Hyper-V

Configuration de plusieurs adaptateurs réseau 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 VMwareESXi.

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 des tâches sur la console locale de machine virtuelle

Configuration de plusieurs adaptateurs réseau sur un hôte Microsoft Hyper-V

La procédure suivante suppose que l'ordinateur virtuel de la passerelle a déjà une carte réseau définie et que vous ajoutez une deuxième carte. Cette procédure montre comment ajouter une carte pour un hôte Microsoft Hyper-V.

Pour configurer votre passerelle afin d'utiliser une carte réseau supplémentaire dans un hôte Microsoft Hyper-V

1. 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 des tâches sur la console locale de 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.

vSphere HA fonctionne en regroupant les machines virtuelles et les hôtes sur lesquels elles résident dans un cluster à des fins de redondance. Les hôtes du cluster sont surveillés et en cas de panne, les machines virtuelles d'un hôte défaillant sont redémarrées sur d'autres hôtes. Généralement, cette

restauration s'effectue rapidement et sans perte de données. Pour plus d'informations sur vSphere HA, consultez la section Fonctionnement de vSphere HA dans la documentation. VMware

> **Note**
>
> Le temps nécessaire pour redémarrer une machine virtuelle défaillante et rétablir la connexion iSCSI sur un nouvel hôte dépend de nombreux facteurs, tels que le système d'exploitation hôte et la charge des ressources, la vitesse du disque, la connexion réseau et l'infrastructure SAN/stockage. Pour minimiser les temps d'arrêt liés au basculement, mettez en œuvre les recommandations décrites dans de la passerelle.
> Pour utiliser Storage Gateway avec VMware HA, nous vous recommandons de procéder comme suit :
>
> - Déployez le package `.ova` téléchargeable VMware ESX qui contient la machine virtuelle Storage Gateway sur un seul hôte d'un cluster.
> - Lors du déploiement du package `.ova`, sélectionnez une banque de données qui ne soit pas locale pour un hôte. Utilisez plutôt une banque de données accessible à tous les hôtes du cluster. Si vous sélectionnez une banque de données locale pour un hôte et que ce dernier connaît une défaillance, la source de données risque de ne pas être accessible à d'autres hôtes du cluster et il est possible que le basculement vers un autre hôte échoue.
> - Pour éviter que l'initiateur se déconnecte des cibles de volumes de stockage au cours du basculement, suivez les paramètres iSCSI recommandés pour votre système d'exploitation. En cas de basculement, un ordinateur virtuel de passerelle peut mettre de quelques secondes à plusieurs minutes pour se lancer sur un nouvel hôte du cluster de basculement. Les délais d'attente iSCSI recommandés pour les clients Windows et Linux sont supérieurs à la durée classique d'un basculement. Pour plus d'informations sur la personnalisation des paramètres de délai d'attente des clients Windows, consultez Personnalisation des paramètres iSCSI Windows. Pour plus d'informations sur la personnalisation des paramètres de délai d'attente des clients Linux, consultez Personnalisation de vos paramètres iSCSI Linux.
> - Avec les clusters, si vous déployez le package `.ova` sur le cluster, sélectionnez un hôte lorsque vous êtes invité à le faire. Vous pouvez aussi déployer directement sur l'hôte d'un cluster.

Les rubriques suivantes décrivent comment déployer Storage Gateway dans un cluster VMware HA :

Rubriques

- Configuration de votre cluster vSphere HA VMware
- Téléchargez l'image .ova depuis la console Storage Gateway
- 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 à l'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.

Téléchargez l'image .ova depuis la console Storage Gateway

Pour télécharger l'image .ova pour votre passerelle

- Sur la page Configurer la passerelle de la console Storage Gateway, sélectionnez le type de passerelle et la plateforme hôte, puis utilisez le lien fourni dans la console pour télécharger le fichier .ova, comme indiqué dans Configurer une passerelle de bande.

Déployer la passerelle

Dans votre cluster configuré, déployez l'image .ova sur l'un des hôtes du cluster.

Pour déployer l'image .ova de la passerelle

1. Déployez l'image .ova sur l'un des hôtes du cluster.
2. Assurez-vous que les magasins de données que vous choisissez pour le disque racine et le cache sont disponibles pour tous les hôtes du cluster. Lors du déploiement du fichier Storage

Gateway .ova dans un environnement VMware ou sur site, les disques sont décrits comme des disques SCSI paravirtualisés. La paravirtualisation est un mode où la machine virtuelle de passerelle fonctionne avec le système d'exploitation hôte pour que la console puisse identifier les disques virtuels que vous ajoutez à la machine virtuelle.

Pour configurer votre machine virtuelle afin d'utiliser les contrôleurs paravirtualisés

1. Dans le client VMware vSphere, ouvrez le menu contextuel (clic droit) de votre machine virtuelle de passerelle, puis choisissez Modifier les paramètres.
2. Dans la boîte de dialogue Propriétés de la machine virtuelle, choisissez l'onglet Matériel, puis sélectionnez le Contrôleur SCSI 0 et choisissez Modifier le type.
3. Dans la boîte de dialogue Modifier le type de contrôleur SCSI, sélectionnez le type de contrôleur SCSI VMware paravirtuel, puis cliquez sur OK.

(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 .ova de votre passerelle déployé, activez votre passerelle. Les instructions sur la façon de procéder sont différentes pour chaque type de passerelle.

Pour activer la passerelle

- Suivez les procédures décrites dans les rubriques suivantes :

  a. Connectez votre Tape Gateway à AWS
  b. Vérifier les paramètres et activer votre passerelle de bande
  c. Configurer votre passerelle de bande

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 trouverez des informations sur les événements VMware HA dans les groupes de CloudWatch journaux Amazon. Pour plus d'informations, voir Getting Tape Gateway Health Logs with CloudWatch Log Groups .

Utilisation des ressources de stockage Tape Gateway

Les rubriques de cette section décrivent comment gérer les ressources de stockage associées à votre passerelle de bandes, telles que les disques physiques connectés à la plate-forme hôte virtuelle d'une passerelle, les volumes Amazon EBS attachés à l' EC2 instance Amazon d'une passerelle, les périphériques de votre bibliothèque de bandes virtuelles tels que les changeurs de support et les bandes de vos librairies de bandes virtuelles.

Rubriques

- Suppression de disques de votre passerelle- Découvrez ce qu'il convient de faire si vous devez supprimer un disque de la plate-forme hôte virtuelle de votre passerelle, par exemple en cas de défaillance d'un disque.
- Gestion des volumes Amazon EBS sur les passerelles Amazon EC2- Découvrez comment augmenter ou réduire la quantité de volumes Amazon EBS alloués pour être utilisés comme mémoire tampon de téléchargement ou stockage de cache pour une passerelle hébergée sur une instance Amazon EC2.
- Utilisation des dispositifs VTL- Découvrez comment gérer les périphériques de votre bibliothèque de bandes virtuelle, notamment comment sélectionner un changeur de support pour une passerelle de bande, comment mettre à jour le pilote du périphérique pour un changeur de support et comment afficher les codes-barres pour les bandes dans Microsoft System Center Data Protection Manager.
- Gestion des bandes dans votre bibliothèque de bandes virtuelle- Découvrez comment gérer les bandes et les librairies de bandes virtuelles associées à votre Tape Gateway, notamment comment archiver manuellement les bandes et annuler l'archivage des bandes en cours.

Suppression de disques de votre passerelle

Même si nous ne recommandons pas de supprimer les disques sous-jacents de votre passerelle, vous pouvez avoir besoin d’effectuer cette opération, par exemple lorsqu’un disque est défaillant.

Suppression d'un disque d'une passerelle hébergée sur VMware ESXi

Vous pouvez utiliser la procédure suivante pour supprimer un disque de votre passerelle hébergée sur un VMware hyperviseur.

Pour supprimer un disque alloué à la mémoire tampon de téléchargement (VMware ESXi)

1. Dans le client vSphere, ouvrez le menu contextuel (clic droit), choisissez le nom de la machine virtuelle de la passerelle, puis choisissez Modifier les paramètres.
2. Sur l’onglet Matériel de la boîte de dialogue Propriétés de la machine virtuelle, sélectionnez le disque alloué comme tampon de chargement, puis choisissez Supprimer.

   Vérifiez que la valeur Nœud de l’appareil virtuel dans la boîte de dialogue Propriétés de la machine virtuelle a la même valeur que celle notée précédemment. Vous veillerez ainsi à bien supprimer le bon disque.
3. Sélectionnez l’option appropriée dans le volet Options de suppression, puis choisissez OK pour terminer le processus de suppression du disque.

Suppression d’un disque d’une passerelle hébergée sur Microsoft Hyper-V

À l’aide de la procédure suivante, vous pouvez supprimer un disque de la passerelle hébergée sur un hyperviseur Microsoft Hyper-V.

Pour supprimer un disque sous-jacent alloué au tampon de chargement (Microsoft Hyper-V)

1. Dans Microsoft Hyper-V Manager, ouvrez le menu contextuel (clic droit), choisissez le nom de la machine virtuelle de la passerelle, puis sélectionnez Paramètres.
2. Dans la liste Matériel de la boîte de dialogue Paramètres, sélectionnez le disque à supprimer, puis choisissez Supprimer.

   Les disques que vous ajoutez à une passerelle apparaissent sous l’entrée Contrôleur SCSI de la liste Matériel. Vérifiez que les valeurs des champs Contrôleur et Emplacement sont identiques à celles que vous aviez notées. Vous veillerez ainsi à bien supprimer le bon disque.

Le premier contrôleur SCSI affiché dans le gestionnaire Microsoft Hyper-V est contrôleur 0.

3. Choisissez OK pour appliquer la modification.

Suppression d'un disque d'une passerelle hébergée sur KVM Linux

Pour détacher un disque de votre passerelle hébergée sur l'hyperviseur KVM (machine virtuelle basée sur le noyau Linux), vous pouvez utiliser une commande `virsh` similaire à la suivante.

```
$ virsh detach-disk domain_name /device/path
```

Pour plus d'informations sur la gestion des disques KVM, consultez la documentation de votre distribution Linux.

Gestion des volumes Amazon EBS sur les passerelles Amazon EC2

Lorsque vous avez initialement configuré votre passerelle pour qu'elle s'exécute en tant qu' EC2 instance Amazon, vous avez alloué des volumes Amazon EBS à utiliser comme tampon de téléchargement et stockage de cache. Au fil du temps, lorsque vos applications ont besoin d'évoluer, vous pouvez allouer des volumes Amazon EBS supplémentaires à cet effet. Vous pouvez également réduire le stockage que vous avez alloué en supprimant les volumes Amazon EBS alloués auparavant. Pour plus d'informations sur Amazon EBS, consultez Amazon Elastic Block Store (Amazon EBS) dans le guide de l'utilisateur Amazon. EC2

Avant d'ajouter du stockage à la passerelle, réfléchissez à la façon dont vous souhaitez dimensionner le stockage de tampon de chargement et de cache en fonction des besoins de votre application. Pour cela, consultez les pages Détermination de la taille de tampon de chargement à allouer et Détermination de la taille du stockage de cache à allouer.

Vous devez respecter des quotas de stockage maximum susceptible d'être alloué en tant que stockage de tampon de chargement et de cache. Vous pouvez attacher autant de volumes Amazon EBS à votre instance que vous le souhaitez, mais vous pouvez uniquement configurer ces volumes comme espace de stockage de tampon de chargement et de cache conformément à ces quotas de stockage. Pour plus d'informations, consultez AWS Storage Gateway quotas.

Pour ajouter un volume Amazon EBS et le configurer pour votre passerelle

1. Créez un volume Amazon EBS. Pour obtenir des instructions, consultez la section Création ou restauration d'un volume Amazon EBS dans le guide de l' EC2 utilisateur Amazon.

2. Attachez le volume Amazon EBS à votre EC2 instance Amazon. Pour obtenir des instructions, consultez la section Attacher un volume Amazon EBS à une instance dans le guide de l' EC2 utilisateur Amazon.
3. Configurez le volume Amazon EBS que vous avez ajouté comme tampon de chargement ou stockage de cache. Pour obtenir des instructions, consultez Gestion des disques locaux pour Storage Gateway.

Dans certains cas, vous découvrirez que vous n'avez pas besoin de tout le stockage alloué au tampon de chargement.

Pour supprimer un volume Amazon EBS

> **Warning**
>
> Ces étapes s'appliquent uniquement aux volumes Amazon EBS alloués comme espace de tampon de chargement et non aux volumes alloués au cache. Si vous supprimez un volume Amazon EBS alloué comme stockage de cache à partir d'une passerelle de bande, les bandes virtuelles de la passerelle auront le statut IRRÉCUPÉRABLE et vous risquez de perdre des données. Pour plus d'informations sur le statut IRRÉCUPÉRABLE, consultez Comprendre les informations sur l'état d'une bande dans une VTL.

1. Arrêtez la passerelle en suivant l'approche décrite à la section Arrêt de la machine virtuelle de la passerelle.
2. Détachez le volume Amazon EBS de votre instance Amazon EC2 . Pour obtenir des instructions, consultez la section Détachement d'un volume Amazon EBS d'une instance dans le guide de EC2 l'utilisateur Amazon.
3. Supprimez le volume Amazon EBS. Pour obtenir des instructions, consultez Supprimer un volume Amazon EBS dans le guide de l' EC2 utilisateur Amazon.
4. Démarrez la passerelle en suivant l'approche décrite à la section Arrêt de la machine virtuelle de la passerelle.

Utilisation des dispositifs VTL

Lorsque vous activez votre Tape Gateway, vous sélectionnez votre application de sauvegarde dans la liste et vous utilisez le changeur de support approprié. Si votre application de sauvegarde n'est pas

répertoriée, choisissez Autre, puis sélectionnez le changeur de média compatible avec l'application de sauvegarde. Pour obtenir la liste des changeurs de média recommandés pour les applications de sauvegarde prises en charge, consultezhttps://docs.aws.amazon.com/storagegateway/latest/tgw/Requirements.html#requirements-backup-sw-for-vtl.

La configuration de votre passerelle de bande fournit les périphériques iSCSI suivants, que vous sélectionnez lors de l'activation de votre passerelle.

Changeurs de taille moyenne :

- AWS-Gateway-VTL : cet appareil est fourni avec la passerelle.
- STK-L700 : cette émulation d'appareil est fournie avec la passerelle.

Lecteurs de bande :

- IBM- ULT358 0- TD5 —Cette émulation de périphérique est fournie avec la passerelle.

Rubriques

- Sélection d'un changeur de média après l'activation de la passerelle
- Mise à jour le pilote d'appareil pour votre changeur de média
- Affichage des codes-barres pour les bandes dans Microsoft System Center DPM

Sélection d'un changeur de média après l'activation de la passerelle

Une fois la passerelle activée, vous pouvez opter pour un changeur de média différent.

Pour sélectionner un type de changeur de média différent après l'activation de la passerelle

1. Arrêtez tous les travaux connexes qui sont en cours d'exécution dans votre logiciel de sauvegarde.
2. Sur le serveur Windows, ouvrez la fenêtre de propriétés de l'initiateur iSCSI.
3. Choisissez l'onglet Cibles afin d'afficher les cibles découvertes.
4. Dans le volet Cibles découvertes, choisissez le changeur de média que vous voulez modifier, sélectionnez Se déconnecter, puis choisissez OK.
5. Dans la console Storage Gateway, sélectionnez Passerelles dans le volet de navigation, puis choisissez la passerelle pour laquelle vous souhaitez modifier le changeur de média.

6. Choisissez l'onglet Appareils VTL, sélectionnez le changeur de média que vous voulez modifier, puis choisissez Modifier le changeur de média.
7. Dans la boîte de dialogue Modifier le type de changeur de média qui s'affiche, sélectionnez un changeur de média dans la liste déroulante, puis choisissez Enregistrer.

Mise à jour le pilote d'appareil pour votre changeur de média

1. Ouvrez le gestionnaire d'appareils sur votre serveur Windows et développez l'arborescence Appareils du changeur de média.
2. Ouvrir le menu contextuel (clic droit) pour Changeur de média inconnu, puis choisissez Mettre à jour le logiciel de pilote pour ouvrir la fenêtre Mettre à jour le changeur de média du logiciel de pilote.
3. Dans la section Comment voulez-vous rechercher le pilote ?, choisissez Rechercher un pilote sur mon ordinateur.
4. Choisissez Me laisser choisir parmi une liste de pilotes d'appareils sur mon ordinateur.

   > **Note**
   >
   > Nous vous recommandons d'utiliser le pilote Sony TSL-A500C Autoloader avec les logiciels de sauvegarde Veeam Backup & Replication 11A et Microsoft System Center Data Protection Manager. Ce pilote Sony a été testé avec ces types de logiciels de sauvegarde jusqu'à Windows Server 2019 inclus.

5. Dans la section Sélectionner le pilote d'appareil que vous souhaitez installer pour ce matériel, désactivez la case à cocher Afficher le matériel compatible, choisissez Sony dans la liste Fabricant, choisissez Sony - TSL-A500C Autoloader dans la liste Modèle, puis sélectionnez Suivant.
6. Dans la zone d'avertissement qui s'affiche, cliquez sur Oui. Si le pilote est installé avec succès, fermez la fenêtre Mettre à jour le logiciel du lecteur.

Affichage des codes-barres pour les bandes dans Microsoft System Center DPM

Si vous utilisez le pilote de changeur de média pour le Sony TSL-A500C Autoloader, Microsoft System Center Data Protection Manager n'affiche pas automatiquement les codes-barres pour les bandes virtuelles créées dans Storage Gateway. Pour afficher correctement les codes-barres de vos cassettes, remplacez le pilote du changeur de média par Sun/ LibraryStorageTek .

Pour afficher les codes-barres

1. Assurez-vous que toutes les tâches de sauvegarde sont terminées et qu'aucune tâche n'est en attente ou en cours.
2. Éjectez et déplacez les bandes vers le stockage hors connexion (S3 Glacier Flexible Retrieval or S3 Glacier Deep Archive) et quittez la console Administrateur DPM. Pour obtenir des informations sur l'éjection d'une bande dans DPM, consultez Archivage d'une bande à l'aide de DPM.
3. Dans Outils d'administration, choisissez Services et ouvrez le menu contextuel (clic droit) de Service DPM dans le volet Détails, puis choisissez Propriétés.
4. Dans l'onglet Général, assurez-vous que le Type de démarrage est défini sur Automatique et choisissez Arrêter pour arrêter le service DPM.
5. Obtenez les StorageTek pilotes à partir du catalogue Microsoft Update sur le site Web de Microsoft.

   > **Note**
   >
   > Vous remarquerez que différents pilotes sont proposés pour les différentes tailles.

   Pour la Taille 18K, choisissez les pilotes x86.

   Pour la Taille 19K, choisissez les pilotes x64.
6. Sur votre serveur Windows, ouvrez le gestionnaire de périphériques et développez l'arborescence Changeurs de média.
7. Ouvrir le menu contextuel (clic droit) pour Changeur de média inconnu, puis choisissez Mettre à jour le logiciel de pilote pour ouvrir la fenêtre Mettre à jour le changeur de média du logiciel de pilote.
8. Suivez le chemin d'accès vers l'emplacement du nouveau pilote, puis installez-le. Le pilote apparaît sous le nom Sun/ StorageTek Library. Les lecteurs de bande restent sous la forme d'un périphérique séquentiel IBM ULT358 TD5 0-SCSI.
9. Redémarrez le serveur DPM.
10. Dans la console Storage Gateway, créez des bandes.

11. Ouvrez la console administrateur DPM, choisissez Management (Gestion), puis choisissez Rescan for new tape libraries (Effectuer une nouvelle recherche de bibliothèques de bandes). Vous devriez voir le Sun/ la StorageTek bibliothèque.
12. Choisissez la bibliothèque, puis Inventory (Inventaire).
13. Choisissez Add Tapes (Ajouter des bandes) pour ajouter les nouvelles bandes dans DPM. Les nouvelles bandes devraient maintenant afficher leur code-barres.

Gestion des bandes dans votre bibliothèque de bandes virtuelle

Votre passerelle de bande fournit une bibliothèque de bandes virtuelles (VTL) pour chaque passerelle que vous activez. A l'origine, la bibliothèque ne contient aucune bande, mais vous pouvez créer des bandes chaque fois que vous en avez besoin. Votre application peut lire et écrire sur n'importe quelle bande disponible sur votre passerelle de bande. Le statut de la bande doit être DISPONIBLE pour que vous puissiez écrire dessus. Ces bandes sont prise en charge par Amazon Simple Storage Service (Amazon S3), c'est-à-dire que, lorsque vous écrivez sur ces bandes, la passerelle de bande stocke les données dans Amazon S3. Pour plus d'informations, consultez Comprendre les informations sur l'état d'une bande dans une VTL.

Rubriques

- Archivage des bandes
- Annulation de l'archivage d'une bande

La bibliothèque de bandes affiche les bandes dans votre passerelle de bande. La bibliothèque contient le code barre, l'état et la taille de la bande, la quantité de bande utilisée, ainsi que la passerelle à laquelle celle-ci est associée.

Lorsque vous avez un grand nombre de bandes dans la bibliothèque, la console prend en charge la recherche de bandes par code à barres, par état ou les deux. Lorsque vous effectuez une recherche par code à barres, vous pouvez filtrer par état et passerelle.

Pour effectuer une recherche par code à barres, état et passerelle

1. Ouvrez la console Storage Gateway à la https://console.aws.amazon.com/storagegateway/maison.
2. Dans le volet de navigation, sélectionnez Bandes, puis tapez une valeur dans la zone de recherche. La valeur peut être le code à barres, l'état ou la passerelle. Par défaut, Storage

Gateway recherche dans toutes les bandes virtuelles. Cependant, vous pouvez également filtrer votre recherche par état.

Si vous filtrez par statut, les bandes qui correspondent à vos critères apparaissent dans la bibliothèque de la console Storage Gateway.

Si vous filtrez par passerelle, les bandes qui sont associées à cette passerelle apparaissent dans la bibliothèque de la console Storage Gateway.

> **Note**
>
> Par défaut, Storage Gateway affiche toutes les bandes quel que soit le statut.

Archivage des bandes

Vous pouvez archiver les bandes virtuelles qui se trouvent dans Storage Gateway. Lorsque vous archivez une bande, Storage Gateway la transfère vers l'archive.

Pour archiver une bande, vous utilisez votre logiciel de sauvegarde. Le processus d'archivage des bandes comprend trois étapes qui correspondent à leurs différents états : EN COURS D'ACHEMINEMENT A VTS, ARCHIVAGE et ARCHIVÉ.

- Pour archiver une bande, utilisez la commande fournie par votre application de sauvegarde. Lorsque le processus d'archivage commence, le statut de la bande passe à EN COURS D'ACHEMINEMENT A VTS. La bande n'est alors plus accessible par votre application de sauvegarde. À ce stade, votre Tape Gateway télécharge les données vers AWS. Si nécessaire, vous pouvez annuler l'archivage en cours. Pour plus d'informations sur l'annulation de l'archivage, consultez Annulation de l'archivage d'une bande.

  > **Note**
  >
  > Les étapes de l'archivage d'une bande dépendent de votre application de sauvegarde. Pour obtenir des instructions détaillées, consultez la documentation de votre application de sauvegarde.

- Une fois le téléchargement des données AWS terminé, le statut de la bande passe à ARCHIVING et Storage Gateway commence à déplacer la bande vers l'archive. Vous ne pouvez pas annuler le processus d'archivage à ce stade.

- Une fois que la bande est transférée vers l'archive, son état devient ARCHIVÉ. Vous pouvez alors la transférer vers l'une de vos passerelles. Pour plus d'informations sur l'extraction de la bande, consultez Récupération des bandes archivées.

Les étapes de l'archivage d'une bande dépendent de votre logiciel de sauvegarde. Pour obtenir des instructions sur l'archivage d'une bande à l'aide du NetBackup logiciel Symantec, reportez-vous à la section Archivage de la bande.

Annulation de l'archivage d'une bande

Une fois que vous avez commencé l'archivage d'une bande, vous pouvez décider que vous avez finalement besoin de cette bande. Par exemple, vous pouvez avoir besoin d'annuler le processus d'archivage et de récupérer la bande parce que le processus d'archivage est trop long ou parce que vous devez lire les données de la bande. Une bande qui est plus archivée passe par trois états, comme illustré ci-après :

- EN COURS D'ACHEMINEMENT À VTS : votre passerelle de bande charge les données sur AWS.
- ARCHIVAGE : le chargement des données est terminé et la passerelle de bande transfère la bande vers l'archive.
- ARCHIVÉ : la bande a été transférée et l'archive est disponible pour la récupération.

Vous pouvez annuler l'archivage uniquement lorsque le statut de la bande est EN COURS D'ACHEMINEMENT À VTS. Selon les critères, par exemple la bande passante de chargement et la quantité de données en cours de chargement, ce statut est visible ou masqué sur la console Storage Gateway. Pour annuler un archivage sur bande, utilisez l'CancelRetrievalaction indiquée dans la référence de l'API.

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 Storage Gateway, les modèles d'images de machine virtuelle et EC2 Amazon Amazon Machine Images (AMI) 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

L'exemple suivant vous montre 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. Si vous vous connectez à votre EC2 instance Amazon depuis un ordinateur Windows, connectez-vous 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 la AWS région dans laquelle 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.

Connexion aux initiateurs iSCSI

Lorsque vous gérez votre passerelle, vous utilisez des volumes ou des périphériques de la bibliothèque de bandes virtuelles (VTL) qui sont exposés en tant que cibles iSCSI (Internet Small Computer System Interface). Pour les passerelles de volume, les cibles iSCSI sont des volumes. Pour les passerelles de bande, les cibles sont des appareils VTL. Dans le cadre de ce travail, vous effectuez des tâches telles que la connexion à ces cibles, la personnalisation des paramètres iSCSI, la connexion d'un client Red Hat Linux et la configuration du protocole CHAP (Challenge-Handshake Authentication Protocol).

Rubriques

- Connexion de vos appareils VTL à un client Windows
- Connecter les appareils VTL de vos à un client Linux
- Personnalisation des paramètres iSCSI
- Configuration de l'authentification CHAP pour vos cibles iSCSI

La norme iSCSI est une norme de réseau de stockage basée sur le protocole Internet (IP) qui permet d'établir et de gérer les connexions entre les appareils de stockage basés sur l'IP et les clients. La liste suivante définit certains termes qui sont utilisés pour décrire la connexion iSCSI et les composants concernés.

Initiateur iSCSI

Le composant client d'un réseau iSCSI. L'initiateur envoie des demandes à la cible iSCSI. Les initiateurs peuvent être implémentés dans le logiciel ou le matériel. Storage Gateway prend uniquement en charge les initiateurs logiciels.

Cible iSCSI

Le composant serveur du réseau iSCSI qui reçoit et répond aux demandes des initiateurs. Chaque volume est exposé comme cible iSCSI. Connectez un seul initiateur iSCSI à chaque cible iSCSI.

Initiateur iSCSI Microsoft

Le programme logiciel sur les ordinateurs Microsoft Windows qui vous permet de connecter un ordinateur client (c'est-à-dire, l'ordinateur qui exécute l'application dont vous souhaitez écrire les données sur la passerelle) à un tableau externe basé sur iSCSI (c'est-à-dire, la passerelle). La connexion est effectuée à l'aide de la carte réseau Ethernet de l'ordinateur hôte. L'initiateur Microsoft iSCSI a été validé avec Storage Gateway sous Windows Server 2022. L'initiateur est intégré au système d'exploitation.

Initiateur iSCSI Red Hat

Le package RPM (Resource Package Manager) `iscsi-initiator-utils` vous fournit un initiateur iSCSI mis en œuvre dans le logiciel pour Red Hat Linux. Le package comprend un server démon pour le protocole iSCSI.

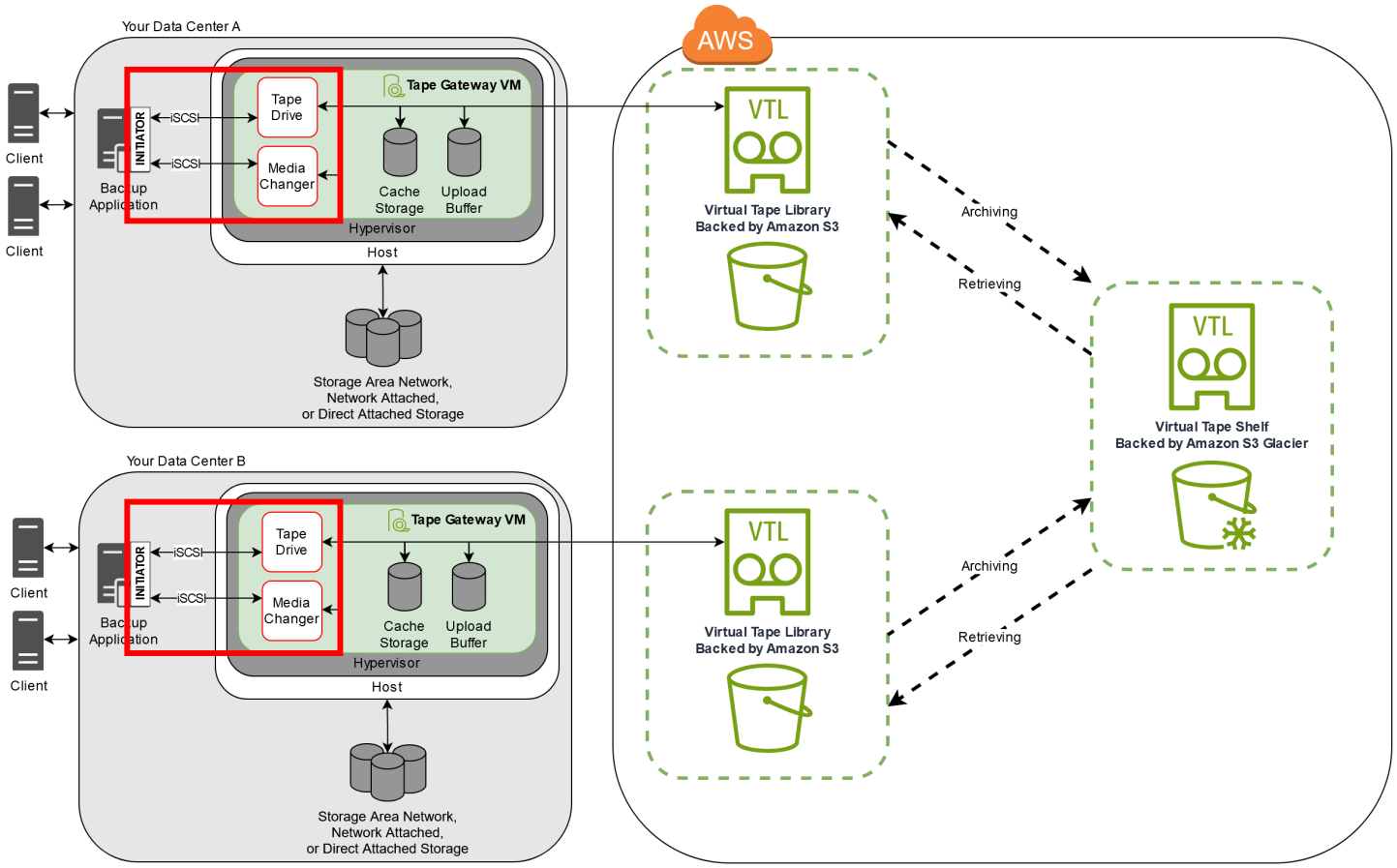
Chaque type de passerelle peut se connecter aux appareils iSCSI et vous pouvez personnaliser ces connexions, tel que décrit ci-après.

Connexion de vos appareils VTL à un client Windows

Une passerelle de bande expose plusieurs lecteurs de bandes et un changeur de média, nommés collectivement appareils VTL, en tant que cibles iSCSI. Pour plus d'informations, consultez Exigences relatives à la configuration de Tape Gateway.

> **Note**
>
> Vous connectez une seule application à chaque cible iSCSI.

Le diagramme suivant met en évidence la cible iSCSI dans le cadre de l'architecture Storage Gateway. Pour plus d'informations sur l'architecture Storage Gateway, consultez Fonctionnement de la passerelle de bande (architecture).



Pour connecter votre client Windows aux appareils VTL

1. Dans le menu Démarrer de votre ordinateur client Windows, entrez **`iscsicpl.exe`** dans la zone Rechercher les programmes et les fichiers, trouvez le programme d'initiateur iSCSI, puis exécutez-le.

   > **Note**
   >
   > Vous devez avoir des droits d'administrateur sur l'ordinateur client pour pouvoir exécuter l'initiateur iSCSI.

2. Si vous y êtes invité, choisissez Oui pour démarrer le service de l'initiateur Microsoft iSCSI.
3. Dans la boîte de dialogue iSCSI Initiator Properties (Propriétés de l'initiateur iSCSI), choisissez l'onglet Discovery (Découverte), puis sélectionnez Discover Portal (Découvrir le portail).

4. Dans la boîte de dialogue Détecter un portail cible, entrez l'adresse IP de votre passerelle de bande pour Adresse IP ou nom DNS, puis choisissez OK. Pour obtenir l'adresse IP de votre passerelle, consultez l'onglet Passerelle de la console Storage Gateway. Si vous avez déployé votre passerelle sur une EC2 instance Amazon, vous pouvez trouver l'adresse IP ou DNS publique dans l'onglet Description de la EC2 console Amazon.

   > **Warning**
   >
   > Pour les passerelles déployées sur une EC2 instance Amazon, l'accès à la passerelle via une connexion Internet publique n'est pas pris en charge. L'adresse IP élastique de l' EC2 instance Amazon ne peut pas être utilisée comme adresse cible.

5. Choisissez l'onglet Cibles, puis sélectionnez Actualiser. Les dix lecteurs de bandes et le changeur de média apparaissent dans la zone Cibles découvertes. L'état des cibles est Inactif.
6. Sélectionnez le premier appareil, puis choisissez Connecter. Vous connectez les appareils un à la fois.
7. Dans la boîte de dialogue Se connecter à la cible, choisissez OK.
8. Répétez les étapes 6 et 7 pour chacun des appareils afin de tous les connecter, puis choisissez OK dans la boîte de dialogue Propriétés de l'initiateur iSCSI.

Sur un client Windows, le fournisseur de pilotes pour le lecteur de bandes doit être Microsoft. Utilisez la procédure suivante pour vérifier le fournisseur de pilotes et mettez à jour le pilote et le fournisseur si nécessaire.

Pour vérifier le fournisseur de pilotes et (si besoin) mettre à jour le pilote et le fournisseur sur un client Windows

1. Sur le client Windows, démarrez le gestionnaire d'appareils.
2. Développez Lecteurs de bande, choisissez le menu contextuel (clic droit) d'un lecteur de bandes, puis sélectionnez Propriétés.
3. Dans l'onglet Pilote de la boîte de dialogue Propriétés de l'appareil, vérifiez que le Fournisseur de pilote est Microsoft.
4. Si le Fournisseur de pilote n'est pas Microsoft, définissez la valeur comme suit :

   a. Choisissez Mettre à jour le pilote.

b. Dans la boîte de dialogue Mettre à jour le pilote, choisissez Parcourir mon ordinateur pour rechercher le logiciel du pilote.

c. Dans la boîte de dialogue Mettre à jour le logiciel de pilote, sélectionnez Me laisser choisir parmi une liste de pilotes d'appareils sur mon ordinateur.

d. Sélectionnez Lecteur de bandes LTO, puis choisissez Suivant.

e. Choisissez Fermer pour fermer la fenêtre Mettre à jour le logiciel de pilote et vérifiez que la valeur du Fournisseur de pilote est maintenant définie sur Microsoft.

5. Répétez les étapes 4.1 à 4.5 pour mettre à jour tous les lecteurs de bandes.

Connecter les appareils VTL de vos à un client Linux

Lorsque vous utilisez Red Hat Enterprise Linux (RHEL), vous utilisez le package RPM `iscsi-initiator-utils` pour vous connecter aux cibles iSCSI de votre passerelle (volumes ou appareils VTL).

Pour connecter un client Linux aux cibles iSCSI

1. Installez le package RPM `iscsi-initiator-utils`, s'il n'est pas déjà installé sur le client.

   Vous pouvez utiliser la commande suivante pour installer le package.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. Veillez à ce que le démon iSCSI soit en cours d'exécution.

   a. Vérifiez que le démon iSCSI est en cours d'exécution à l'aide de l'une des commandes suivantes.

      Pour RHEL 8 ou 9, utilisez la commande suivante.

      ```
      sudo service iscsid status
      ```

   b. Si la commande de l'état ne renvoie pas l'état en cours d'exécution, démarrez le démon à l'aide de l'une des commandes suivantes.

      Pour RHEL 8 ou 9, utilisez la commande suivante. Il n'est généralement pas nécessaire de démarrer explicitement le `iscsid` service.

```
sudo service iscsid start
```

3. Pour découvrir le volume ou les cibles d'appareils VTL définis pour une passerelle, utilisez la commande de découverte suivante.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

Remplacez l'adresse IP de votre passerelle par la *[GATEWAY_IP]* variable de la commande précédente. Vous trouverez l'IP de la passerelle dans les propriétés Informations cibles iSCSI d'un volume sur la console Storage Gateway.

Le résultat de la commande de découverte ressemble à l'exemple de sortie suivant.

Pour les passerelles de volume : *[GATEWAY_IP]*`:3260, 1 iqn.1997-05.com.amazon:myvolume`

Pour les passerelles de bande : `iqn.1997-05.com.amazon:`*[GATEWAY_IP]*`-tapedrive-01`

Votre nom qualifié iSCSI (IQN) sera différent de celui qui est affiché précédemment, car les valeurs de nom qualifié sont propres à une organisation. Le nom de la cible est celui que vous avez spécifié lorsque vous avez créé le volume. Ce nom se trouve également dans le volet des propriétés Informations cibles iSCSI lorsque vous sélectionnez un volume sur la console Storage Gateway.

4. Pour vous connecter à une cible, utilisez la commande suivante.

Notez que vous devez spécifier le bon *[GATEWAY_IP]* IQN dans la commande connect.

> **Warning**
>
> Pour les passerelles déployées sur une EC2 instance Amazon, l'accès à la passerelle via une connexion Internet publique n'est pas pris en charge. L'adresse IP élastique de l' EC2 instance Amazon ne peut pas être utilisée comme adresse cible.

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. Pour vérifier que le volume est attaché à l'ordinateur client (l'initiateur), utilisez la commande suivante.

```
ls -l /dev/disk/by-path
```

Le résultat de la commande ressemble à l'exemple de sortie suivant.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

Une fois que vous avez configuré votre initiateur, nous vous recommandons vivement de personnaliser vos paramètres iSCSI comme indiqué dans Personnalisation de vos paramètres iSCSI Linux.

Personnalisation des paramètres iSCSI

Une fois que vous avez configuré l'initiateur, nous vous recommandons vivement de personnaliser vos paramètres iSCSI pour empêcher l'initiateur de se déconnecter des cibles.

En augmentant les valeurs de délai iSCSI comme illustré dans les étapes suivantes, vous permettez à votre application de mieux traiter les opérations d'écriture qui prennent beaucoup de temps et d'autres questions temporaires telles que les interruptions de réseau.

> **Note**
>
> Avant d'apporter des modifications au registre, vous devez créer une copie de sauvegarde du registre. Pour plus d'informations sur la création d'une copie de sauvegarde et sur les autres bonnes pratiques à suivre lors de l'utilisation du registre, consultez la section Meilleures pratiques du registre dans la Microsoft TechNet Library.

Rubriques

- Personnalisation des paramètres iSCSI Windows
- Personnalisation de vos paramètres iSCSI Linux

Personnalisation des paramètres iSCSI Windows

Pour la configuration d'une passerelle de bande, la connexion à vos appareils VTL à l'aide d'un initiateur iSCSI Microsoft est un processus en deux étapes :

1. Connectez les appareils de votre passerelle de bande à votre client Windows.
2. Si vous utilisez une application de sauvegarde, configurez-la de façon à utiliser ces appareils.

La configuration de l'exemple de mise en route fournit des instructions relatives à ces deux étapes. Il utilise l'application de NetBackup sauvegarde Symantec. Pour plus d'informations, consultez Connexion de vos appareils VTL et Configuration des périphériques NetBackup de stockage.

Pour personnaliser vos paramètres iSCSI Windows

1. Augmentez la durée maximale pendant laquelle les demandes sont mises en attente.

   a. Démarrez l'éditeur de registre (`Regedit.exe`).

   b. Accédez à la clé GUID pour la classe d'appareil qui contient les paramètres du contrôleur iSCSI, comme indiqué ci-après.

   > **Warning**
   >
   > Assurez-vous que vous travaillez dans la CurrentControlSetsous-clé et non dans un autre ensemble de contrôles, tel que ControlSet001 ou ControlSet002.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
   ```

   c. Recherchez la sous-clé de l'initiateur Microsoft iSCSI, illustrée ci-dessous sous la forme. *[<Instance Number]*

   La clé est représentée par un nombre à quatre chiffres, par exemple `0000`.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
   ```

En fonction de ce qui est installé sur votre ordinateur, l'initiateur iSCSI Microsoft ne peut pas être la sous-clé `0000`. Vous pouvez vous assurer que vous avez sélectionné la bonne sous-clé en vérifiant que la chaîne `DriverDesc` contient la valeur`Microsoft iSCSI Initiator`.

d. Pour afficher les paramètres iSCSI, choisissez la sous-clé Paramètres.

e. Ouvrez le menu contextuel (clic droit) pour la valeur MaxRequestHoldTimeDWORD (32 bits), choisissez Modifier, puis remplacez la valeur par. **`600`**

MaxRequestHoldTimeindique pendant combien de secondes l'initiateur Microsoft iSCSI doit maintenir et réessayer les commandes en attente avant de notifier un événement à la couche supérieure. `Device Removal` Cette valeur représente un temps d'attente de 600 secondes.

2. Vous pouvez augmenter la quantité maximale de données pouvant être envoyées dans les paquets iSCSI en modifiant les paramètres suivants :

- FirstBurstLengthcontrôle la quantité maximale de données qui peuvent être transmises dans le cadre d'une demande d'écriture non sollicitée. Définissez cette valeur sur **`262144`** ou sur la valeur par défaut du système d'exploitation Windows, en choisissant la valeur la plus élevée.
- MaxBurstLengthest similaire à FirstBurstLength, mais il définit la quantité maximale de données pouvant être transmises dans des séquences d'écriture sollicitées. Définissez cette valeur sur **`1048576`** ou sur la valeur par défaut du système d'exploitation Windows, en choisissant la valeur la plus élevée.
- MaxRecvDataSegmentLengthcontrôle la taille maximale des segments de données associés à une unité de données à protocole unique (PDU). Définissez cette valeur sur **`262144`** ou sur la valeur par défaut du système d'exploitation Windows, en choisissant la valeur la plus élevée.

> **Note**
>
> Différents logiciels de sauvegarde peuvent être optimisés pour fonctionner au mieux à l'aide de différents paramètres iSCSI. Pour vérifier les valeurs de ces paramètres qui offrent les meilleures performances, consultez la documentation de votre logiciel de sauvegarde.

3. Augmentez la valeur de délai d'attente du disque, comme illustré ci-après:

a. Démarrez l'éditeur de registre (`Regedit.exe`), si vous ne l'avez pas déjà fait.

b. Accédez à la sous-clé Disk dans la sous-clé Services du CurrentControlSet, comme indiqué ci-dessous.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
```

c. Ouvrez le menu contextuel (clic droit) pour la valeur TimeOutValueDWORD (32 bits), choisissez Modifier, puis remplacez la valeur par. **`600`**

TimeOutValueindique pendant combien de secondes l'initiateur iSCSI attendra une réponse de la cible avant de tenter de restaurer une session en interrompant puis en rétablissant la connexion. Cette valeur représente un délai d'attente de 600 secondes.

4. Pour veiller à ce que les nouvelles valeurs de configuration prennent effet, redémarrez votre système.

Avant de redémarrer, vous devez vous assurer que les résultats de toutes les opérations d'écriture pour les volumes ont été nettoyés. Pour ce faire, prenez n'importe quel disque de volume de stockage mappé hors ligne avant de redémarrer.

Personnalisation de vos paramètres iSCSI Linux

Une fois que vous avez configuré l'initiateur pour la passerelle, nous vous recommandons vivement de personnaliser vos paramètres iSCSI pour empêcher l'initiateur de se déconnecter des cibles. En augmentant les valeurs de délai iSCSI comme illustré ci-après, vous permettez à votre application de mieux traiter les opérations d'écriture qui prennent beaucoup de temps et d'autres questions temporaires telles que les interruptions de réseau.

> **Note**
>
> Les commandes peuvent être légèrement différentes pour d'autres types de Linux. Les exemples suivants sont basés sur Red Hat Linux.

Pour personnaliser vos paramètres iSCSI Linux

1. Augmentez la durée maximale pendant laquelle les demandes sont mises en attente.

a. Ouvrez le fichier `/etc/iscsi/iscsid.conf` et recherchez les lignes suivantes.

```
node.session.timeo.replacement_timeout = [replacement_timeout_value]
```

```
node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
```

b. Définissez la *[replacement_timeout_value]* valeur sur**600**.

Définissez la *[noop_out_interval_value]* valeur sur**60**.

Définissez la *[noop_out_timeout_value]* valeur sur**600**.

Ces trois valeurs sont exprimées en secondes.

> **Note**
>
> Les paramètres `iscsid.conf` doivent être définis avant la découverte de la passerelle. Si vous avez déjà découvert votre passerelle ou si vous vous êtes connecté à la cible, ou les deux, vous pouvez supprimer l'entrée de la base de données de découverte à l'aide de la commande suivante. Vous pouvez ensuite redécouvrir ou vous connecter à nouveau pour récupérer la nouvelle configuration.
>
> ```
> iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
> ```

2. Augmentez les valeurs maximales pour la quantité de données pouvant être transmises dans chaque réponse.

a. Ouvrez le fichier `/etc/iscsi/iscsid.conf` et recherchez les lignes suivantes.

```
node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
node.conn[0].iscsi.MaxRecvDataSegmentLength
 = [replacement_segment_length_value]
```

b. Nous recommandons les valeurs suivantes pour obtenir de meilleures performances. Votre logiciel de sauvegarde peut être optimisé pour utiliser différentes valeurs. Consultez donc la documentation de ce dernier pour obtenir les meilleurs résultats.

Définissez la *[replacement_first_burst_length_value]* valeur sur **262144** ou la valeur par défaut du système d'exploitation Linux, selon la valeur la plus élevée.

Définissez la *[replacement_max_burst_length_value]* valeur sur **1048576** ou la valeur par défaut du système d'exploitation Linux, selon la valeur la plus élevée.

Définissez la *[replacement_segment_length_value]* valeur sur **262144** ou la valeur par défaut du système d'exploitation Linux, selon la valeur la plus élevée.

> **Note**
>
> Différents logiciels de sauvegarde peuvent être optimisés pour fonctionner au mieux à l'aide de différents paramètres iSCSI. Pour vérifier les valeurs de ces paramètres qui offrent les meilleures performances, consultez la documentation de votre logiciel de sauvegarde.

3. Redémarrez le système pour veiller à ce que les nouvelles valeurs de configuration prennent effet.

   Avant de redémarrer, vous devez vous assurer que les résultats de toutes les opérations d'écriture pour les bandes ont été nettoyées. Pour ce faire, démontez les bandes avant de redémarrer.

Configuration de l'authentification CHAP pour vos cibles iSCSI

Storage Gateway prend en charge l'authentification entre votre passerelle et les initiateurs iSCSI grâce au protocole CHAP (Challenge-Handshake Authentication Protocol). Le protocole CHAP fournit une protection contre les attaques de lecture en vérifiant régulièrement l'identité d'un initiateur iSCSI authentifié pour accéder à un volume et à un appareil VTL cible.

> **Note**
>
> La configuration CHAP est facultative, mais vivement recommandée.

Pour configurer le protocole CHAP, vous devez le configurer à la fois sur la console Storage Gateway et dans le logiciel initiateur iSCSI que vous utilisez pour vous connecter à la cible. Storage Gateway utilise le protocole CHAP mutuel, c'est-à-dire lorsque l'initiateur authentifie la cible et que la cible authentifie l'initiateur.

Pour paramétrer l'authentification CHAP mutuelle pour vos cibles

1. Configurez CHAP sur la console , comme indiqué dans Pour configurer CHAP pour une cible d'appareil VTL sur la console Storage Gateway.

2. Dans votre logiciel initiateur client, finalisez la configuration de CHAP :

   - Pour configurer l'authentification CHAP mutuelle sur un client Windows, consultez Pour configurer l'authentification CHAP mutuelle sur un client Windows.
   - Pour configurer l'authentification CHAP mutuelle sur un client Red Hat Linux, consultez Pour configurer l'authentification CHAP mutuelle sur un client Red Hat Linux.

Pour configurer CHAP pour une cible d'appareil VTL sur la console Storage Gateway

Au cours de cette procédure, vous spécifiez deux clés secrètes qui sont utilisées pour lire et écrire sur une bande virtuelle. Ces mêmes clés sont utilisées dans la procédure pour configurer l'initiateur du client.

1. Dans le volet de navigation, choisissez Passerelles.
2. Sélectionnez votre passerelle, puis choisissez l'onglet Périphériques VTL afin d'afficher tous vos périphériques VTL.
3. Choisissez l'appareil pour lequel vous souhaitez configurer CHAP.
4. Fournissez les informations demandées dans la boîte de dialogue Configurer l'authentification CHAP.

   a. Pour Nom de l'initiateur, entrez le nom de votre initiateur iSCSI. Ce nom est un nom qualifié Amazon iSCSI (IQN) qui est ajouté à `iqn.1997-05.com.amazon:`, suivi du nom de la cible. Voici un exemple.

      `iqn.1997-05.com.amazon:`*`your-tape-device-name`*

      Vous trouverez le nom de l'initiateur en utilisant votre logiciel d'initiateur iSCSI. Par exemple, pour les clients Windows, le nom est la valeur de l'onglet Configuration de l'initiateur iSCSI. Pour plus d'informations, consultez Pour configurer l'authentification CHAP mutuelle sur un client Windows.

      > **Note**
      >
      > Pour modifier le nom d'un initiateur, vous devez d'abord désactiver CHAP, modifier le nom de l'initiateur dans votre logiciel d'initiateur iSCSI, puis activer le protocole CHAP avec le nouveau nom.

   b. Pour Secret utilisé pour authentifier l'initiateur, entrez le secret demandé.

Ce secret doit comporter 12 caractères au minimum et 16 caractères au maximum. Cette valeur est la clé secrète que l'initiateur (autrement dit, le client Windows) doit connaître pour participer à CHAP avec la cible.

c. Pour Secret utilisé pour authentifier la cible (authentification CHAP mutuelle), entrez le secret demandé.

   Ce secret doit comporter 12 caractères au minimum et 16 caractères au maximum. Cette valeur est la clé secrète que la cible doit connaître pour participer à CHAP avec l'initiateur.

> **Note**
>
> Le secret utilisé pour authentifier la cible doit être différent de celui utilisé pour authentifier l'initiateur.

d. Choisissez Save (Enregistrer).

5. Sur l'onglet Périphériques VTL, vérifiez que le champ de l'authentification CHAP iSCSI est défini sur vrai.

Pour configurer l'authentification CHAP mutuelle sur un client Windows

Au cours de cette procédure, vous configurez CHAP dans l'initiateur iSCSI Microsoft à l'aide des mêmes clés que celles utilisées pour configurer CHAP pour le volume de la console.

1. Si l'initiateur iSCSI n'a pas encore été démarré, dans le menu Démarrer de l'ordinateur client Windows, choisissez Exécuter, entrez **`iscsicpl.exe`**, puis choisissez OK pour exécuter le programme.
2. Configurez l'authentification CHAP mutuelle pour l'initiateur (autrement dit, le client Windows) :

   a. Cliquez sur l'onglet Configuration.

> **Note**
>
> La valeur Nom de l'initiateur est unique pour l'initiateur et votre société. Le nom indiqué précédemment est la valeur que vous avez utilisée dans la boîte de dialogue Configurer l'authentification CHAP de la console Storage Gateway.

Le nom affiché dans l'exemple d'image est uniquement utilisé à des fins d'illustration.

b. Choisissez CHAP.

c. Dans la boîte de dialogue Secret Chap mutuel initiateur iSCSI, entrez la valeur secrète de l'authentification CHAP mutuelle.

   Dans cette boîte de dialogue, vous entrez le secret que l'initiateur (le client Windows) utilise pour authentifier la cible (le volume de stockage). Ce secret permet à la cible de lire et d'écrire sur l'initiateur. Ce secret est le même que celui saisi dans la zone Secret utilisé pour authentifier la cible (authentification CHAP mutuelle) de la boîte de dialogue Configurer l'authentification CHAP. Pour plus d'informations, consultez Configuration de l'authentification CHAP pour vos cibles iSCSI.

d. Si la clé que vous avez saisie comporte moins de 12 caractères ou plus de 16 caractères, une boîte de dialogue d'erreur Secret CHAP de l'initiateur s'affiche.

   Choisissez OK, puis entrez la clé à nouveau.

3. Configurez la cible avec le secret de l'initiateur pour finaliser la configuration CHAP mutuelle.

   a. Choisissez l'onglet Cibles.

   b. Si la cible que vous souhaitez configurer pour CHAP est actuellement connectée, déconnectez-la en la sélectionnant, puis en choisissant Se déconnecter.

   c. Sélectionnez la cible que vous souhaitez configurer pour CHAP, puis choisissez Se connecter.

   d. Dans la boîte de dialogue Se connecter à la cible, choisissez Avancé.

   e. Dans la boîte de dialogue Paramètres avancés, configurez CHAP.

      i. Sélectionnez Activer la connexion CHAP.

      ii. Saisissez le secret obligatoire pour authentifier l'initiateur. Ce secret est le même que celui saisi dans la zone Secret utilisé pour authentifier l'initiateur de la boîte de dialogue Configurer l'authentification CHAP. Pour plus d'informations, consultez Configuration de l'authentification CHAP pour vos cibles iSCSI.

      iii. Sélectionnez Effectuer une authentification mutuelle.

      iv. Pour appliquer ces modifications, choisissez OK.

   f. Dans la boîte de dialogue Se connecter à la cible, choisissez OK.

4. Si vous avez fourni la clé secrète correcte, la cible affiche l'état Connecté.

Pour configurer l'authentification CHAP mutuelle sur un client Red Hat Linux

Au cours de cette procédure, vous configurez CHAP dans l'initiateur iSCSI Linux à l'aide des mêmes clés que celles utilisées pour configurer CHAP pour le volume de la console Storage Gateway.

1. Veillez à ce que le démon iSCSI soit en cours d'exécution et connectez-vous à une cible au préalable. Si vous n'avez pas terminé ces deux tâches, consultez Connexion à un client Linux.
2. Déconnectez-vous et supprimez toute configuration existante pour la cible pour laquelle vous êtes sur le point de configurer CHAP.

   a. Pour trouver le nom de la cible et vérifier qu'il s'agit bien d'une configuration définie, répertoriez les configurations enregistrées à l'aide de la commande suivante.

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. Déconnectez-vous de la cible.

   La commande suivante déconnecte de la cible nommée **myvolume** qui est définie dans le nom qualifié iSCSI Amazon (IQN). Changez le nom de la cible et le nom qualifié comme requis dans votre cas de figure.

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. Supprimez la configuration pour la cible.

   La commande suivante supprime la configuration de la cible **myvolume**.

   ```
   sudo /sbin/iscsiadm --mode node --op delete --targetname
    iqn.1997-05.com.amazon:myvolume
   ```

3. Modifiez le fichier de configuration iSCSI pour activer le protocole CHAP.

   a. Obtenez le nom de l'initiateur (autrement dit, le client que vous utilisez).

   La commande suivante obtient le nom de l'initiateur dans le fichier `/etc/iscsi/initiatorname.iscsi`.

```
sudo cat /etc/iscsi/initiatorname.iscsi
```

La sortie de cette commande ressemble à ceci :

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. Ouvrez le fichier `/etc/iscsi/iscsid.conf`.

c. Décommentez les lignes suivantes du fichier et spécifiez les valeurs correctes pour*username*, *passwordusername_in*, et*password_in*.

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

Pour des conseils sur les valeurs à spécifier, consultez le tableau suivant.

Paramètre de configuration	Valeur
username	Le nom de l'initiateur que vous avez trouvé lors d'une étape précédente de cette procédure. La valeur commence par iqn. Par exemple, **iqn.1994-05.com.redhat:8e89b27b5b8** est une *username* valeur valide.
password	La clé secrète utilisée pour authentifier l'initiateur (le client que vous utilisez) quand il communique avec le volume.
username_in	L'IQN du volume cible. La valeur commence par iqn et se termine par le nom de la cible. Par exemple, **iqn.1997-05.com.amazon:myvolume** est une *username_in* valeur valide.
password_in	La clé secrète utilisée pour authentifier la cible (le volume) quand il communique avec l'initiateur.

d. Enregistrez les modifications dans le fichier de configuration, puis fermez le fichier.

4. Découvrez la cible et connectez-vous à celle-ci. Pour ce faire, suivez les étapes décrites dans Connexion à un client Linux.

Utilisation AWS Direct Connect avec Storage Gateway

AWS Direct Connect relie votre réseau interne au cloud Amazon Web Services. AWS 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 AWS 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' AWS Direct Connect emplacement, ou dans une autre AWS région.

L'illustration suivante montre un exemple de AWS 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 AWS 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 AWS Direct Connect dans le Guide de l'utilisateur AWS Direct Connect .
2. Connectez votre appliance Storage Gateway sur site au AWS Direct Connect routeur.
3. Créez une interface virtuelle publique et configurez votre routeur sur site en conséquence. Même avec Direct Connect, les points de terminaison VPC doivent être créés avec le. HAProxy Pour plus d'informations, consultez Création d'une interface virtuelle dans le Guide de l'utilisateur AWS Direct Connect .

Pour plus de détails AWS Direct Connect, voir Qu'est-ce que c'est AWS Direct Connect ? dans le guide de AWS Direct Connect l'utilisateur.

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 EC2 passerelles Amazon, vous pouvez également obtenir l'adresse IP de votre EC2 instance Amazon depuis la console de EC2 gestion Amazon. 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
- EC2 hôte : Obtenir une adresse IP auprès d'un EC2 hôte Amazon

Lorsque vous localisez l'adresse IP, prenez-en note. Retournez ensuite à la console Storage Gateway et tapez l'adresse IP dans la console.

Obtenir une adresse IP auprès d'un EC2 hôte Amazon

Pour obtenir l'adresse IP de l' EC2 instance Amazon sur laquelle votre passerelle est déployée, connectez-vous à la console locale de l' EC2 instance. Obtenez ensuite l'adresse IP en haut de la page de la console. Pour obtenir des instructions, consultez Connexion à votre console locale Amazon EC2 Gateway.

Vous pouvez également obtenir l'adresse IP depuis l'Amazon EC2 Management Console. 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 EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances, puis sélectionnez l' EC2 instance 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 EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances, puis sélectionnez l' EC2 instance 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.
4. Une fois votre passerelle activée, choisissez-la, puis cliquez sur l'onglet Appareils VTL dans le volet inférieur.
5. Obtenez les noms de tous vos appareils VTL.
6. Pour chaque cible, exécutez la commande suivante pour configurer la cible.

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```
7. Pour chaque cible, exécutez la commande suivante pour vous connecter.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   Votre passerelle est désormais connectée à l'aide de l'adresse IP élastique de l' EC2instance.

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 incluent généralement ce qui suit : volume, bande virtuelle, cible iSCSI et appareil vtl.

Ceux-ci sont appelés des sous-ressources, qui n'existent pas tant qu'elles n'ont pas été associées à une passerelle.

Ces ressources et sous-ressources sont associées à des noms de ressources Amazon uniques (ARNs), comme indiqué dans le tableau suivant.

Type de ressource	Format ARN
ARN de passerelle	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
Bande ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:tape/`*`tapebarcode`*
Cible ARN (cible iSCSI)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*
ARN du dispositif VTL	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/device/`*`vtldevice`*

Storage Gateway prend également en charge l'utilisation d' EC2 instances, de volumes EBS et de snapshots. Ces ressources sont EC2 des ressources Amazon utilisées dans Storage Gateway.

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. Un ID de volume a le format `vol-3344CCDD`, `vol` correspondant à l'identificateur de ressource pour les volumes.

Pour les bandes virtuelles, vous pouvez ajouter un préfixe comportant jusqu'à quatre caractères à l'ID du code à barres pour vous aider à organiser les bandes.

IDs Les ressources Storage Gateway sont en majuscules. Toutefois, lorsque vous utilisez ces ressources IDs avec l' EC2 API Amazon, Amazon EC2 attend des ressources IDs en minuscules.

Vous devez modifier votre identifiant de ressource en minuscules pour pouvoir l'utiliser avec l' EC2 API. Par exemple, dans Storage Gateway, l'ID d'un volume peut être `vol-1122AABB`. Lorsque vous utilisez cet identifiant avec l' EC2 API, vous devez le remplacer par`vol-1122aabb`. Dans le cas contraire, l' EC2 API risque de ne pas se comporter comme prévu.

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.

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 balises

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 de crayon en regard de la balise que vous voulez modifier, puis modifiez la balise.
5. Lorsque vous avez fini de modifier la balise, choisissez Enregistrer.

Pour supprimer une balise

1. Ouvrez la console Storage Gateway 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 Storage Gateway

Cette section décrit les outils et licences tiers dont nous dépendons pour fournir les fonctionnalités de Storage Gateway.

Le code source de certains composants de logiciels open source qui sont inclus dans le logiciel AWS Storage Gateway est disponible en téléchargement aux emplacements suivants :

- Pour les passerelles déployées sur VMware ESXi, téléchargez le fichier sources.tar
- Pour les passerelles déployées sur Microsoft Hyper-V, téléchargez sources_hyperv.tar
- Pour les passerelles déployées sur une machine virtuelle de noyau Linux (KVM), téléchargez Sources_KVM.tar

Ce produit comprend un logiciel développé par OpenSSL Project pour une utilisation dans OpenSSL Toolkit (http://www.openssl.org/). Pour connaître les licences pertinentes pour tous les outils tiers dépendants, veuillez consulter Licences tierces.

AWS Storage Gateway quotas

Dans cette rubrique, vous trouverez des informations sur les quotas de volume et de bande, la configuration et les limites de performances pour Storage Gateway.

Rubriques

- Quotas pour les bandes
- Tailles des disques locaux recommandées pour votre passerelle

Quotas pour les bandes

Le tableau suivant répertorie les quotas pour les bandes.

Description	Passerelle de bande
Taille minimale d'une bande virtuelle	100 Gio
Taille maximale d'une bande virtuelle	15 Tio
Nombre maximal de bandes virtuelles attribuées à une passerelle	1 500
Taille totale de toutes les bandes attribuées à une passerelle	1 Pio
Nombre maximal de bandes virtuelles dans une archive	Aucune limite
Taille totale de toutes les bandes dans une archive	Aucune limite

Tailles des disques locaux recommandées pour votre passerelle

Le tableau suivant recommande des tailles pour le stockage du disque local associé à la passerelle déployée.

Type de passerelle	Cache (minimum)	Cache (maximum)	Tampon de chargement (minimum)	Tampon de chargement (maximum)	Autres disques locaux requis
Passerelle de bandes	150 Gio	64 Tio	150 Gio	2 Tio	—

> **Note**
>
> Vous pouvez configurer un ou plusieurs disques locaux pour votre cache et votre tampon de chargement, dans la limite de leur capacité maximale.
> Lorsque vous ajoutez un cache ou une mémoire tampon de téléchargement à une passerelle existante, il est important de créer de nouveaux disques sur votre hôte (hyperviseur ou EC2 instance Amazon). Ne modifiez pas la taille des disques existants si les disques ont été alloués entant que tampons de cache ou de chargement.

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 utiliser le AWS SDKs lorsque vous développez des applications avec AWS Storage Gateway. AWS SDKs Pour Java, .NET et PHP, ils encapsulent l' AWS Storage Gateway API 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

- En-têtes de requêtes obligatoires pour Storage Gateway
- Signature des requêtes
- Réponses d'erreur
- Actions

En-têtes de requêtes obligatoires pour Storage Gateway

Cette section décrit les en-têtes obligatoires que vous devez envoyer avec toutes les demandes POST à 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
```

Voici les en-têtes qui doivent être inclus avec vos demandes POST à 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 à Storage Gateway de déterminer si la demande est une action valide pour la personne à l'origine de la demande. 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`	Utilisez `application/x-amz-json-1.1` en tant que type de contenu pour toutes les demandes à Storage Gateway. `Content-Type: application/x-amz-json-1.1`

En-tête	Description
`Host`	Utilisez l'en-tête hôte pour spécifier le point de terminaison Storage Gateway vers lequel 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'informa tion sur les points de terminaison disponibles pour Storage Gateway, consultez Points de terminaison et quotas AWS Storage Gateway dans le document Références générales AWS. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	Vous devez fournir l'horodatage dans l'`Date`en-tête HTTP ou dans l' AWS `x-amz-date` en-tête. (Certaines bibliothèques client HTTP ne vous permettent pas de définir l'en-tête `Date`.) Lorsqu'un en-tête `x-amz-date` est présent, Storage Gateway ignore tout en-tête `Date` au cours de l'authentification de la demande. Le `x-amz-date` format doit être ISO86 01 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 être ISO86 01. `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. D'autres calculs de référence sont inclus dans le package Signature Version 4 Test Suite du Glossaire Amazon Web Services.

Dans cet exemple il est supposé que :

- L'horodatage de la demande est « Lun, 10 septembre 2012 00:00:00 GMT ».
- Le point de terminaison est la région USA Est (Ohio).

La syntaxe générale de la 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")
```

S'il s'agit de la clé d'accès secrète, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, est utilisé, alors la signature calculée est :

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

L'étape finale consiste à construire l'en-tête `Authorization`. Pour la clé d'accès à la démonstration AKIAIOSFODNN7EXAMPLE, l'en-tête (avec des sauts de ligne ajoutés pour plus de lisibilité) 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 ou l'opération demandée 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 Opérations dans Storage Gateway.	400 Requête erronée
`UnrecognizedClientException`	Le jeton de sécurité inclus dans la demande n'est pas valide.	400 Requête erronée
`ValidationException`	La valeur du paramètre d'entrée est inexacte ou hors de portée.	400 Requête erronée

Codes d'erreur d'opération

Le tableau suivant 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

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 demande spécifiée contient des paramètres non valides.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`LocalStorageLimitExceeded`	La limite de stockage local a été dépassée.	AddCache AddUploadBuffer AddWorkingStorage
`LunInvalid`	Le préfixe LUN spécifié est incorrect.	CreateStorediSCSIVolume

Code d'erreur d'opération	Message	Opérations qui retournent ce code d'erreur
`MaximumVolumeCount Exceeded`	Le nombre de volumes maximum a été dépassé.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurati onChanged`	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."
}
```

Opérations dans Storage Gateway

Pour obtenir la liste des opérations Storage Gateway consultez Actions dans Référence d'API AWS Storage Gateway .

Historique du document de guide de l'utilisateur de passerelle de bande

- Version de l'API : 2013-06-30
- Dernière date de mise à jour de la documentation : 24 novembre 2020

Le tableau ci-après décrit les modifications importantes dans chaque édition du Guide de l'utilisateur AWS Storage Gateway 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 inclure des mises à niveau du système d'exploitation et des logiciels, des correctifs pour améliorer la stabilité, les performances et la sécurité, ainsi que l'accès aux nouvelles fonctionnalités. Vous pouvez désormais configurer un paramètre pour activer ou désactiver ces mises à jour pour chaque passerelle individuelle de votre déploiement. Pour plus d'informations, voir Gestion des mises à jour de passerelle à l'aide de la AWS Storage Gateway console .	6 juin 2024
Support obsolète pour Tape Gateway sur Snowball Edge	Il n'est plus possible d'héberger Tape Gateway sur les appareils Snowball Edge.	14 mars 2024

Instructions mises à jour pour tester la configuration de votre passerelle à l'aide d'applications tierces	Les instructions pour tester la configuration de votre passerelle à l'aide d'applications tierces décrivent désormais le comportement attendu si votre passerelle redémarre pendant une tâche de sauvegarde en cours. Pour plus d'informations, consultez Utilisation d'un logiciel de sauvegarde pour tester la configuration de votre passerelle.	24 octobre 2023
CloudWatch Alarmes recommandées mises à jour	L' CloudWatch `HealthNotifications` alarme s'applique désormais et est recommandée pour tous les types de passerelles et de plateformes hôtes. Les paramètres de configuration recommandés ont également été mis à jour pour `HealthNotifications` et`AvailabilityNotifications` . Pour plus d'informations, voir Comprendre les CloudWatch alarmes .	2 octobre 2023

Augmentation de la taille maximale de bande à 15 Tio pour les passerelles de bande	Pour les passerelles de bande, la taille maximale d'une bande virtuelle est désormais augmentée de 5 Tio à 15 Tio. Pour plus d'informations, consultez Quotas pour les bandes dans le Guide de l'utilisateur de Storage Gateway.	4 octobre 2022
Des guides de l'utilisateur de passerelle de bande et de passerelle de volume indépendants	Le guide de l'utilisateur de Storage Gateway, qui contenait auparavant des informations à la fois sur les types de passerelle de bande et de passerelle de volume, a été scindé en un guide de l'utilisateur de passerell e de bande et un guide de l'utilisateur de passerelle de volume, chacun contenant des informations sur un seul type de passerelle. Pour plus d'informations, consultez le Guide de l'utilisateur de passerelle de bande et le Guide de l'utilisateur de passerelle de volume.	23 mars 2022
Mise à jour des procédures de création de passerelle	Les procédures de création de tous les types de passerelles à l'aide de la console Storage Gateway ont été mises à jour. Pour plus d'informations, consultez Création de votre passerelle.	18 janvier 2022

Nouvelle interface de bandes	La page de présentation des bandes dans la AWS Storage Gateway console a été mise à jour avec de nouvelles fonctionnalités de recherche et de filtrage. Toutes les procédures pertinentes de ce guide ont été mises à jour pour décrire les nouvelles fonctionn alités. Pour plus d'informa tions, consultez la section Gestion de votre passerelle de bande.	23 septembre 2021
Support pour Quest NetVault Backup 13 pour Tape Gateway	Tape Gateway prend désormais en charge Quest NetVault Backup 13 sous Microsoft Windows Server 2012 R2 ou Microsoft Windows Server 2016. Pour plus d'informations, voir Tester votre configuration à l'aide de Quest NetVault Backup.	22 août 2021
Suppression des rubriques relatives à la passerelle de fichiers S3 des guides de passerelle de bande et de volume	Afin de faciliter la compréhen sion des guides d'utilisation de passerelle de bande et de passerelle de volume par les clients qui configurent leurs types de passerelles respectif s, certaines rubriques inutiles ont été supprimées.	21 juillet 2021

Prise en charge d'IBM Spectrum Protect 8.1.10 sous Windows et Linux pour la passerelle de bande	La passerelle de bande prend désormais en charge IBM Spectrum Protect version 8.1.10 sur Microsoft Windows Server et Linux. Pour plus d'informations, consultez Test de votre configuration en utilisant IBM Spectrum Protect.	24 novembre 2020
Conformité au programme FedRAMP	Storage Gateway est désormais conforme à FedRAMP. Pour plus d'informations, consultez Validation de conformité pour Storage Gateway.	24 novembre 2020
Limitation de la bande passante basée sur la planification	Storage Gateway prend désormais en charge la limitation de la bande passante basée sur la planification pour les passerelles de bande et de volume. Pour plus d'informations, consultez Planification de la limitation de la bande passante à l'aide de la console Storage Gateway.	9 novembre 2020

Volume mis en cache et stockage en cache local des passerelles de bande multiplié par 4	Storage Gateway prend désormais en charge un cache local pouvant atteindre 64 To pour les volumes mis en cache et les passerell es de bande, amélioran t ainsi les performances des applications sur site en fournissant un accès à faible latence à des jeux de données de travail plus importants. Pour plus d'informations, consultez Tailles de disque local recommandées pour votre passerelle.	9 novembre 2020
Migration de passerelle	Storage Gateway prend désormais en charge la migration des passerelles de volume mis en cache vers de nouvelles machines virtuelle s. Pour plus d'informations, consultez Déplacement de volumes mis en cache vers une nouvelle machine virtuelle de passerelle de volume mis en cache.	10 septembre 2020

Support pour le verrouillage par rétention des bandes et la protection des bandes write-once-read-many (WORM)	Storage Gateway prend en charge le verrouillage de rétention de bande sur les bandes virtuelles et à inscription unique et lecture multiple (WORM). Le verrouillage de rétention de bande vous permet de définir le mode et la durée de conservation des bandes virtuelles archivées, empêchant ainsi leur suppression pendant une durée fixe pouvant aller jusqu'à 100 ans. Cela inclut les contrôles d'autorisation permettant de déterminer qui peut supprimer des bandes ou modifier les paramètres de rétention. Pour plus d'informations, consultez Utilisation du verrouillage de rétention de bande. Les bandes virtuelles activées par WORM permettent de garantir que les données des bandes actives de votre bibliothèque de bandes virtuelles ne peuvent pas être remplacées ou effacées. Pour plus d'informations, consultez la section Protection des bandes à inscription unique et lecture multiple (WORM).	19 août 2020

Commandez l'appliance matérielle via la console	Vous pouvez désormais commander l'appliance matérielle par le biais de la AWS Storage Gateway console. Pour plus d'informations, consultez Utilisation de l'appliance matérielle de Storage Gateway.	12 août 2020
Prise en charge des points de terminaison FIPS (Federal Information Processing Standard) dans de nouvelles régions AWS	Vous pouvez désormais activer une passerelle avec des points de terminaison on 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
Migration de passerelle	Storage Gateway prend désormais en charge la migration des passerelles de bande et de volume stocké vers de nouvelles machines virtuelles. Pour plus d'informations, consultez Déplacement de vos données vers une nouvelle passerelle.	31 juillet 2020

Afficher les CloudWatch alarmes Amazon dans la console Storage Gateway	Vous pouvez désormais consulter les CloudWatch alarmes dans la console Storage Gateway. Pour plus d'informations, voir 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 volume, consultez Choix d'un point de terminaison de service. Pour choisir un point de terminaison FIPS pour une passerelle de bande, consultez Connexion de votre passerelle de bande à AWS.	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
Doublement des performances de lecture et d'écriture de la passerelle de bande	Storage Gateway double les performances de lecture et d'écriture des bandes virtuelles sur une passerelle de bande, ce qui vous permet d'effectuer des sauvegardes et des récupérations plus rapidement qu'auparavant. Pour plus d'informations, consultez Recommandations en matière de performances pour les passerelles de bande dans le Guide de l'utilisateur Storage Gateway.	23 avril 2020

Prise en charge de la création automatique de bande	Storage Gateway permet désormais de créer automatiquement de nouvelles bandes virtuelles. Une passerelle de bande crée automatiquement de nouvelles bandes virtuelles afin de maintenir le nombre minimal de bandes disponibles configurées et met ensuite ces nouvelles bandes à disposition aux fins de l'importation par l'application de sauvegarde, ce qui permet à vos tâches de sauvegarde de s'exécuter sans interruption. Pour plus d'informations, consultez Création automatique de bandes dans le Guide de l'utilisateur Storage Gateway.	23 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'hyperviseurs 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 performances. Pour plus d'informations, consultez Performances dans le Guide de l'utilisateur Storage Gateway.	20 novembre 2019

Nouvelle AWS région pour Tape Gateway	La passerelle de bande est désormais disponible dans la région Amérique du Sud (São Paulo). Pour plus d'informations, consultez Points de terminaison et quotas AWS Storage Gateway dans le Références générales AWS.	24 septembre 2019
Prise en charge d'IBM Spectrum Protect version 7.1.9 sur Linux et, pour les passerelles de bande, augmentation de la taille de bande maximale à 5 Tio	Les passerelles de bande prennent désormais en charge IBM Spectrum Protect (Tivoli Storage Manager) version 7.1.9 s'exécutant sous Linux, en plus de s'exécuter sur Microsoft Windows. Pour plus d'informations, consultez Test de votre configuration à l'aide d'IBM Spectrum Protect dans le Guide de l'utilisateur Storage Gateway. De plus, pour les passerelles de bande, la taille maximale d'une bande virtuelle est désormais augmentée de 2,5 Tio à 5 Tio. Pour plus d'informations, consultez Quotas pour les bandes dans le Guide de l'utilisateur de Storage Gateway.	10 septembre 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 AWS région	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 AWS région	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
Prise en charge du transfert de bandes virtuelles depuis S3 Glacier Flexible Retrieval vers S3 Glacier Deep Archive	Vous pouvez maintenant déplacer vos bandes virtuelles qui sont archivées dans la classe de stockage S3 Glacier Flexible Retrieval vers la classe de stockage S3 Glacier Deep Archive pour une conservation des données économique et à long terme. Pour plus d'informations, consultez Déplacement d'une bande depuis S3 Glacier Flexible Retrieval vers S3 Glacier Deep Archive.	28 mai 2019

Support du partage de fichiers SMB pour Microsoft Windows ACLs	Pour les passerelles de fichiers, vous pouvez désormais utiliser les listes de contrôle d'accès Microsoft Windows (ACLs) pour contrôler l'accès aux partages de fichiers SMB (Server Message Block). Pour plus d'informations, voir Utilisation de Microsoft Windows ACLs pour contrôler l'accès à un partage de fichiers SMB.	8 mai 2019
Intégration à S3 Glacier Deep Archive	La passerelle de bande s’intègre à S3 Glacier Deep Archive. Vous pouvez désormais archiver les bandes virtuelles dans S3 Glacier Deep Archive pour la conservation des données à long terme. Pour plus d’informations, consultez Archivage des bandes virtuelles.	27 mars 2019

Disponibilité de l'appareil Storage Gateway Hardware Appliance en Europe	L'appareil Storage Gateway Hardware Appliance est maintenant disponible à l'achat en Europe. Pour plus d'informations, consultez Régions d'appliance matérielle AWS Storage Gateway dans le document Références générales AWS. De plus, vous pouvez désormais augmenter le stockage utilisable sur l'appareil Storage Gateway Hardware Appliance de 5 To à 12 To et remplacer la carte réseau cuivre installée par une carte réseau à fibre optique 10 gigabits. Pour plus d'informations, consultez Configuration de votre appliance matérielle.	25 février 2019
Intégration avec AWS Backup	Storage Gateway s'intègre à AWS Backup. Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder des applications professionnelles sur site qui utilisent des volumes Storage Gateway pour un stockage basé sur le cloud. Pour plus d'informations, consultez Sauvegarde de vos volumes.	16 janvier 2019

Prise en charge de Bacula Enterprise et IBM Spectrum Protect	Les passerelles de bande prennent maintenant en charge Bacula Enterprise et IBM Spectrum Protect. Storage Gateway prend également désormais en charge les nouvelles versions de Veritas NetBackup, Veritas Backup Exec et Quest backup. NetVault Vous pouvez désormais utiliser ces applications de sauvegarde pour sauvegarder vos données sur Amazon S3 et les archiver directement dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Utilisation d'un logiciel de sauvegarde pour tester la configuration de votre passerelle.	13 novembre 2018
Prise en charge de l'appliance matérielle Storage Gateway	L'appliance matérielle de 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

Compatibilité avec Microsoft System Center 2016 Data Protection Manager (DPM)	Les passerelles de bande sont désormais compatible avec Microsoft System Center 2016 Data Protection Manager (DPM). Vous pouvez désormais utiliser Microsoft DPM pour sauvegarder vos données sur Amazon S3 et les archiver directement dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Test de votre configuration à l'aide de Microsoft System Center Data Protection Manager.	18 juillet 2018
Prise en charge du protocole SMB (Server Message Block)	Ajout de la prise en charge du protocole SMB (Server Message Block) pour le partage de fichiers.des passerelles de fichiers. Pour plus d'informations, consultez Création d'un partage de fichiers.	le 20 juin 2018

Prise en charge du chiffrement sur partage de fichiers, volumes mis en cache et bande virtuelle	Vous pouvez désormais utiliser AWS Key Management Service (AWS KMS) pour chiffrer les données écrites sur un partage de fichiers, un volume mis en cache ou une bande virtuelle. Actuellement, vous pouvez utiliser l'API AWS Storage Gateway pour ce faire. Pour plus d'informations, consultez Chiffrement des données à l'aide de AWS KMS.	12 juin 2018
Support pour NovaStor DataCenter /Network	Les passerelles sur bande prennent désormais en charge les NovaStor DataCenter/Network. You can now use NovaStor DataCenter/Network versions 6.4 ou 7.1 pour sauvegarder vos données sur Amazon S3 et les archiver directement sur un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre configuration à l'aide de NovaStor DataCenter /Network.	24 mai 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.

Modification	Description	Date de modification
Prise en charge de la classe de stockage S3 One Zone_IA	Pour les passerelles de fichiers, vous pouvez désormais choisir la classe de stockage S3 One Zone_IA comme classe de stockage par défaut pour vos partages de fichiers. L'utilisation de cette classe de stockage vous permet de stocker vos données d'objet dans une seule zone de disponibilité dans Amazon S3. Pour plus d'informations, consultez Créer un partage de fichiers.	4 avril 2018
Nouvelle région	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
Support pour les notifications d'actualisation du cache, le paiement par le demandeur et l'analyse ACLs des buckets Amazon S3.	Les passerelles de fichiers vous permettent désormais d'être informé lorsque la passerelle termine l'actualisation du cache pour votre compartiment Amazon S3. Pour plus d'informations, consultez le RefreshCachefichier .html dans le Storage Gateway API Reference. Les passerelles de fichiers permettent désormais au demandeur ou au lecteur de payer les frais d'accès au lieu du propriétaire du compartiment. Les passerelles de fichiers vous permettent désormais de donner le contrôle total au propriétaire du compartiment S3 qui est mappé sur le partage de fichiers NFS. Pour plus d'informations, consultez Créer un partage de fichiers.	1er mars 2018

Modification	Description	Date de modification
Support pour Dell EMC NetWorker V9.x	Les passerelles sur bande sont désormais compatibles avec Dell EMC NetWorker V9.x. Vous pouvez désormais utiliser Dell EMC NetWorker V9.x pour sauvegarder vos données sur Amazon S3 et les archiver directement sur un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre installation à l'aide de Dell EMC NetWorker.	27 février 2018
Nouvelle région	Storage Gateway est désormais disponible dans la Région Europe (Paris). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	18 décembre 2017
Prise en charge de la notification de chargement de fichier et de la détermination du type MIME	Les passerelles de fichiers vous permettent désormais d'être notifié lorsque tous les fichiers écrits dans votre partage de fichiers NFS ont été chargés dans Amazon S3. Pour plus d'informations, consultez NotifyWhenUploadedle manuel Storage Gateway API Reference. Les passerelles de fichiers vous permettent désormais de deviner le type MIME des objets chargés en fonction des extensions de fichier. Pour plus d'informations, consultez Créer un partage de fichiers.	21 novembre 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

Modification	Description	Date de modification
Compatibilité avec Commvault 11	Les passerelles de bande sont maintenant compatibles avec Commvault 11. Vous pouvez désormais utiliser Commvault pour sauvegarder vos données sur Amazon S3 et les archiver directement dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Test de votre configuration à l'aide de Commvault.	12 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
Prise en charge de trois à cinq heures d'extraction de bandes d'une archive	Pour une passerelle de bande, vous pouvez désormais extraire vos bandes d'une archive en trois à cinq heures. Vous pouvez également déterminer la quantité de données écrites sur la bande à partir de votre application de sauvegarde ou de votre bibliothèque de bandes virtuelles (VTL). Pour plus d'informations, consultez Affichage de l'utilisation de la bande.	23 mai 2017
Nouvelle région	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

Modification	Description	Date de modification
Mises à jour des paramètres de partage de fichiers Prise en charge de l'actualisation du cache pour les partages de fichiers	Les passerelles de fichiers ajoutent désormais des options de montage aux paramètres de partage de fichiers. Vous pouvez désormais définir des options d'écrasement et de lecture seule pour votre partage de fichiers. Pour plus d'informations, consultez Créer un partage de fichiers. Les passerelles de fichiers peuvent désormais rechercher dans le compartiment Amazon S3 les objets qui ont été ajoutés ou supprimés depuis que la passerelle a répertorié pour la dernière fois le contenu du compartiment et mis en cache les résultats . Pour plus d'informations, consultez RefreshCachela référence de l'API.	28 mars 2017
Prise une charge du clonage d'un volume	Pour les passerelles de volumes mises en cache, il AWS Storage Gateway est désormais possible de cloner un volume à partir d'un volume existant. Pour plus d'informations, consultez Clonage d'un volume.	16 mars 2017

Modification	Description	Date de modification
Support pour les passerelles de fichiers sur Amazon EC2	AWS Storage Gateway permet désormais de déployer une passerelle de fichiers sur Amazon EC2. Vous pouvez lancer une passerelle de fichiers dans Amazon à EC2 l'aide de l'AMI Storage Gateway Amazon Machine Image (AMI) désormais disponible en tant qu'AMI communautaire. Pour plus d'informations sur la façon de créer une passerelle de fichiers et de la déployer sur une EC2 instance, consultez Créer et activer une passerelle de fichiers Amazon S3 ou Créer et activer une passerelle de FSx fichiers Amazon. Pour plus d'informations sur le lancement d'une AMI de passerelle de fichiers, consultez Déploiement d'une passerelle de fichiers S3 sur un EC2 hôte Amazon ou Déploiement d'une passerelle de FSx fichiers sur un EC2 hôte Amazon.	08 février 2017
Compatibilité avec Arcserve 17	La passerelle de bande est maintenant compatible avec Arcserve 17. Vous pouvez désormais utiliser Arcserve pour sauvegarder vos données sur Amazon S3 et les archiver directement sur S3 Glacier Flexible Retrieval. Pour plus d'informations, consultez Tester votre configuration à l'aide d'Arcserve Backup r17.0.	17 janvier 2017
Nouvelle région	Storage Gateway est désormais disponible dans la région UE (Londres). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	13 décembre 2016
Nouvelle région	Storage Gateway est désormais disponible dans la région Canada (Centre). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	08 décembre 2016

Modification	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
Backup Exec 16	La passerelle de bande est maintenant compatible avec Backup Exec 16. Vous pouvez désormais utiliser Backup Exec 16 pour sauvegarder vos données sur Amazon S3 et les archiver directement dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre configuration à l'aide de Veritas Backup Exec.	7 novembre 2016
Compatibilité avec Micro Focus (HPE) Data Protector 9.x	La passerelle de bande est maintenant compatible avec Micro Focus (HPE) Data Protector 9.x. Vous pouvez désormais utiliser HPE Data Protector pour sauvegarder vos données sur Amazon S3 et les archiver directement sur S3 Glacier Flexible Retrieval. Pour plus d'informations, consultez Test de votre configuration à l'aide de Micro Focus (HPE) Data Protector.	2 novembre 2016
Nouvelle région	Storage Gateway est désormais disponible dans la région USA Est (Ohio). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	17 octobre 2016

Modification	Description	Date de modification
Nouvelle conception de la console Storage Gateway	La console de gestion de Storage Gateway a été modifiée pour faciliter la configuration, la gestion et la surveillance de vos passerelles, volumes et bandes virtuelles. L'interface utilisateur fournit désormais des vues qui peuvent être filtrées et fournit des liens directs vers AWS des services intégrés tels qu' CloudWatch Amazon EBS. Pour de plus amples informations, veuillez consulter Inscrivez-vous pour AWS Storage Gateway.	30 août 2016
Compatibilité avec Veeam Backup & Replication V9 Mise à jour 2 ou ultérieure	La passerelle de bande est maintenant compatible avec Veeam Backup & Replication V9 Mise à jour 2 ou ultérieure (c'est-à-dire la version 9.0.0.1715 ou ultérieure). Vous pouvez désormais utiliser Veeam Backup & Replication V9 Mise à jour 2 ou ultérieure pour sauvegarder vos données sur Amazon S3 et les archiver directement dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre configuration à l'aide de Veeam Backup & Replication.	15 août 2016
Volume et capture d'écran plus longs IDs	Storage Gateway introduit une version plus longue IDs pour les volumes et les instantanés. Vous pouvez activer le format d'identifiant plus long pour vos volumes, instantanés et autres AWS ressources prises en charge. Pour de plus amples informations, veuillez consulter Comprendre les ressources et les ressources de Storage Gateway IDs.	25 avril 2016

Modification	Description	Date de modification
Nouvelle région Prise en charge du stockage jusqu'à 512 Tio pour les volumes stockés Autres mises à jour et améliorations de la passerelle sur la console locale Storage Gateway	La passerelle de bande est désormais disponible dans la région Asie-Pacifique (Séoul). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway. Pour les volumes stockés, vous pouvez désormais créer jusqu'à 32 volumes de stockage, chacun pouvant accueillir 16 Tio de données, pour un maximum de 512 Tio de stockage. Pour plus d'informations, consultez Architecture des volumes stockés et AWS Storage Gateway quotas. La taille totale de toutes les bandes d'une bibliothèque de bandes virtuelles passe à 1 Pio. Pour plus d'informations, consultez AWS Storage Gateway quotas. Vous pouvez désormais définir le mot de passe de la console locale de la machine virtuelle sur la console Storage Gateway. Pour plus d'informations, veuillez consulter Définition du mot de passe de la console locale à partir de la console Storage Gateway.	21 mars 2016
Compatibilité avec pour Dell EMC NetWorker 8.x	Tape Gateway est désormais compatible avec Dell EMC NetWorker 8.x. Vous pouvez désormais utiliser Dell EMC NetWorker pour sauvegarder vos données sur Amazon S3 et les archiver directement sur un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre installation à l'aide de Dell EMC NetWorker.	29 février 2016

Modification	Description	Date de modification
Support de l' VMware ESXi hyperviseur version 6.0 et de l'initiateur iSCSI Red Hat Enterprise Linux 7	AWS Storage Gateway prend désormais en charge la version 6.0 de l' VMware ESXi hyperviseur et l'initiateur iSCSI Red Hat Enterprise Linux 7. Pour plus d'informations, consultez Hyperviseurs pris en charge et exigences pour l'hôte et Initiateurs iSCSI pris en charge.	20 octobre 2015
Restructuration du contenu	Cette version inclut cette amélioration : la documentation inclut maintenant une section sur la gestion de la passerelle activée qui regroupe les tâches de gestion communes à toutes les solutions de passerelle. Vous trouverez ci-dessous des instructions sur la gestion de la passerelle après son déploiement et son activation. Pour plus d'informations, consultez Gestion de votre Tape Gateway.	

Modification	Description	Date de modification
Prise en charge du stockage jusqu'à 1 024 Tio pour les volumes mis en cache	Pour les volumes mis en cache, vous pouvez désormais créer jusqu'à 32 volumes de stockage, chacun pouvant accueillir 32 Tio de données, pour un maximum de 1 024 Tio de stockage. Pour plus d'informations, consultez Architecture des volumes mis en cache et AWS Storage Gateway quotas.	16 septembre 2015
Support du type d'adaptateur réseau VMXNET3 (10 GbE) dans VMware ESXi l'hyperviseur	Si votre passerelle est hébergée sur un VMware ESXi hyperviseur, vous pouvez la reconfigurer pour utiliser le type d' VMXNET3 adaptateur. Pour de plus amples informations, veuillez consulter Configuration des adaptateurs réseau pour votre passerelle.	
Améliorations des performances	Le taux de chargement maximal pour Storage Gateway a augmenté à 120 Mo par seconde et le taux de téléchargement maximal a augmenté de 20 Mo par seconde.	
Diverses améliorations et mises à jour de la console locale Storage Gateway	La console locale Storage Gateway a été mise à jour et améliorée avec des fonctionnalités supplémentaires vous permettant d'effectuer des tâches de maintenance. Pour plus d'informations, consultez Configuration de votre passerelle réseau.	
Prise en charge du balisage	Storage Gateway prend désormais en charge le balisage des ressources. Vous pouvez maintenant ajouter des balises aux passerelles, volumes et bandes virtuelles afin de faciliter leur gestion. Pour plus d'informations, consultez Balisage des ressources Storage Gateway.	2 septembre 2015

Modification	Description	Date de modification
Compatibilité avec Quest (anciennement Dell) NetVault Backup 10.0	Tape Gateway est désormais compatible avec Quest NetVault Backup 10.0. Vous pouvez désormais utiliser Quest NetVault Backup 10.0 pour sauvegarder vos données sur Amazon S3 et les archiver directement sur un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre configuration à l'aide de Quest NetVault Backup.	22 juin 2015

Modification	Description	Date de modification
Prise en charge des volumes de stockage de 16 Tio pour les configurations de passerelle de volume stocké	Storage Gateway prend désormais en charge les volumes de stockage de 16 Tio pour les configurations de passerelle de volume stocké. Vous pouvez désormais créer 12 volumes de 16 Tio pour un maximum de 192 Tio de stockage. Pour plus d'informations, consultez Architecture des volumes stockés.	3 juin 2015
Prise en charge des contrôles de ressources système sur la console locale Storage Gateway	Vous pouvez désormais déterminer si les ressources de votre système (cœurs virtuels du processeur, taille du volume racine et RAM) sont suffisantes pour que la passerelle fonctionne correctement. Pour plus d'informations, consultez Affichage de l'état des ressources système de la passerelle ou Affichage de l'état des ressources système de la passerelle.	
Prise en charge de l'initiateur iSCSI Red Hat Enterprise Linux 6	Storage Gateway prend désormais en charge l'initiateur iSCSI Red Hat Enterprise Linux 6. Pour plus d'informations, consultez Exigences relatives à la configuration de Tape Gateway.	
	Cette version comprend les mises à jour et améliorations de Storage Gateway suivantes : • Sur la console Storage Gateway, vous pouvez maintenant voir la date et l'heure de la dernière mise à jour du logiciel de la passerelle. Pour plus d'informations, consultez Gestion des mises à jour de passerelle. • Storage Gateway fournit maintenant une API que vous pouvez utiliser pour afficher les initiateurs iSCSI connectés à vos volumes de stockage. Pour	

Modification	Description	Date de modification
	plus d'informations, consultez ListVolumeInitiatorsla référence de l'API.	
Prise en charge de l'hyperviseur Microsoft Hyper-V versions 2012 et 2012 R2	Storage Gateway prend désormais en charge l'hyperviseur Microsoft Hyper-V versions 2012 et 2012 R2. Cette prise en charge s'ajoute à celle de l'hyperviseur Microsoft Hyper-V version 2008 R2. Pour plus d'informations, consultez Hyperviseurs pris en charge et exigences pour l'hôte.	30 avril 2015
Compatibilité avec Symantec Backup Exec 15	La passerelle de bande est maintenant compatible avec Symantec Backup Exec 15. Vous pouvez désormais utiliser Symantec Backup Exec 15 pour sauvegarder vos données sur Amazon S3 et les archiver directement dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre configuration à l'aide de Veritas Backup Exec.	6 avril 2015
Prise en charge de l'authentification CHAP pour les volumes de stockage	Storage Gateway prend désormais en charge la configuration de l'authentification CHAP pour les volumes de stockage. Pour plus d'informations, consultez Configurer l'authentification CHAP pour vos volumes.	2 avril 2015
Support pour les versions 5.1 et 5.5 de l' VMware ESXi hyperviseur	Storage Gateway prend désormais en charge les versions 5.1 et 5.5 de l' VMware ESXi hyperviseur. Cela s'ajoute à la prise en charge des versions 4.1 et 5.0 de l' VMware ESXi hyperviseur. Pour de plus amples informations, veuillez consulter Hyperviseurs pris en charge et exigences pour l'hôte.	30 mars 2015

Modification	Description	Date de modification
Prise en charge de l'utilitaire Windows CHKDSK	Storage Gateway prend désormais en charge l'utilitaire Windows CHKDSK. Vous pouvez utiliser cet utilitaire pour vérifier l'intégrité de vos volumes et corriger des erreurs sur ces derniers. Pour plus d'informations, consultez Résolution des problèmes de volume.	04 mars 2015
Intégration avec AWS CloudTrail pour capturer les appels d'API	Storage Gateway est désormais intégré à AWS CloudTrail. AWS CloudTrail capture les appels d'API effectués par ou pour le compte de Storage Gateway dans votre compte Amazon Web Services et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Pour de plus amples informations, veuillez consulter Connexion et surveillance dans AWS Storage Gateway. Cette version comprend la mise à jour et l'amélioration de Storage Gateway suivantes : • Des bandes virtuelles comportant des données imprécises dans le stockage de cache (c'est-à-dire contenant des éléments qui n'ont pas été téléchargés sur AWS) sont maintenant récupérées lorsque lecteur mis en cache de la passerelle est modifié. Pour plus d'informations, consultez Récupération d'une bande virtuelle à partir d'une passerelle irrécupérable.	16 décembre 2014

Modification	Description	Date de modification
Compatibilité avec des logiciels de sauvegarde supplémentaires et le changeur de média	La passerelle de bande est maintenant compatible avec les logiciels de sauvegarde suivants : • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 Vous pouvez désormais utiliser ces quatre produits logiciels de sauvegarde avec la bibliothèque de bandes virtuelles (VTL) de Storage Gateway pour les sauvegardes dans Amazon S3 et l'archivage direct dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Utilisation d'un logiciel de sauvegarde pour tester la configuration de votre passerelle. Storage Gateway fournit maintenant un changeur de média supplémentaire qui fonctionne avec le nouveau logiciel de sauvegarde. Cette version inclut diverses AWS Storage Gateway améliorations et mises à jour.	3 novembre 2014
Région Europe (Francfort)	Storage Gateway est désormais disponible dans la région Europe (Francfort). Pour plus d'informations, consultez Régions AWS compatibles avec Storage Gateway.	23 octobre 2014

Modification	Description	Date de modification
Restructuration du contenu	Création d'une section Mise en route commune à toutes les solutions de passerelle. Vous trouverez ci-dessous des instructions pour vous permettre de télécharger, de déployer et d'activer une passerelle. Une fois que vous avez déployé et activé une passerelle, vous pouvez passer à des instructions propres aux configurations de passerelle de volume stocké, de passerelle de volume mis en cache ou de passerelle de bande. Pour plus d'informations, consultez Création d'une passerelle de bande.	19 mai 2014
Compatibilité avec Symantec Backup Exec 2012	La passerelle de bande est maintenant compatible avec Symantec Backup Exec 2012. Vous pouvez désormais utiliser Symantec Backup Exec 2012 pour sauvegarder vos données sur Amazon S3 et les archiver directement dans un stockage hors ligne (S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive). Pour plus d'informations, consultez Tester votre configuration à l'aide de Veritas Backup Exec.	28 avril 2014

Modification	Description	Date de modification
Prise en charge du clustering de basculement Windows Server Support pour l' VMware initiateur ESX Prise en charge de l'exécution des tâches de configuration sur la console locale Storage Gateway	• Storage Gateway permet désormais de connecter plusieurs hôtes au même volume, si les hôtes coordonnent leur accès en utilisant le clustering de basculement Windows Server (WSFC). Toutefois, la connexion de plusieurs hôtes au même volume ne peut se faire sans utiliser WSFC. • Storage Gateway vous permet maintenant de gérer la connectivité de stockage directement par le biais de votre hôte ESX. Cela constitue une alternative à l'utilisation d'initiateurs résidant dans le système d'exploitation invité de votreVMs. • Storage Gateway prend désormais en charge l'exécution des tâches de configuration sur la console locale Storage Gateway. Pour plus d'informations sur l'exécution des tâches de configuration sur des passerelles déployées sur site, consultez Exécution des tâches sur la console locale de machine virtuelle ou Exécution des tâches sur la console locale de machine virtuelle . Pour plus d'informations sur l'exécution de tâches de configuration sur les passerelles déployées sur une EC2 instance, consultez Exécution de tâches sur la console EC2 locale Amazon ouExécution de tâches sur la console EC2 locale Amazon.	31 janvier 2014

Modification	Description	Date de modification
Prise en charge de la bibliothèque de bandes virtuelles (VTL) et présentation de l'API version 2013-06-30	Storage Gateway connecte une appliance logicielle sur site à un stockage basé sur le cloud afin d'intégrer votre environnement informatique sur site à l'infrastructure AWS de stockage. Outre les passerelles de volume (volumes mis en cache et volumes stockés), Storage Gateway prend désormais en charge les passerelles et les bibliothèques de bandes virtuelles (VTL). Vous pouvez configurer la passerelle de bande avec jusqu'à 10 lecteurs de bandes virtuelles par passerelle. Chaque lecteur de bandes virtuelles répond à l'ensemble de commandes SCSI afin que les applications de sauvegarde sur site existantes fonctionnent sans modification. Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur AWS Storage Gateway . • Pour une présentation de l'architecture, consultez Fonctionnement de la passerelle de bande (architecture). • Pour commencer à utiliser la passerelle de bande, consultez Création d'une passerelle de bande.	5 novembre 2013
Prise en charge de Microsoft Hyper-V	Storage Gateway offre maintenant la possibilité de déployer une passerelle sur site sur la plateforme de virtualisation de Microsoft Hyper-V. Les passerelles déployées sur Microsoft Hyper-V ont toutes les mêmes fonctions et fonctionnalités que la passerelle Storage Gateway sur site existante. Pour commencer à déployer une passerelle avec Microsoft Hyper-V, consultez Hyperviseurs pris en charge et exigences pour l'hôte.	10 avril 2013

Modification	Description	Date de modification
Support pour le déploiement d'une passerelle sur Amazon EC2	Storage Gateway permet désormais de déployer une passerelle dans Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez lancer une instance de passerelle dans Amazon à EC2 l'aide de l'AMI Storage Gateway disponible dans AWS Marketplace. Pour commencer à déployer une passerelle à l’aide de l’AMI Storage Gateway, consultez Déployez une EC2 instance Amazon personnalisée pour Tape Gateway.	15 janvier 2013

Modification	Description	Date de modification
Prise en charge des volumes mis en cache et présentation de l'API version 2012-06-30	Dans cette version, Storage Gateway prend en charge les volumes mis en cache. Les volumes mis en cache réduisent le besoin de redimensionner votre infrastructure de stockage sur site, tout en fournissant à vos applications un accès à faible latence à leurs données actives. Vous pouvez créer des volumes de stockage allant jusqu'à 32 Tio et les monter comme appareils iSCSI à partir de vos serveurs d'applications sur site. Les données écrites sur les volumes mis en cache sont stockées dans Amazon Simple Storage Service (Amazon S3), avec seulement un cache en local pour vos données récemment écrites et consultées sur votre matériel de stockage sur site. Les volumes mis en cache vous permettent d'utiliser Amazon S3 pour les données où des latences de récupération plus élevées sont acceptables, notamment pour les données peu consultées ou plus anciennes, tout en maintenant un stockage sur site pour les données nécessitant un accès à faible latence. Dans cette version, Storage Gateway présente également une nouvelle version d'API qui, en plus de soutenir les opérations en cours, fournit de nouvelles opérations pour prendre en charge les volumes mis en cache. Pour plus d'informations sur les deux solutions Storage Gateway, consultez Fonctionnement d'une passerelle de bande. Vous pouvez également effectuer une configuration de test. Pour plus d'informations, consultez Création d'une passerelle de bande.	29 octobre 2012

Modification	Description	Date de modification
Prise en charge des API et d'IAM	Dans cette version, Storage Gateway introduit la prise en charge des API ainsi que la prise en charge de AWS Identity and Access Management(IAM). • Prise en charge des API : vous pouvez désormais configurer et gérer vos ressources Storage Gateway par programme. Pour plus d'informations sur les API, consultez Référence d'API pour Storage Gateway dans le Guide d'utilisateur AWS Storage Gateway . • Prise en charge d'IAM : AWS Identity and Access Management (IAM) vous permet de créer des utilisateurs et de gérer l'accès utilisateur à vos ressources Storage Gateway à l'aide de politiques IAM. Pour obtenir des exemples de politiques IAM, consultez Identity and Access Management pour AWS Storage Gateway. Pour plus d'informations sur IAM, consultez page détaillée de AWS Identity and Access Management (IAM).	9 mai 2012
Prise en charge des adresses IP statiques	Vous pouvez maintenant spécifier une adresse IP statique pour votre passerelle locale. Pour plus d'informations, consultez Configuration de votre passerelle réseau.	5 mars 2012
Nouveau guide	Il s'agit de la première version du Guide de l'utilisateur AWS Storage Gateway .	24 janvier 2012

Notes de mise à jour relatives au logiciel de l'appliance Tape Gateway

Ces notes de mise à jour décrivent les fonctionnalités nouvelles et mises à jour, les améliorations et les correctifs inclus dans chaque version de l'appliance Tape Gateway . Chaque version du logiciel est identifiée par sa date de sortie et un numéro de version unique.

Vous pouvez déterminer le numéro de version logicielle d'une passerelle en consultant sa page de détails dans la console Storage Gateway ou en appelant l'action DescribeGatewayInformationAPI à l'aide d'une AWS CLI commande similaire à la suivante :

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

Le numéro de version est renvoyé dans le `SoftwareVersion` champ de réponse de l'API.

> **Note**
>
> Une passerelle ne communiquera pas les informations relatives à la version du logiciel dans les cas suivants :
>
> - La passerelle est hors ligne.
> - La passerelle exécute un logiciel plus ancien qui ne prend pas en charge les rapports de version.
> - Le type de passerelle est FSx File Gateway.

Pour plus d'informations sur les mises à jour de Tape Gateway , notamment sur la façon de modifier le calendrier de maintenance et de mise à jour automatique par défaut pour une passerelle, consultez Gestion des mises à jour de passerelle à l'aide de la console AWS Storage Gateway .

Passerelles basées sur Amazon Linux 2023 (AL2023)

Le tableau suivant répertorie les notes de mise à jour pour les passerelles basées sur AL2 023.

> **Note**
>
> Les versions 2.x.x de Gateway ne peuvent pas être mises à jour vers la version 3.x.x.

Date de parution	Version du logiciel	Notes de mise à jour
16/07/2025	3.0.0	• Version initiale du nouveau système d'exploitation

Passerelles basées sur Amazon Linux (2AL2)

Le tableau suivant répertorie les notes de mise à jour pour les passerelles basées surAL2.

Date de parution	Version du logiciel	Notes de mise à jour
31/07/2025	2,12,12	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
2025-07-01	2.12,11	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
02/06/2025	2,1,10	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes

Date de parution	Version du logiciel	Notes de mise à jour
01/05/2025	2.12,9	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
01/05/2025	2.12,8	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
01/04/2025	2.12,7	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
04/03/2025	2.12,6	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes

Date de parution	Version du logiciel	Notes de mise à jour
04/02/2025	2,1,5	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes • Résolution d'un problème selon lequel les passerelles pouvaient rester bloquées à l'état d'arrêt après une mise à jour logicielle
07-01-2025	2.12.3	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
2024-12-06	2.12.2	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
06/11/2024	2.12.1	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes

Date de parution	Version du logiciel	Notes de mise à jour
2024-10-03	2.12.0	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
30/08/2024/	2.11.0	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes
29/07/2024	2.10.0	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes • Corrections de bogues et améliorations diverses
17/06/2024	2.9.2	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des passerelles nouvelles et existantes

Date de parution	Version du logiciel	Notes de mise à jour
28/05/2024	2.9.0	• Réduction du temps de redémarrage de la passerelle lors des mises à jour logicielles • Réduction de la quantité de données transférées pour estimer la bande passante du réseau
08-05-2024/	2.8.3	• Résolution d'un problème de connectivité au cloud lors de l'utilisation d' SOCKS5 un proxy • Résolution du problème de dégradation des performances de téléchargement dans certaines conditions (telles qu'un nombre élevé d'opérations d'effacement de bande)
10/04/2024-04	2.8.1	• Résolution d'un problème d'utilisation de la mémoire introduit dans la version 2.8.0 • mises à jour des correctifs de sécurité • Processus de mise à jour logicielle amélioré • Correction d'un composant NTP (Network Time Protocol) manquant pour les nouvelles passerelles

Date de parution	Version du logiciel	Notes de mise à jour
06/03/2024	2.8.0	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des nouvelles passerelles • mises à jour des correctifs de sécurité • Performances améliorées pour les charges de travail simultanées de sauvegarde et de restauration
19/12/2023	2.7.0	• Système d'exploitation et éléments logiciels mis à jour pour améliorer la sécurité et les performances des nouvelles passerelles
14/12/2023	2.6.6	• Correction d'un problème de positionnement relatif sur des cassettes de plus de 5 TiB
19/10/2023	2.6.5	• Protection accrue contre le remplacement des bandes par les clients après le redémarrage de la passerell e

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.