aws

Guide de l’utilisateur

Amazon EBS

Amazon EBS: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon Elastic Block Store ?

Amazon Elastic Block Store (Amazon EBS) fournit des ressources de stockage par blocs évolutives et performantes qui peuvent être utilisées avec les instances Amazon Elastic Compute Cloud (Amazon EC2). Avec Amazon Elastic Block Store, vous pouvez créer et gérer les ressources de stockage par blocs suivantes :

- Volumes Amazon EBS : il s'agit de volumes de stockage que vous associez aux EC2 instances Amazon. Après avoir attaché un volume à une instance, vous pouvez l'utiliser de la même manière que vous utiliseriez un disque dur local connecté à un ordinateur, par exemple pour stocker des fichiers ou installer des applications.
- Instantanés Amazon EBS : il s'agit de point-in-time sauvegardes de volumes Amazon EBS qui sont conservées indépendamment du volume lui-même. Vous pouvez créer des instantanés pour sauvegarder les données sur vos volumes Amazon EBS. Vous pouvez ensuite restaurer de nouveaux volumes à partir de ces instantanés à tout moment.

Rubriques

Fonctions d'Amazon EBS

Amazon EBS propose les fonctionnalités et avantages suivants :

- Plusieurs types de volumes : Amazon EBS propose plusieurs types de volumes qui vous permettent d'optimiser les performances et les coûts de stockage pour un large éventail d'applications. Les types de volumes sont divisés en deux grandes catégories : le stockage sur SSD pour les charges de travail transactionnelles et le stockage sur disque dur pour les charges de travail gourmandes en débit.
- Évolutivité — Vous pouvez créer des volumes Amazon EBS avec des spécifications de capacité et de performance qui répondent à vos besoins. À mesure que vos besoins évoluent, vous pouvez utiliser les opérations Elastic Volumes pour augmenter dynamiquement la capacité ou optimiser les performances, sans interruption de service.

- Sauvegarde et restauration : utilisez les instantanés Amazon EBS pour sauvegarder les données stockées sur vos volumes. Vous pouvez ensuite utiliser ces instantanés pour restaurer instantanément des volumes ou pour migrer des données entre des AWS comptes, des AWS régions ou des zones de disponibilité.
- Protection des données : utilisez le chiffrement Amazon EBS pour chiffrer vos volumes Amazon EBS et vos instantanés Amazon EBS. Les opérations de chiffrement ont lieu sur les serveurs hébergeant les EC2 instances Amazon, garantissant ainsi la sécurité data-in-transit entre une instance et le volume attaché et les instantanés ultérieurs. data-at-rest
- Disponibilité et durabilité des données : les volumes io2 Block Express offrent une durabilité de 99,999 % avec un taux de défaillance annuel de 0,001 %. Les autres types de volumes offrent une durabilité de 99,8 % à 99,9 % avec un taux de défaillance annuel de 0,1 % à 0,2 %. En outre, les données de volume sont automatiquement répliquées sur plusieurs serveurs d'une zone de disponibilité afin d'éviter toute perte de données due à la défaillance d'un seul composant.
- Archivage des données : EBS Snapshots Archive fournit un niveau de stockage peu coûteux pour archiver des point-in-time copies complètes des instantanés EBS que vous devez conserver pendant 90 jours ou plus pour des raisons réglementaires et de conformité, ou pour les versions futures de projets.

Services connexes

Amazon EBS fonctionne avec les services suivants :

- Amazon Elastic Compute Cloud : un service qui vous permet de lancer et de gérer des machines virtuelles (EC2 instances Amazon) dans le AWS cloud. Vous pouvez associer des volumes EBS à ces instances et les utiliser de la même manière que vous utiliseriez un disque dur local, par exemple pour stocker des fichiers ou installer des applications. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EC2 ?
- AWS Key Management Service— Un service géré qui vous permet de créer et de gérer des clés cryptographiques. Vous pouvez utiliser des clés AWS KMS cryptographiques pour chiffrer les données stockées sur vos volumes Amazon EBS et dans vos instantanés Amazon EBS. Pour plus d'informations, consultez Comment Amazon EBS utilise AWS KMS.
- Amazon Data Lifecycle Manager : service géré qui automatise la création, la conservation et la suppression des instantanés EBS et des copies sauvegardées par EBS. AMIs Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser les sauvegardes de vos volumes Amazon

EBS et de vos EC2 instances Amazon. Pour de plus amples informations, veuillez consulter Automatisez les sauvegardes avec Amazon Data Lifecycle Manager.

- EBS direct APIs : service qui vous permet de créer des instantanés EBS, d'écrire des données directement dans vos instantanés, de lire les données de vos instantanés et d'identifier les différences ou les modifications entre deux instantanés. Pour de plus amples informations, veuillez consulter Utiliser EBS direct APIs pour accéder au contenu d'un instantané EBS.
- Corbeille : service de récupération de données qui vous permet de restaurer des instantanés EBS supprimés accidentellement et sauvegardés par EBS. AMIs Pour plus d'informations, consultez la section Corbeille.

Accès à Amazon EBS

Vous pouvez créer et gérer vos ressources Amazon EBS à l'aide des interfaces suivantes :

EC2 Console Amazon

Interface Web permettant de créer et de gérer des volumes et des instantanés. Si vous avez créé un AWS compte, vous pouvez accéder à la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

AWS Command Line Interface

Un outil de ligne de commande qui vous permet de gérer les ressources Amazon EBS à l'aide de commandes dans votre shell de ligne de commande. Elle est prise en charge sur Windows, Mac et Linux. Pour plus d'informations, consultez le guide de AWS Command Line Interface l'utilisateur et les commandes ec2.

AWS Tools for PowerShell

Ensemble de PowerShell modules qui vous permettent de scripter des opérations sur vos ressources Amazon EBS à partir de la ligne de PowerShell commande. Pour plus d'informations, consultez le guide de l'AWS Tools for Windows PowerShell utilisateur et le manuel de référence des AWS Tools for PowerShell applets de commande.

AWS CloudFormation

AWS Service entièrement géré qui vous permet de créer des modèles JSON ou YAML réutilisables décrivant vos AWS ressources, puis de les approvisionner et de les configurer pour vous. Pour plus d'informations, consultez le AWS CloudFormation Guide de l'utilisateur .

API Amazon EC2 Query

L'API Amazon EC2 Query fournit des requêtes HTTP ou HTTPS qui utilisent le verbe HTTP `GET` ou `POST` un paramètre de requête nommé`Action`. Pour plus d'informations, consultez le Amazon EC2 API Reference.

AWS SDKs

Spécifiques au langage APIs qui vous permettent de créer des applications intégrées aux AWS services. AWS SDKs sont disponibles pour de nombreux langages de programmation populaires. Pour plus d'informations, consultez la section Outils sur lesquels vous pouvez vous appuyer AWS.

Tarification

Avec Amazon EBS, vous ne payez que ce que vous allouez. Pour plus d'informations, consultez la section Tarification d'Amazon EBS.

Configuration pour Amazon EBS

Effectuez les tâches décrites dans cette section pour vous préparer à utiliser les ressources Amazon EBS.

Tâches

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif
- (Facultatif) Créez et utilisez une clé gérée par le client pour le chiffrement Amazon EBS
- (Facultatif) Activez le blocage de l'accès public pour les instantanés Amazon EBS

Inscrivez-vous pour un Compte AWS

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

Pour vous inscrire à un Compte AWS

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

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

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

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d’un accès à d’autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d’autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d’un ensemble d’autorisations dans le Guide de l’utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l’utilisateur AWS IAM Identity Center .

(Facultatif) Créez et utilisez une clé gérée par le client pour le chiffrement Amazon EBS

Le chiffrement Amazon EBS est une solution de chiffrement qui utilise des clés AWS KMS cryptographiques pour chiffrer vos volumes Amazon EBS et vos instantanés Amazon EBS. Amazon EBS crée automatiquement une clé KMS AWS gérée unique pour le chiffrement Amazon EBS dans chaque région. Cette clé clé KMS possède l’alias `aws/ebs`. Vous ne pouvez pas faire pivoter la clé KMS par défaut ni gérer ses autorisations. Pour plus de flexibilité et de contrôle sur la clé KMS utilisée pour le chiffrement Amazon EBS, vous pouvez envisager de créer et d'utiliser une clé gérée par le client.

Pour créer et utiliser une clé gérée par le client pour le chiffrement Amazon EBS

1. Créez une clé KMS de chiffrement symétrique.
2. Sélectionnez la clé KMS comme clé KMS par défaut pour le chiffrement Amazon EBS.
3. Autorisez les utilisateurs à utiliser la clé KMS pour le chiffrement Amazon EBS.

(Facultatif) Activez le blocage de l'accès public pour les instantanés Amazon EBS

Pour empêcher le partage public de vos instantanés, vous pouvez activer le blocage de l'accès public pour les instantanés. Une fois que vous avez activé le blocage de l'accès public pour les instantanés dans une région, toute tentative de partage public d'instantanés dans cette région est automatiquement bloquée. Cela peut vous aider à améliorer la sécurité de vos instantanés et à protéger les données de vos instantanés contre tout accès non autorisé ou involontaire.

Pour de plus amples informations, veuillez consulter Bloquer l'accès public aux instantanés Amazon EBS.

Console

Pour activer le blocage de l'accès public aux instantanés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez EC2 Tableau de bord, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. Dans la section Bloquer l'accès public pour les instantanés EBS, choisissez Gérer.
4. Sélectionnez Bloquer l'accès public, puis choisissez l'une des options suivantes :
   - Bloquer tous les accès publics : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
   - Bloquer les nouveaux partages publics : pour bloquer tout nouveau partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.
5. Choisissez Mettre à jour.

AWS CLI

Pour activer le blocage de l'accès public aux instantanés

Utilisez la commande enable-snapshot-block-public-access. Pour `--state`, spécifiez l'une des valeurs suivantes :

- `block-all-sharing` : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- `block-new-sharing` : pour bloquer uniquement les nouveaux partages publics de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

```
aws ec2 enable-snapshot-block-public-access --state block-all-sharing|block-new-sharing
```

Volumes Amazon EBS

Un volume Amazon EBS est un dispositif de stockage durable au niveau bloc que vous pouvez attacher à vos instances. Après avoir attaché un volume à une instance, vous pouvez l'utiliser comme n'importe quel autre disque dur physique. Les volumes EBS sont flexibles. Pour des volumes de génération actuelle attachés à des types d'instances de génération actuelle, vous pouvez augmenter dynamiquement la taille, modifier la capacité IOPS provisionnée et changer le type des volumes de production en direct.

Vous pouvez utiliser des volumes EBS comme stockage principal pour des données nécessitant des mises à jour fréquentes, telles que le lecteur système pour une instance ou le stockage pour une application de base de données. Vous pouvez également les utiliser pour les applications à débit élevé qui effectuent des analyses continues du disque. Les volumes EBS persistent indépendamment de la durée de vie d'une EC2 instance.

Vous pouvez également attacher plusieurs volumes EBS à une seule instance. Le volume et l'instance doivent être dans la même zone de disponibilité. En fonction du volume et des types d'instances, vous pouvez utiliser Multi-Attach pour monter un volume sur plusieurs instances en même temps.

Amazon EBS fournit les types de volumes suivants : SSD à usage général (`gp2` et `gp3`), SSD IOPS provisionnés (`io1` et `io2`), HDD optimisé pour le débit (`st1`), HDD à froid (`sc1`) et magnétique (`standard`). Ils se distinguent par leurs caractéristiques de performance et leurs tarifs, ce qui vous permet d'adapter vos performances de stockage et vos coûts en fonction des besoins de vos applications. Pour de plus amples informations, veuillez consulter Types de volume Amazon EBS.

Votre compte a une limite sur le stockage total dont vous disposez. Pour plus d'informations sur ces limites et pour savoir comment demander leur augmentation, consultez Points de terminaison et quotas Amazon EBS (français non garanti).

Un volume EBS géré est géré par un fournisseur de services, tel qu'Amazon EKS Auto Mode. Vous ne pouvez pas modifier directement les paramètres d'un volume EBS géré. Les volumes EBS gérés sont identifiés par une valeur vraie dans le champ Géré. Pour plus d'informations, consultez la section Instances EC2 gérées par Amazon.

Pour plus d'informations sur la tarification, consultez Tarification Amazon EBS.

Table des matières

Caractéristiques et avantages des volumes Amazon EBS

Les volumes EBS offrent des avantages supplémentaires par rapport aux volumes de stockage d'instances.

Avantages

- Disponibilité des données
- Persistance des données
- Chiffrement des données
- Sécurité des données
- Instantanés
- Flexibilité

Disponibilité des données

Lorsque vous créez un volume EBS, il est automatiquement répliqué au sein la zone de disponibilité pour empêcher toute perte de données consécutive à la défaillance d'un composant matériel. Vous pouvez associer un volume EBS à n'importe quelle EC2 instance de la même zone de disponibilité. Une fois qu'un volume est attaché, il se présente comme un périphérique de stockage en mode bloc natif similaire à un disque dur ou à un autre périphérique physique. À ce stade, l'instance peut interagir avec le volume de la même façon qu'avec un périphérique local. Vous pouvez vous connecter à l'instance et formater le volume EBS à l'aide d'un système de fichiers, par exemple NTFS pour une instance Linux ou Windows, puis installer des applications. Ext4

Si vous attachez plusieurs volumes à un périphérique que vous avez nommé, vous pouvez agréger les données par bandes entre ces volumes pour de meilleures performances I/O et en matière de débit.

Vous pouvez attacher les volume EBS `io1` et `io2` à un maximum de 16 instances basées sur Nitro. Pour plus d'informations, consultez Associer un volume EBS à plusieurs EC2 instances à l'aide de l'option Multi-Attach. Sinon, vous pouvez attacher un volume EBS à une seule instance.

Vous pouvez obtenir des données de surveillance pour vos volumes EBS, y compris les données pour les volumes du périphérique racine des instances basées sur EBS, sans coût supplémentaire. Pour plus d'informations sur la surveillance des métriques, consultez CloudWatch Métriques Amazon pour Amazon EBS. Pour plus d'informations sur le suivi de l'état de vos volumes, consultez EventBridge Événements Amazon pour Amazon EBS.

Persistance des données

Un volume EBS est un stockage hors instance qui peut persister indépendamment de la vie d'une instance. Vous continuez à payer pour l'utilisation du volume tant que les données persistent.

Les volumes EBS attachés à une instance en cours d'exécution peuvent se détacher automatiquement de l'instance avec leurs données intactes lorsque l'instance est résiliée si vous décochez la case Supprimer à la résiliation lorsque vous configurez les volumes EBS pour votre instance sur la console. EC2 Le volume peut être attaché à une nouvelle instance, ce qui permet une récupération rapide. Si la case Supprimer en cas de résiliation est cochée, le ou les volumes seront supprimés à la fin de l' EC2 instance. Si vous utilisez une instance basée sur EBS, vous pouvez arrêter et redémarrer l'instance sans affecter les données stockées dans le volume attaché. Le volume reste attaché pendant le cycle d'arrêt-démarrage. Cela vous permet de traiter et de stocker indéfiniment les données sur votre volume, en utilisant les ressources de traitement et de stockage uniquement lorsque cela est nécessaire. Les données persistent sur le volume jusqu'à ce que ce volume soit explicitement supprimé. Le stockage par blocs physique utilisé par les volumes EBS supprimés est remplacé par des zéros ou des données cryptographiquement pseudo-aléatoires avant d'être alloué à un nouveau volume. Si vous travaillez avec des données sensibles, nous vous recommandons de chiffrer vos données manuellement ou de les stocker sur un volume protégé par Chiffrement Amazon EBS. Pour de plus amples informations, veuillez consulter EBSChiffrement Amazon.

Par défaut, le volume EBS racine qui est créé et attaché à une instance au moment du lancement est supprimé lorsque cette instance prend fin. Vous pouvez modifier ce comportement en changeant la valeur de l'indicateur `DeleteOnTermination` en `false` lorsque vous lancez l'instance. En

modifiant cette valeur, le volume persiste même après que l'instance ait pris fin, ce qui vous permet de l'attacher à une autre instance.

Par défaut, les volumes EBS supplémentaires qui sont créés et attachés à une instance au moment du lancement ne sont pas supprimés lorsque cette instance prend fin. Vous pouvez modifier ce comportement en changeant la valeur de l'indicateur `DeleteOnTermination` en `true` lorsque vous lancez l'instance. Cette valeur modifiée entraîne la suppression des volumes lorsque l'instance prend fin.

Chiffrement des données

Pour simplifier le chiffrement des données, vous pouvez créer des volumes EBS chiffrés avec la fonction Chiffrement Amazon EBS. Tous les types de volume EBS prennent en charge le chiffrement. Vous pouvez utiliser des volumes EBS chiffrés pour répondre à un large éventail d'exigences de data-at-rest chiffrement pour les données et applications réglementées/auditées. Le chiffrement Amazon EBS utilise des algorithmes Advanced Encryption Standard à 256 bits (AES-256) et une infrastructure de clés gérée par Amazon. Le chiffrement s'effectue sur le serveur qui héberge l' EC2 instance, fournissant le chiffrement data-in-transit entre l' EC2 instance et le stockage Amazon EBS. Pour de plus amples informations, veuillez consulter EBSChiffrement Amazon.

Le chiffrement Amazon EBS est utilisé AWS KMS keys lors de la création de volumes chiffrés et de tous les instantanés créés à partir de vos volumes chiffrés. La première fois que vous créez un volume EBS chiffré dans une région, une clé KMS AWS gérée par défaut est créée automatiquement pour vous. Cette clé est utilisée pour le chiffrement Amazon EBS, sauf si vous créez et utilisez une clé gérée par le client. La création de votre propre clé gérée par le client vous donne plus de flexibilité, notamment la possibilité de créer, de faire pivoter, de désactiver, de définir des contrôles d'accès et d'auditer les clés de chiffrement utilisées pour protéger vos données. Pour plus d'informations, consultez le Guide du développeur AWS Key Management Service.

Sécurité des données

Les volumes Amazon EBS vous sont présentés comme des périphériques de stockage en mode bloc bruts non formatés. Ces appareils sont des périphériques logiques créés sur l'infrastructure EBS et le service Amazon EBS garantit que les appareils sont logiquement vides (c'est-à-dire que les blocs bruts sont mis à zéro ou contiennent des données pseudo-aléatoires cryptographiques) avant toute utilisation ou réutilisation par un client.

Si vous avez des procédures qui exigent que toutes les données soient effacées à l'aide d'une méthode spécifique, après ou avant utilisation (ou les deux), telles que celles détaillées dans DoD

5220.22-M (National Industrial Security Program Operating Manual) ou NIST 800-88 (Guidelines for Media Sanitization), vous avez la possibilité de le faire sur Amazon EBS. Cette activité de niveau bloc sera reflétée sur le support de stockage sous-jacent du service Amazon EBS.

Instantanés

Amazon EBS donne la possibilité de créer des instantanés (sauvegardes) d'un volume EBS et de copier les données dans le volume sur Amazon S3, où elles sont stockées de façon redondante dans plusieurs zones de disponibilité. Le volume n'a pas besoin d'être attaché à une instance en cours d'exécution pour pouvoir créer un instantané. Alors que vous continuez à écrire des données sur un volume, vous pouvez créer régulièrement un instantané de ce dernier afin de l'utiliser comme base pour de nouveaux volumes. Ces instantanés peuvent être utilisés pour créer plusieurs volumes EBS ou déplacer des volumes entre les zones de disponibilité. Les instantanés de volumes EBS chiffrés sont chiffrés automatiquement.

Lorsque vous créez un volume à partir d'un instantané, celui-ci est une copie exacte du volume initial au moment où l'instantané a été créé. Les volumes EBS qui sont créés à partir d'instantanés chiffrés sont automatiquement chiffrés. En spécifiant éventuellement une zone de disponibilité différente, vous pouvez utiliser cette fonctionnalité pour dupliquer un volume dans cette zone. Les instantanés peuvent être partagés avec des AWS comptes spécifiques ou rendus publics. Lorsque vous créez des instantanés, vous occasionnez des frais dans Amazon S3 en fonction de la taille des données sauvegardées, et non de la taille du volume source. Les instantanés suivants du même volume sont des instantanés incrémentiels. Ils incluent uniquement les données modifiées et nouvelles écrites sur le volume depuis la création du dernier instantané, et la facturation ne concerne que ces données modifiées et nouvelles.

Les instantanés sont des sauvegardes incrémentielles, ce qui signifie que seuls les blocs du volume qui ont changé depuis l'instantané le plus récent sont enregistrés. Si vous avez un volume de 100 Gio de données mais que seulement 5 Gio ont changé depuis votre dernier instantané, seuls ces 5 Gio de données modifiées sont écrits sur Amazon S3. Bien que les instantanés soient enregistrés de manière incrémentielle, le processus de suppression de l'instantané prévoit que vous avez uniquement besoin de conserver l'instantané le plus récent.

Pour vous aider à classer et à gérer vos volumes et instantanés, vous pouvez les étiqueter avec les métadonnées de votre choix.

Pour la sauvegarde automatique vos volumes, vous pouvez utiliser Amazon Data Lifecycle Manager ou AWS Backup.

Flexibilité

Les volumes EBS acceptent les modifications de configuration en direct en cours de production. Vous pouvez modifier le type de volume, la taille du volume et la capacité IOPS sans interruption de service. Pour plus d'informations, consultez Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes.

Types de volume Amazon EBS

Amazon EBS fournit les types de volume suivants, qui ont des caractéristiques de performances et des prix différents, ce qui vous permet d'adapter vos performances de stockage et vos coûts en fonction des besoins de vos applications.

> **Important**
>
> Plusieurs facteurs peuvent affecter les performances des volumes EBS, tels que la configuration d'instance, les caractéristiques I/O et la demande en matière de charge de travail. Pour utiliser pleinement les IOPS provisionnés sur un volume EBS, utilisez des instances optimisées pour EBS. Pour plus d'informations sur la façon d'exploiter au mieux vos volumes EBS, consultez Performances des volumes Amazon EBS.

Pour plus d'informations sur la tarification, consultez Tarification Amazon EBS.

Types de volume

- Volumes de disque SSD (solid state drive)
- Volumes de disque dur (HDD)
- Volumes de la génération précédente

Volumes de disque SSD (solid state drive)

Les volumes sauvegardés sur SSD sont optimisés pour les charges de travail transactionnelles impliquant des read/write operations with small I/O tailles fréquentes, où le principal attribut de performance est le nombre d'E/S par seconde. Les types de volume basés sur SSD incluent les SSD à usage général et les SSD IOPS provisionnés. Voici un résumé des cas d'utilisation et des caractéristiques des volumes basés sur SSD.

	Volumes SSD à usage général Amazon EBS		Volumes SSD IOPS provisionnés par Amazon EBS	
Type de volume	gp3	gp2	io2 Block Express [3]	io1
Durabilité	99,8 % - 99,9 % (taux de défaillance annuel de 0,1 % - 0,2 %)		Durabilité de 99,999 % (taux de défaillance annuel de 0,001 %)	Durabilité de 99,8 % - 99,9 % (taux de défaillance annuel de 0,1 % - 0,2 %)
Cas d'utilisation	• Charges de travail transactionnelles • Bureaux virtuels • Bases de données à instance unique de taille Medium • Applications interactives à faible latence • Volumes de démarrage • Environnements de développement et de test		Charges de travail nécessitant : • Une latence moyenne inférieure à la milliseconde • Performance IOPS soutenue • Plus de 64 000 IOPS ou 1 000 Mio/s de débit	• Charges de travail nécessitant des performances IOPS soutenues ou supérieures à 16,000 IOPS • Charges de travail de base de données à fort taux d'I/O.
Taille du volume	1 GIB - 16 Tio		4 Gio - 64 Tio [4]	4 Gio - 16 Tio
Nombre maximal d'IOPS	16 000 (64 Kio E/S 6)	16 000 (16 Kio E/S 6)	256 000 [5] (16 Kio E/S 6)	64 000 (16 Kio E/S 6)
Débit maximal	1,000 Mio/s	250 Mio/s [1]	4 000 Mio/s	1 000 Mio/s [2]
Multi-Attach	Non pris en charge		Pris en charge	

	Volumes SSD à usage général Amazon EBS	Volumes SSD IOPS provisionnés par Amazon EBS	
Amazon EBS			
NVMe réservations	Non pris en charge	Pris en charge	Non pris en charge
Volume de démarrag	Pris en charge		

[1] La limite de débit est comprise entre 128MiB/s and 250 MiB/s, en fonction de la taille du volume. Pour de plus amples informations, veuillez consulter Performances du volume gp2. Les volumes créés avant le 3 décembre 2018 et qui n'ont pas été modifiés depuis leur création peuvent ne pas atteindre des performances optimales, sauf si vous modifiez le volume.

[2] Pour atteindre un débit maximal de 1 000 Mbits/s, le volume doit être provisionné avec 64 000 IOPS et il doit être attaché à une instance basée sur le système Nitro. Les volumes créés avant le 6 décembre 2017 et qui n'ont pas été modifiés depuis leur création peuvent ne pas atteindre des performances optimales, sauf si vous modifiez le volume.

[3] Tous les volumes `io2` créés après le 21 novembre 2023 sont des volumes `io2` Block Express. Les volumes `io2` créés avant le 21 novembre 2023 peuvent être convertis en volumes `io2` Block Express en modifiant les IOPS ou la taille du volume.

[4] Les volumes de plus de 16 TiB ne peuvent être attachés qu'à des instances créées sur le système Nitro.

[5] Les volumes supérieurs à 64 000 IOPS ne peuvent être attachés qu'à des instances créées sur le système Nitro. Des volumes allant jusqu'à 64 000 IOPS peuvent être attachés à des instances autres que Nitro, mais ils ne peuvent atteindre que 32 000 IOPS.

[6] Représente la taille d'E/S requise pour atteindre le maximum d'IOPS dans les limites de débit du volume.

Pour de plus amples informations sur les types de volume basés sur SSD, veuillez consulter les rubriques suivantes :

- Volumes SSD à usage général Amazon EBS
- Volumes SSD IOPS provisionnés par Amazon EBS

Volumes de disque dur (HDD)

Les volumes basés sur HDD sont optimisés pour les charges de travail importantes en streaming où l'attribut de performance dominant est le débit. Les types de volume HDD incluent les HDD à débit optimisé et les HDD à froid. Voici un résumé des cas d'utilisation et des caractéristiques des volumes basés sur HHD.

	Volumes HDD à débit optimisé	Volumes HDD à froid
Type de volume	`st1`	`sc1`
Durabilité	99,8 % - 99,9 % (taux de défaillance annuel de 0,1 % - 0,2 %)	
Cas d'utilisation	• Big Data • Entrepôts de données • Traitement de fichiers journaux	• Stockage axé sur le débit pour les données consultées de manière occasionnelle • Scénarios dans lesquels il est important que le coût de stockage soit le plus bas possible
Taille du volume	125 Gio - 16 Tio	
IOPS maximum par volume (1 Mio d'I/O)	500	250
Débit maximal par volume	500 Mio/s	250 Mio/s
Multi-Attach Amazon EBS	Non pris en charge	

	Volumes HDD à débit optimisé	Volumes HDD à froid
Volume de démarrage	Non pris en charge	

Pour de plus amples informations sur les volumes des disques durs (HDD), veuillez consulter Volumes HDD et Cold HDD optimisés pour le débit Amazon EBS.

Volumes de la génération précédente

Les volumes magnétiques (`standard`) sont des volumes de génération précédente basés sur des disques magnétiques. Ils conviennent aux charges de travail comportant des jeux de données réduits où l'accès aux données est rare et où les performances n'ont pas une importance primordiale. Ces volumes fournissent en moyenne 100 IOPS, avec la possibilité d'émettre en rafale jusqu'à des centaines d'IOPS. Leur taille varie entre 1 Gio et 1 Tio.

> **Tip**
>
> Les volumes magnétiques sont des volumes de génération précédente. Si vous avez besoin de performances supérieures ou plus homogènes que les volumes de la génération précédente, nous vous recommandons d'utiliser l'un des types de volume plus récents.

Le tableau suivant décrit les types de volume EBS de la génération précédente.

	Magnétique
Type de volume	`standard`
Cas d'utilisation	Charges de travail où l'accès aux données est occasionnel
Taille du volume	1 Gio - 1 Tio
IOPS maximum par volume	40–200
Débit maximal par volume	40–90 Mio/s

	Magnétique
Volume de démarrage	Pris en charge

Pour plus d'informations, veuillez consulter la rubrique Volumes de la génération précédente.

Volumes SSD à usage général Amazon EBS

Les volumes SSD à usage général (gp2 et gp3) sont soutenus par des disques SSD (). SSDs Ils constituent un bon compromis en termes de prix et de performances pour un large éventail de charges de travail transactionnelles. Il s'agit notamment des bureaux virtuels, des bases de données à instance unique de taille moyenne, des applications interactives sensibles à la latence, des environnements de développement et de test, ainsi que des volumes de démarrage. Nous recommandons ces volumes pour la plupart des charges de travail.

Amazon EBS propose les types suivants de volumes SSD à usage général :

Types

- Volumes SSD à usage général (gp3)
- Volumes SSD à usage général (gp2)

Volumes SSD à usage général (gp3)

Les volumes SSD à usage général (gp3) sont la dernière génération de volumes SSD à usage général, et le volume SSD le moins cher proposé par Amazon EBS. Ce type de volume permet de fournir le bon équilibre entre le prix et les performances pour la plupart des applications. Il vous permet également de faire évoluer les performances du volume indépendamment de sa taille. Cela signifie que vous pouvez fournir la performance requise sans avoir besoin de fournir une capacité de stockage en mode bloc supplémentaire. En outre, les volumes gp3 offrent un prix par Gio inférieur de 20 % à celui des volumes SSD à usage général (gp2).

Les volumes gp3 offrent une latence à un chiffre en millisecondes et une durabilité de 99,8 % à 99,9 % avec un taux de défaillance annuel (AFR) inférieur à 0,2 %, ce qui se traduit par un maximum de deux défaillances de volume pour 1 000 volumes en cours d'exécution sur une période d'un an. AWS conçoit les volumes gp3 pour fournir leurs performances provisionnées 99 % du temps.

Table des matières

Performances des volumes gp3

> **Tip**
>
> Les volumes gp3 n'utilisent pas de performances en rafale. Ils peuvent maintenir indéfiniment leurs meilleures performances en termes d'IOPS provisionnés et de débit.

Performance IOPS

Les volumes gp3 offrent une performance IOPS de base constante de 3 000 IOPS, qui est incluse dans le prix du stockage. Vous pouvez provisionner des IOPS supplémentaires (jusqu'à un maximum de 16 000) moyennant un coût additionnel, à raison de 500 IOPS par Gio de taille de volume. Les IOPS maximales peuvent être provisionnées pour les volumes de 32 Gio ou plus (500 IOPS par Gio × 32 Gio = 16 000 IOPS).

Performances de débit

Les volumes gp3 offrent une performance de débit de référence constante (125 %)MiB/s, which is included with the price of storage. You can provision additional throughput (up to a maximum of 1,000 MiB/s) for an additional cost at a ratio of 0.25 MiB/s per provisioned IOPS. Maximum throughput can be provisioned at 4,000 IOPS or higher and 8 GiB or larger (4,000 IOPS × 0.25 MiB/s per IOPS = 1,000 MiB/s.

Taille du volume gp3

La taille d'un volume gp3 peut varier de 1 Gio à 16 Tio.

Migrer vers gp3 depuis gp2

Si vous utilisez actuellement des volumes gp2, vous pouvez migrer vos volumes vers gp3 en utilisant les opérations Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes. Vous pouvez utiliser les opérations Amazon EBS Elastic Volumes pour modifier le type de volume, les IOPS et le débit de vos volumes existants sans interrompre vos instances Amazon. EC2 Lorsque vous utilisez la console pour créer un volume ou pour créer une AMI à partir d'un instantané, le type

de volume sélectionné par défaut est le stockage SSD à usage général gp3. Dans les autres cas, gp2 est sélectionné par défaut. Dans ces cas, vous pouvez sélectionner gp3 comme type de volume au lieu d'utiliser gp2.

Pour savoir combien vous pouvez économiser en migrant vos volumes gp2 vers gp3, utilisez le calculateur d'économies de coûts de migration de gp2 à gp3 d'Amazon EBS.

Volumes SSD à usage général (gp2)

Ils offrent un stockage économique idéal pour un large éventail de charges de travail transactionnelles. Avec les volumes gp2, les performances évoluent avec la taille du volume.

> **Tip**
>
> Les volumes gp3 sont la dernière génération de volumes SSD à usage général. Ils offrent une évolution des performances plus prévisible et des prix jusqu'à 20 % inférieurs à ceux des volumes gp2. Pour de plus amples informations, veuillez consulter Volumes SSD à usage général (gp3).
> Pour savoir combien vous pouvez économiser en migrant vos volumes gp2 vers gp3, utilisez le calculateur d'économies de coûts de migration de gp2 à gp3 d'Amazon EBS.

gp2les volumes offrent une latence à un chiffre en millisecondes et une durabilité de 99,8 % à 99,9 % avec un taux de défaillance annuel (AFR) inférieur à 0,2 %, ce qui se traduit par un maximum de deux défaillances de volume pour 1 000 volumes en cours d'exécution sur une période d'un an. AWS conçoit gp2 les volumes de manière à fournir les performances qu'ils ont fournies 99 % du temps.

Table des matières

Performances du volume **gp2**

Performance IOPS

Les performances IOPS de base évoluent de façon linéaire entre un minimum de 100 et un maximum de 16 000, à raison de 3 IOPS par Gio de taille de volume. Les performances IOPS sont provisionnées comme suit :

- Les volumes de 33,33 Gio et moins sont provisionnés avec un minimum de 100 IOPS.
- Les volumes supérieurs à 33,33 Gio sont provisionnés avec 3 IOPS par Gio de taille de volume jusqu'au maximum de 16 000 IOPS, qui est atteint à 5 334 Gio (3 X 5 334).
- Les volumes de 5 334 Gio et plus sont provisionnés avec 16 000 IOPS.

Les volumes gp2 de moins de 1 Tio (et qui sont provisionnés avec moins de 3 000 IOPS) peuvent atteindre 3 000 IOPS en cas de besoin pendant une période prolongée. La capacité d'un volume à passer en rafale est régie par les crédits d'E/S. Lorsque la demande d'E/S est supérieure aux performances de base, le volume dépense des crédits d'E/S pour atteindre le niveau de performance requis (jusqu'à 3 000 IOPS). En mode rafale, les crédits d'E/S ne sont pas accumulés et ils sont dépensés au rythme de l'IOPS utilisé au-dessus de l'IOPS de base (taux de dépense = IOPS de rafale - IOPS de base). Plus un volume a accumulé de crédits d'E/S, plus il peut maintenir ses performances en rafale. Vous pouvez calculer la durée des rafales comme suit :

```
                        (I/O credit balance)
Burst duration  =  -----------------------------
                  (Burst IOPS) - (Baseline IOPS)
```

Lorsque la demande d'E/S chute au niveau de performance de base ou à un niveau inférieur, le volume commence à accumuler des crédits d'E/S à un taux de 3 crédits d'E/S par Gio de taille de volume par seconde. Les volumes ont une limite d'accumulation de crédits d'E/S de 5,4 millions de crédits d'E/S, ce qui est suffisant pour maintenir la performance de rafale maximale de 3 000 IOPS pendant au moins 30 minutes.

> **Note**
>
> Chaque volume reçoit un solde initial de crédits d'E/S de 5,4 millions de crédits d'E/S, ce qui permet un cycle de démarrage initial rapide pour les volumes de démarrage et une bonne expérience de démarrage pour les autres applications.

Le tableau suivant présente des exemples de tailles de volume et les performances de base associées du volume, la durée des rafales (en commençant avec 5,4 millions de crédits d'E/S) et le temps nécessaire pour recharger un solde de crédits d'E/S vide.

Taille du volume (Gio)	Performances de base (IOPS)	Durée de performances en rafale à 3 000 IOPS (en secondes)	Temps nécessaire pour recharger un solde de crédits vide (en secondes)
1 à 33,33	100	1,862	54 000
100	300	2 000	18 000
334 (taille minimale pour débit maximal)	1 002	2 703	5 389
750	2 250	7 200	2 400
1 000	3 000	N/A*	N/A*
5 334 (taille minimale pour IOPS maximum) et plus	16,000	N/A*	N/A*

* Les performances de base du volume dépassent les celles en rafale maximales.

Vous pouvez surveiller le solde créditeur d'E/S d'un volume à l'aide de la `BurstBalance` métrique Amazon EBS sur Amazon. CloudWatch Cette métrique indique le pourcentage de crédits d'E/S restants pour gp2. Pour de plus amples informations, veuillez consulter Caractéristiques et surveillance des E/S Amazon EBS. Vous pouvez définir une alarme qui vous notifie lorsque la valeur `BurstBalance` tombe à un certain niveau. Pour plus d'informations, consultez la section Création d' CloudWatch alarmes.

Performances de débit

gp2les volumes fournissent un débit compris entre 128MiB/s and 250 MiB/s, en fonction de la taille du volume. Les performances de débit sont provisionnées comme suit :

- Les volumes de 170 Gio et moins offrent un débit maximal de 128 Mio/s.
- Les volumes dont la taille est supérieure à 170 Gio mais inférieure à 334 Gio peuvent atteindre un débit maximal de 250 Mio/s.
- Les volumes de 334 Gio et plus offrent un débit de 250 Mio/s.

Le débit d'un volume gp2 peut être calculé à l'aide de la formule suivante, jusqu'à la limite de débit de 250 Mio/s :

```
Throughput in MiB/s = IOPS performance × I/O size in KiB / 1,024
```

Taille du volume **gp2**

La taille des volumes gp2 peut aller de 1 Gio à 16 Tio. N'oubliez pas que les performances du volume évoluent de façon linéaire avec sa taille.

Volumes SSD IOPS provisionnés par Amazon EBS

Les volumes SSD IOPS provisionnés sont soutenus par des disques SSD (). SSDs Ce sont les volumes de stockage Amazon EBS les plus performants, conçus pour les charges de travail critiques, à forte intensité d'IOPS et de débit, qui nécessitent une faible latence. Les volumes SSD IOPS provisionnés fournissent leurs performances d'IOPS provisionnés 99,9 % du temps.

Amazon EBS propose deux types de volumes SSD IOPS provisionnés :

- Volumes SSD IOPS provisionnés (io2) Block Express
- Volumes SSD IOPS provisionnés (io1)

Volumes SSD IOPS provisionnés (**io2**) Block Express

Les volumes Block Express io2 reposent sur la nouvelle génération d'architecture de serveur de stockage Amazon EBS. Il a été conçu dans le but de répondre aux exigences de performance des applications gourmandes en E/S les plus exigeantes qui s'exécutent sur des instances basées sur le système Nitro. Avec une durabilité maximale et une latence minimale, Block Express est idéal pour exécuter des charges de travail stratégiques et exigeantes en termes de performances, telles qu'Oracle, SAP HANA, Microsoft SQL Server et SAS Analytics.

L'architecture Block Express augmente les performances et l'évolutivité des volumes io2. Les serveurs Block Express communiquent avec les instances basées sur le système Nitro à l'aide du protocole réseau SRD (Scalable Reliable Datagram). Cette interface est implémentée dans la carte Nitro dédiée à la fonction I/O Amazon EBS sur le matériel hôte de l'instance. Elle minimise le délai d'I/O et la variation de latence (instabilité réseau), fournissant ainsi des performances plus rapides et plus régulières pour vos applications.

Les volumes io2 Block Express sont conçus pour offrir une durabilité de 99,999 % avec un taux de défaillance annuel (AFR) ne dépassant pas 0,001 %, ce qui se traduit par une défaillance de volume

unique pour 100 000 volumes exécutés sur une période d'un an. `io2` Les volumes Block Express sont adaptés aux charges de travail qui bénéficient d'un volume unique offrant une latence inférieure à la milliseconde et prennent en charge des IOPS plus élevés, un débit supérieur et une capacité supérieure par rapport aux volumes gp3.

Les volumes Block Express (`io2`) SSD à IOPS provisionnés fournissent leurs performances d'IOPS provisionnés 99,9 % du temps.

`io2`Les volumes Block Express sont pris en charge sur toutes les instances créées sur le système Nitro. Pour plus d'informations, veuillez consulter volumes Block Express `io2`.

Rubriques

- Considérations
- Performances

Considérations

- Les volumes `io2` Block Express sont actuellement disponibles dans les régions suivantes : USA Est (Ohio) | USA Est (Virginie du Nord) | USA Ouest (Californie du Nord) | USA Ouest (Oregon) | Asie-Pacifique (Hong Kong) | Asie-Pacifique (Mumbai) | Asie-Pacifique (Séoul) | Asie-Pacifique (Singapour), Asie-Pacifique (Sydney) | Asie-Pacifique (Tokyo) | Canada (Centre) | Europe (Francfort), Europe (Irlande) | Europe (Londres) | Europe (Stockholm) et Moyen-Orient (Bahreïn).
- Tous les volumes `io2` créés après le 21 novembre 2023 sont des volumes `io2` Block Express. Les volumes `io2` créés avant le 21 novembre 2023 peuvent être convertis en volumes `io2` Block Express en modifiant les IOPS ou la taille du volume.
- Les instances basées sur le système Nitro peuvent être associées à des volumes d'une taille maximale de 64 TiB. D'autres types d'instances peuvent être attachés à des volumes d'une taille maximale de 16 Tio.
- Les instances basées sur le système Nitro peuvent être associées à des volumes provisionnés avec un maximum de 256 000 IOPS. D'autres types d'instances peuvent être connectés à des volumes alloués avec jusqu'à 64 000 IOPS, mais peuvent atteindre 32 000 IOPS.
- Pour créer un volume `io2` chiffré dont la taille est supérieure à 16 Tio ou dont le taux d'IOPS est supérieur à 64 000 à partir d'un instantané non chiffré ou d'un instantané chiffré partagé, vous devez effectuer les opérations suivantes
  1. Création d'une copie chiffrée de cet instantané dans votre compte
  2. Utilisation de cette copie d'instantané pour créer le volume

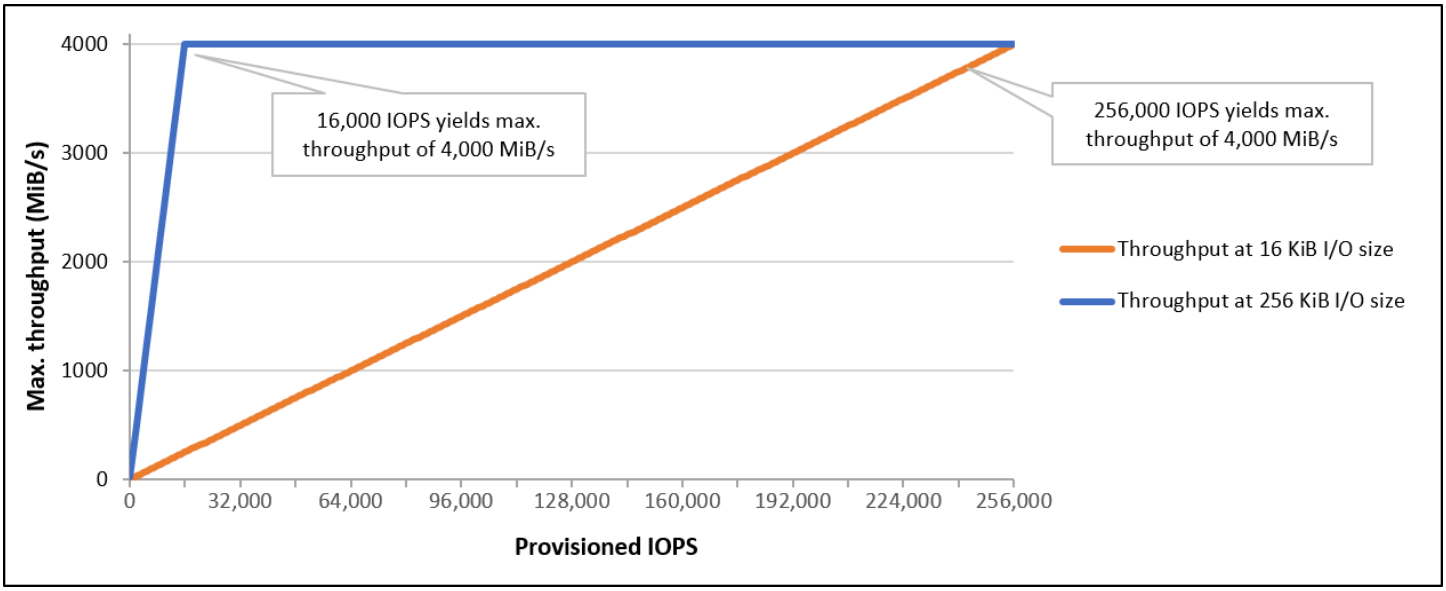
Performances

Avec les volumes Block Express `io2`, vous pouvez provisionner les volumes avec:

- une latence moyenne inférieure à la milliseconde ;
- une capacité de stockage allant jusqu'à 64 Tio (65 536 Gio) ;
- des IOPS provisionnés allant jusqu'à 256 000, avec un ratio IOPS:GIo de 1 000:1. Les IOPS maximaux peuvent être provisionnés avec des volumes de 256 Gio et plus (1 000 IOPS × 256 Gio = 256 000 IOPS).

> **Note**
>
> Vous pouvez atteindre 256 000 IOPS avec des instances basées sur le système Nitro. Sur les autres instances, vous pouvez atteindre des performances maximum de 32 000 IOPS.

- Débit de volume jusqu'à 4 000 MiB/s. Throughput scales proportionally up to 0.256 MiB/s par IOPS provisionnée. Le débit maximal peut être atteint à 16 000 IOPS ou plus.



Volumes SSD IOPS provisionnés (**`io1`**)

Les volumes SSD à IOPS provisionnés (`io1`) sont conçus pour satisfaire les besoins des charges de travail très consommatrices d'I/O, notamment les charges de travail de base de données qui sont sensibles aux performances et à l'homogénéité du stockage. Les volumes SSD IOPS provisionnés

utilisent un taux d'IOPS régulier, que vous spécifiez lors de la création du volume, et Amazon EBS fournit les performances provisionnées 99,9 % du temps.

Les volumes `io1` sont conçus pour offrir une durabilité de 99,8 à 99,99 % avec un taux de défaillance annuel (AFR) ne dépassant pas 0,2 %, ce qui se traduit par un maximum de deux défaillances de volume pour 1 000 volumes exécutés sur une période d'un an.

`io1`les volumes sont disponibles pour tous les types d' EC2 instances Amazon.

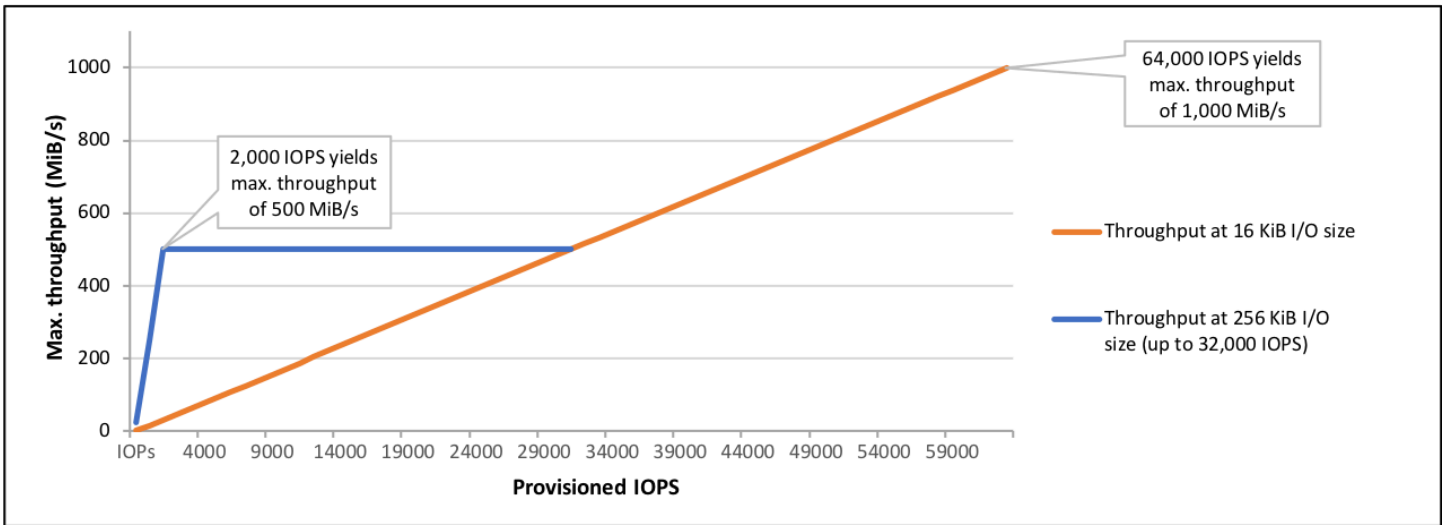
Performances

La taille des volumes `io1` peut aller de 4 Gio à 16 Tio, et vous pouvez allouer de 100 à 64 000 IOPS par volume. Le rapport maximal entre les volumes IOPS provisionnés et le volume demandé (en Gio) est de 50 pour 1. Par exemple, un volume `io1` de 100 Gio peut être allouée avec jusqu'à 5 000 IOPS.

Les IOPS maximum peuvent être allouées pour les volumes de 1 280 Gio ou plus (50 x 1 280 Gio = 64 000 IOPS).

- `io1`les volumes provisionnés avec un maximum de 32 000 IOPS prennent en charge une MiB/s of throughput. With the I/O taille d'E/S maximale de 256 KiB et offrent un rendement allant jusqu'à 500 unités au maximum. Le débit maximal est atteint à 2 000 IOPS.
- Les volumes `io1` alloués avec plus de 32 000 IOPS (jusqu'à 64 000 IOPS maximum) génèrent une augmentation linéaire du débit suivant un débit de 16 Kio par I/O par IOPS provisionné. Par exemple, un volume provisionné avec 48 000 IOPS (peut en supporter jusqu'à 750). MiB/s of throughput (16 KiB per provisioned IOPS × 48,000 provisioned IOPS = 750 MiB/s
- Pour atteindre le débit maximal de 1 000MiB/s, a volume must be provisioned with 64,000 IOPS (16 KiB per provisioned IOPS × 64,000 provisioned IOPS = 1,000 MiB/s).
- Vous pouvez atteindre 64 000 IOPS uniquement sur les instances basées sur le système Nitro. Sur les autres instances, vous pouvez atteindre des performances maximum de 32 000 IOPS.

. Le graphique suivant illustre ces performances :



La latence subie par I/O dépend des IOPS mis en service et de votre profil de charge de travail. Pour bénéficier de la meilleure expérience de latence d'I/O, assurez-vous que vous provisionnez des IOPS afin de respecter le profil d'I/O de votre charge de travail.

Volumes HDD et Cold HDD optimisés pour le débit Amazon EBS

Les volumes de disque dur fournis par Amazon EBS entrent dans les catégories suivantes :

- HDD à débit optimisé — HDD conçu pour les charges de travail à débit élevé fréquemment consultées.
- HDD à froid — HDD le plus abordable pour les charges de travail moins fréquemment consultées.

Rubriques

Restrictions de débit par instance

Le débit des volumes `st1` et `sc1` est toujours déterminé par la limite suivante la plus faible:

- Limites de débit du volume

- Limites de débit de l'instance

Comme pour tous les volumes Amazon EBS, nous vous recommandons de sélectionner une EC2 instance optimisée pour EBS appropriée afin d'éviter les goulots d'étranglement du réseau.

Volumes HDD à débit optimisé

Les volumes HDD à débit optimisé (`st1`) offrent un stockage magnétique économique qui définit les performances en termes de débit plutôt que d'IOPS. Ce type de volume convient aux charges de travail séquentielles et volumineuses comme Amazon EMR, ETL, les entrepôts de données et le traitement des journaux. Les volumes `st1` démarrables ne sont pas pris en charge.

Les volumes HDD à débit optimisé (`st1`) sont similaires aux volumes HDD à froid (`sc1`), mais ils sont conçus pour prendre en charge les données fréquemment consultées.

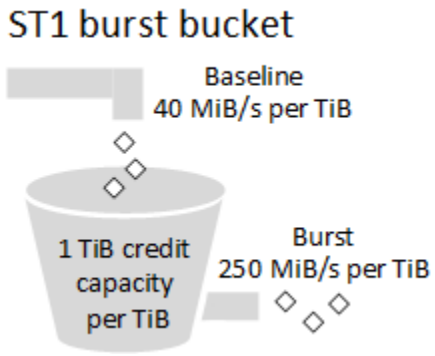
> **Note**
>
> Ce type de volume est optimisé pour les charges de travail impliquant de grandes E/S séquentielles, et nous recommandons aux clients dont les charges de travail utilisent de petites quantités d'E/S aléatoires ou. Volumes SSD à usage général Amazon EBS Volumes SSD IOPS provisionnés par Amazon EBS Pour de plus amples informations, veuillez consulter Manque d'efficacité des lectures/écritures de petite taille sur disque dur.

Les volumes HDD à débit optimisé (`st1`) attachés à des instances optimisées pour EBS sont conçus pour offrir des performances cohérentes, garantissant au moins 90 % des performances de débit prévues, et ce 99 % du temps au cours d'une année donnée.

Crédits de débit et performances en rafale

À l'instar de `gp2`, `st1` utilise un modèle de transmission de compartiment en rafales pour assurer les performances. La taille du volume détermine le débit de base du volume, qui correspond à la vitesse à laquelle le volume accumule des crédits de débit. La taille du volume détermine également le débit de transmission en rafales du volume, qui correspond à la vitesse à laquelle vous pouvez utiliser des crédits lorsqu'ils sont disponibles. Les gros volumes ont un débit de base et de transmission en rafales plus élevé. Plus votre volume a de crédits, plus longtemps il est en mesure d'assurer la transmission des I/O en rafales.

Le schéma suivant illustre le comportement du compartiment en rafales pour `st1`.



Sous réserve de la limite de débit et de crédits, le débit disponible d'un volume `st1` est exprimé par la formule suivante :

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Pour un `st1` volume de 1 To, le débit en rafale est limité à 250MiB/s, the bucket fills with credits at 40 MiB/s, et il peut contenir jusqu'à 1 To de crédits.

Les volumes plus importants redimensionnent ces limites de manière linéaire, avec un débit plafonné à 500 par MiB/s. After the bucket is depleted, throughput is limited to the baseline rate of 40 MiB/s TiB au maximum.

Sur des volumes allant de 0,125 TiB à 16 TiB, le débit de référence varie de 5, qui est atteint à MiB/s to a cap of 500 MiB/s 12,5 TiB comme suit :

```
            40 MiB/s
12.5 TiB × ---------- = 500 MiB/s
             1 TiB
```

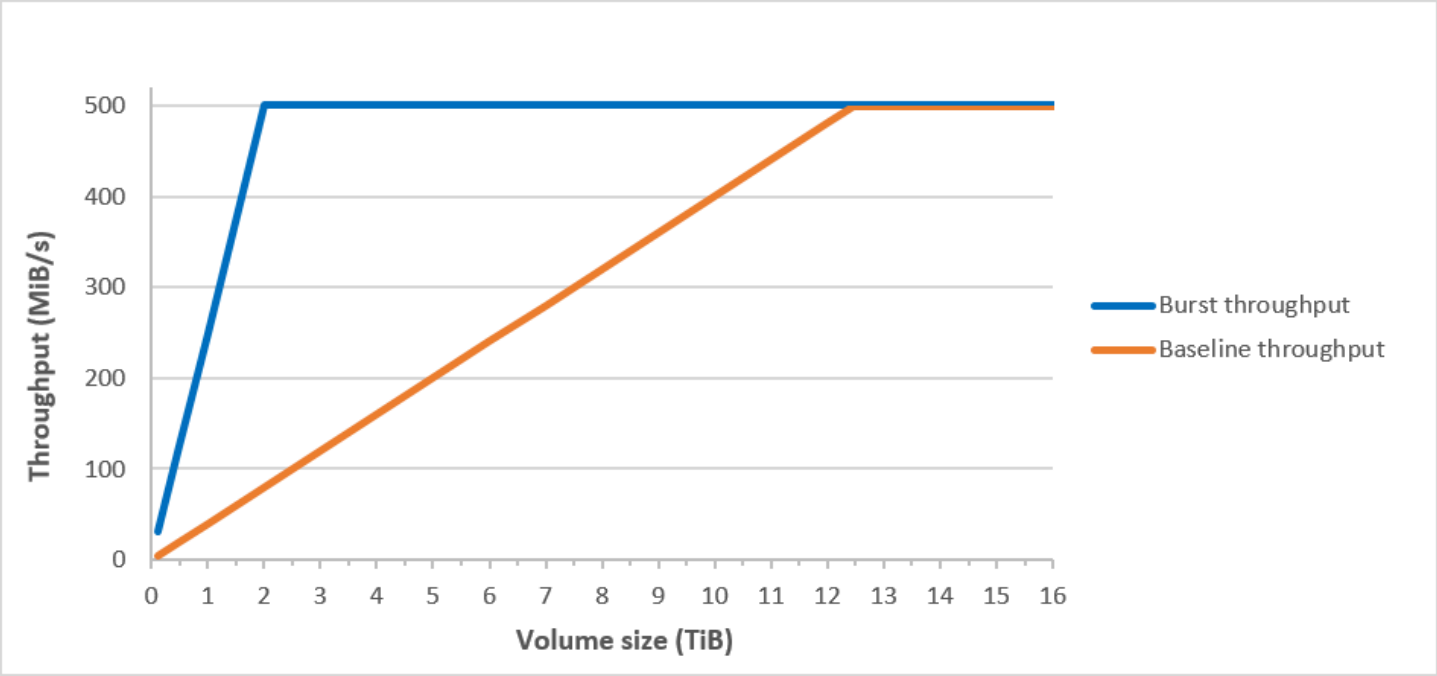
Le débit en rafale varie de 31MiB/s to a cap of 500 MiB/s, qui est atteint à 2 TiB comme suit :

```
         250 MiB/s
2 TiB × ---------- = 500 MiB/s
          1 TiB
```

Le tableau suivant indique l'ensemble des valeurs de base en matière de débit et de transmission en rafales pour `st1`.

Taille du volume (Tio)	ST1 débit de base (Mbits/s)	ST1 débit en rafale (MiB/s)
0.125	5	31
0,5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500
11	440	500
12	480	500
12,5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

Le schéma suivant illustre le tableau de valeurs sous forme de tracé :



> **Note**
>
> Lorsque vous créez un instantané d'un volume HSS à débit optimisé (`st1`), les performances peuvent diminuer jusqu'à la valeur de référence du volume pendant que l'instantané est en cours de création.

Pour plus d'informations sur l'utilisation de CloudWatch métriques et d'alarmes pour surveiller le solde de votre bucket en rafale, consultezSurveiller l'équilibre du compartiment en rafales pour les volumes.

Volumes HDD à froid

Les volumes HDD à froid (`sc1`) offrent un stockage magnétique économique qui définit les performances en termes de débit plutôt que d'IOPS. Avec une limite de débit inférieure à celle des volumes `st1`, `sc1` convient aux charges de travail séquentielles et volumineuses dont les données sont légères. Si vous n'avez pas besoin d'accéder souvent à vos données et si vous cherchez à réaliser des économies, `sc1` fournit un stockage de bloc économique. Les volumes `sc1` démarrables ne sont pas pris en charge.

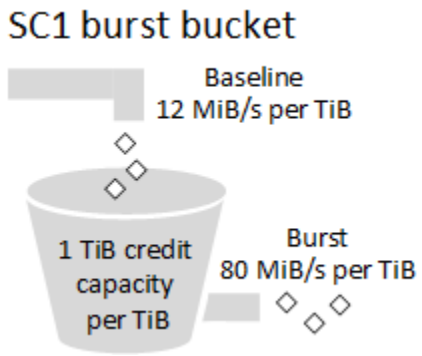
Les volumes HDD à froid (`sc1`) sont similaires aux volumes HDD à débit optimisé (`st1`), mais ils sont conçus pour prendre en charge les données consultées de manière occasionnelle.

> **Note**
>
> Ce type de volume est optimisé pour les charges de travail impliquant de grandes E/S séquentielles, et nous recommandons aux clients dont les charges de travail utilisent de petites quantités d'E/S aléatoires ou. Volumes SSD à usage général Amazon EBS Volumes SSD IOPS provisionnés par Amazon EBS Pour de plus amples informations, veuillez consulter Manque d'efficacité des lectures/écritures de petite taille sur disque dur.

Les volumes HDD à froid (`sc1`) attachés à des instances optimisées pour EBS sont conçus pour offrir des performances cohérentes, garantissant au moins 90 % des performances de débit prévues, et ce 99 % du temps au cours d'une année donnée.

Crédits de débit et performances en rafale

À l'instar de `gp2`, `sc1` utilise un modèle de transmission de compartiment en rafales pour assurer les performances. La taille du volume détermine le débit de base du volume, qui correspond à la vitesse à laquelle le volume accumule des crédits de débit. La taille du volume détermine également le débit de transmission en rafales du volume, qui correspond à la vitesse à laquelle vous pouvez utiliser des crédits lorsqu'ils sont disponibles. Les gros volumes ont un débit de base et de transmission en rafales plus élevé. Plus votre volume a de crédits, plus longtemps il est en mesure d'assurer la transmission des I/O en rafales.



Sous réserve de la limite de débit et de crédits, le débit disponible d'un volume `sc1` est exprimé par la formule suivante :

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Pour un `sc1` volume de 1 To, le débit en rafale est limité à 80MiB/s, the bucket fills with credits at 12 MiB/s, et il peut contenir jusqu'à 1 To de crédits.

Les volumes plus importants redimensionnent ces limites de manière linéaire, avec un débit plafonné à un maximum de 250 par TiB. MiB/s. After the bucket is depleted, throughput is limited to the baseline rate of 12 MiB/s

Sur des volumes allant de 0,125 TiB à 16 TiB, le débit de référence varie de MiB/s to a maximum of 192 MiB/s 1,5, qui est atteint à 16 TiB comme suit :

```
           12 MiB/s
16 TiB × ---------- = 192 MiB/s
            1 TiB
```

Le débit en rafale varie de 10MiB/s to a cap of 250 MiB/s, qui est atteint à 3,125 TiB comme suit :

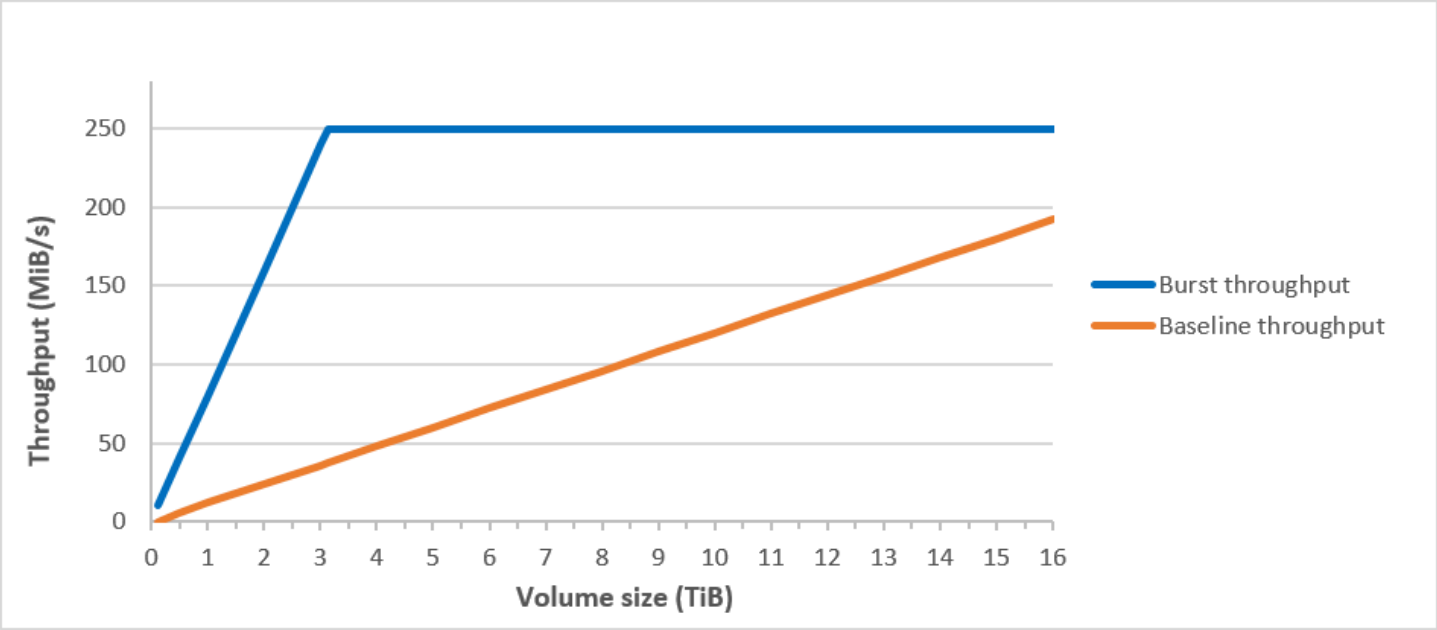
```
             80 MiB/s
3.125 TiB × ----------- = 250 MiB/s
              1 TiB
```

Le tableau suivant indique l'ensemble des valeurs de base en matière de débit et de transmission en rafales pour `sc1`:

Taille du volume (Tio)	SC1 Débit de base (Mbits/s)	SC1 Débit en rafale (Mbits/s)
0.125	1.5	10
0,5	6	40
1	12	80
2	24	160
3	36	240
3,125	37,5	250
4	48	250
5	60	250
6	72	250
7	84	250

Taille du volume (Tio)	SC1 Débit de base (Mbits/s)	SC1 Débit en rafale (Mbits/s)
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250
16	192	250

Le schéma suivant illustre le tableau de valeurs sous forme de tracé :



> **Note**
>
> Lorsque vous créez un instantané d'un volume HDD à froid (`sc1`), les performances peuvent diminuer jusqu'à la valeur de référence du volume pendant que l'instantané est en cours de création.

Pour plus d'informations sur l'utilisation de CloudWatch métriques et d'alarmes pour surveiller le solde de votre bucket en rafale, consultezSurveiller l'équilibre du compartiment en rafales pour les volumes.

Considérations relatives aux performances lors de l'utilisation de volumes HDD

Pour des performances de débit optimales avec les volumes HDD, planifiez vos charges de travail en gardant à l'esprit les éléments suivants.

Comparaison des volumes HDD à débit optimisé et des volumes HDD à froid

Les tailles de compartiment `st1` et `sc1` varient selon la taille du volume, et un compartiment complet contient assez de jetons pour une analyse complète du volume. Cependant, l'analyse des volumes `st1` et `sc1` de plus grande taille est plus longue en raison des limites de débit par instance et par volume. Les volumes attachés à des instances plus petites sont limités par le débit par instance plutôt que par les limites de débit de `st1` ou `sc1`.

`st1` et `sc1` sont conçus pour assurer l'homogénéité des performances de 90 % du débit de transmission en rafales 99 % du temps. Les périodes non conformes sont assez uniformément réparties, en ciblant 99 % du débit total attendu chaque heure.

En général, les durées d'analyse sont exprimées par cette formule :

```
 Volume size
------------ = Scan time
 Throughput
```

Par exemple, en prenant en compte les garanties en matière de cohérence des performances et les autres optimisations, un client `st1` avec un volume de 5 Tio effectue généralement une analyse complète du volume en 2,91 à 3,27 heures.

- Durée d'analyse optimale

```
   5 TiB            5 TiB
```

```
----------- = ------------------ = 10,486 seconds = 2.91 hours
 500 MiB/s     0.00047684 TiB/s
```

- Durée d'analyse maximum

```
  2.91 hours
-------------- = 3.27 hours
 (0.90)(0.99) <-- From expected performance of 90% of burst 99% of the time
```

De même, un client `sc1` avec un volume de 5 Tio effectue généralement une analyse complète du volume en 5,83 à 6,54 heures.

- Durée d'analyse optimale

```
   5 TiB             5 TiB
----------- = ------------------- = 20972 seconds = 5.83 hours
 250 MiB/s     0.000238418 TiB/s
```

- Durée d'analyse maximum

```
  5.83 hours
-------------- = 6.54 hours
 (0.90)(0.99)
```

Le tableau suivant illustre les durées d'analyse idéales pour les volumes de différentes tailles, en supposant que les compartiments sont complets et que le débit d'instance est suffisant.

Taille du volume (Tio)	ST1 durée de numérisation avec rafale (heures) *	SC1 durée de numérisation avec rafale (heures) *
1	1,17	3,64
2	1,17	3,64
3	1,75	3,64
4	2,33	4,66

Taille du volume (Tio)	ST1 durée de numérisation avec rafale (heures) *	SC1 durée de numérisation avec rafale (heures) *
5	2,91	5,83
6	3,50	6,99
7	4,08	8,16
8	4,66	9,32
9	5,24	10,49
10	5,83	11,65
11	6,41	12,82
12	6,99	13,98
13	7,57	15,15
14	8,16	16,31
15	8,74	17,48
16	9,32	18,64

* Ces durées d'analyse supposent une profondeur de file d'attente moyenne (arrondie au nombre entier le plus proche) de quatre éléments ou plus lors de l'exécution de 1 Mio d'I/O séquentielles.

Par conséquent, si vous avez une charge de travail axée sur le débit qui doit effectuer des analyses rapidement (jusqu'à 500 Mo/s) ou qui nécessite plusieurs analyses complètes de volume par jour, utilisez `st1`. Si vous cherchez à optimiser la rentabilité, si vous accédez à vos données de manière occasionnelle et si vous n'avez besoin de performances d'analyse de plus de 250 Mio/s, utilisez `sc1`.

Manque d'efficacité des lectures/écritures de petite taille sur disque dur

Le modèle de performances des volumes `st1` et `sc1` est optimisé pour les I/O séquentielles. Il favorise les charges de travail à haut débit et offre des performances acceptables avec les charges

de travail dont les IOPS et le débit varient, tout en décourageant les charges de travail avec des I/O aléatoires de petite taille.

Par exemple, une requête d'I/O de 1 Mio ou moins correspond à un crédit d'I/O de 1 Mio. Toutefois, si les I/O sont séquentielles, elles sont fusionnées dans des blocs d'I/O de 1 Mio et correspondent uniquement à un crédit d'I/O de 1 Mio.

Surveiller l'équilibre du compartiment en rafales pour les volumes

Vous pouvez surveiller le niveau du bucket en rafale `st1` et les `sc1` volumes à l'aide de la `BurstBalance` métrique Amazon EBS disponible sur Amazon CloudWatch. Cette métrique indique les crédits de débit restants pour `st1` et `sc1` dans le compartiment en rafale. Pour plus d'informations sur la `BurstBalance` métrique et les autres métriques liées aux E/S, consultezCaractéristiques et surveillance des E/S Amazon EBS. CloudWatch vous permet également de définir une alarme qui vous avertit lorsque la `BurstBalance` valeur tombe à un certain niveau. Pour plus d'informations, consultez la section Création d' CloudWatch alarmes.

Contraintes de volume Amazon EBS

La taille d'un volume Amazon EBS est limitée par la physique et l'arithmétique du stockage de données par blocs, ainsi que par les décisions de mise en œuvre des concepteurs de systèmes d'exploitation (OS) et de systèmes de fichiers. AWS impose des limites supplémentaires à la taille des volumes afin de garantir la fiabilité de ses services.

Les sections suivantes décrivent les facteurs les plus importants qui limitent la taille utilisable d'un volume EBS et fournissent des recommandations pour configurer vos volumes EBS.

Sommaire

Capacité de stockage

Le tableau suivant résume les capacités de stockage théoriques et implémentées des systèmes de fichiers les plus courants sur Amazon EBS, en supposant une taille de bloc de 4 096 octets.

Schéma de partitionnement	Nombre max de blocs adressables	Taille max théorique (blocs x taille de blocs)	Taille max implémentée Ext4*	Taille max implémentée XFS**	Taille max implémentée NTFS	Nombre max pris en charge par EBS
MBR	2^{32}	2 TiO	2 TiO	2 TiO	2 TiO	2 TiO
GPT	2^{64}	64 ZiO	1 Eio = 1024^2 Tio (50 TiB certifié) RHEL7	500 TiO (certifié le RHEL7)	256 TiO	64 TiB †

* Ext4 Howto et quelles sont les limites de taille de fichier et de système pour Red Hat Enterprise Linux ?

** Quelles sont les limites de taille de fichier et de système pour Red Hat Enterprise Linux ?

† Les volumes Block Express `io2` prennent en charge jusqu'à 64 TiB pour les partitions GPT. Pour plus d'informations, consultez Volumes SSD IOPS provisionnés (`io2`) Block Express.

Limitations de service

Amazon EBS extrait le stockage distribué massivement d'un centre de données sur des disques durs virtuels. Pour un système d'exploitation installé sur une EC2 instance, un volume EBS attaché apparaît comme un disque dur physique contenant des secteurs de 512 octets. Le système d'exploitation gère l'allocation des blocs de données (ou clusters) sur ces secteurs virtuels au moyen de ses utilitaires de gestion de stockage. L'allocation est conforme à un schéma de partitionnement de volume, comme un MBR (enregistrement de démarrage principal) ou GPT (table de partition GUID), et dans les capacités du système de fichiers installé (ext4, NTFS, etc.).

EBS n'est pas conscient des données contenues dans ses secteurs disque virtuels ; il s'assure uniquement de l'intégrité des secteurs. Cela signifie que les AWS actions et les actions du système d'exploitation sont indépendantes les unes des autres. Lorsque vous sélectionnez une taille de volume, soyez conscient des capacités et des limites de chacune, comme dans les cas suivants :

- A l'heure actuelle, la taille de volume maximal pris en charge par EBS est de 64 TiB. Cela signifie que vous pouvez créer un volume EBS pouvant atteindre 64 TiB. Toutefois, le fait que le système d'exploitation reconnaisse ou non l'ensemble de cette capacité dépend de ses propres caractéristiques de conception et de la façon dont le volume est partitionné.
- Les volumes de démarrage doivent utiliser le schéma de partitionnement MBR ou GPT. L'AMI à partir de laquelle vous lancez une instance détermine le mode de démarrage, puis le schéma de partition utilisé pour le volume de démarrage.

  Avec MBR, les volumes de démarrage sont limités à 2 TiB.

  Avec GPT, les volumes de démarrage peuvent atteindre 64 TiB lorsqu'ils sont utilisés GRUB2 avec le mode de démarrage (Linux) ou UEFI (Windows).

  Pour de plus amples informations, veuillez consulter Rendre un volume Amazon EBS disponible pour utilisation.
- Les volumes non initialisés dont la taille est supérieure ou égale à 2 TiB (2 048 GiB) doivent utiliser une table de partition GPT pour accéder à l'intégralité du volume.

Schémas de partitionnement

Parmi les autres impacts, le schéma de partitionnement détermine le nombre de blocs de données logiques pouvant être traités de manière unique sur un seul volume. Pour plus d'informations, consultez Tailles des blocs de données. Les schémas de partitionnement communs utilisés sont MBR (enregistrement de démarrage principal) et GPT (table de partition GUID). Les différences importantes entre ces schémas peuvent être résumées comme suit.

MBR

MBR utilise une structure de données 32 bits pour stocker les adresses de blocs. Autrement, chaque bloc de données est mappé à l'un des 2^{32} entiers possibles. La taille maximale adressable d'un volume est fournie par la formule suivante :

$$2^{32} \times \text{Block size}$$

La taille des blocs des volumes MBR est limitée par convention à 512 octets. Par conséquent :

$$2^{32} \times 512 \text{ bytes} = 2 \text{ TiB}$$

Les solutions d’ingénierie visant à augmenter cette limite de 2 Tio pour les volumes MBR n’ont pas été adoptées largement dans le secteur. Par conséquent, Linux et Windows ne détectent jamais qu'un volume MBR est supérieur à 2 TiB, même AWS s'il indique que sa taille est supérieure.

GPT

GPT utilise une structure de données 64 bits pour stocker les adresses de blocs. Autrement, chaque bloc de données est mappé à l’un des 2^{64} entiers possibles. La taille maximale adressable d’un volume est fournie par la formule suivante :

$$2^{64} \times \text{Block size}$$

La taille des blocs des volumes GPT est limitée communément à 4 096 octets. Par conséquent :

$$\begin{aligned} & 2^{64} \times 4{,}096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} \\ &= 2^{70} \times 2^{6} \text{ bytes} \\ &= 64 \text{ ZiB} \end{aligned}$$

Les systèmes informatiques réels ne prennent rien en charge qui atteigne ce maximum théorique. La taille du système de fichiers implémenté est actuellement limitée à 50 TiB pour ext4 et à 256 TiB pour NTFS.

Tailles des blocs de données

Le stockage de données sur un disque dur moderne est géré via l’adressage par blocs logiques, une couche d’abstraction qui permet au système d’exploitation de lire et d’écrire des données dans des blocs logiques sans bien connaître le matériel sous-jacent. Le système d'exploitation s'appuie sur le périphérique de stockage pour mapper les blocs à ses secteurs physiques, puis lit et écrit les données sur le disque à l'aide de blocs de données qui sont un multiple de la taille du secteur.

Amazon EBS annonce des secteurs physiques de 512 octets ou de 4 096 octets (4 KiB) au système d'exploitation. Amazon EBS annonce des secteurs physiques de 4 Ko uniquement si le type d' EC2 instance Amazon, le système d'exploitation et le AWS NVMe pilote le prennent en charge. Si le type d'instance, le système d'exploitation ou le AWS NVMe pilote ne prend pas en charge les secteurs physiques de 4 Ko, Amazon EBS annonce des secteurs physiques de 512 octets à la place.

Support des types d' EC2 instances Amazon

Le tableau suivant indique les tailles de secteur annoncées par Amazon EBS pour les différents types d' EC2 instances Amazon.

Taille du secteur physique annoncée	Types d'instances
512 octets	Toutes les instances basées sur Xen et les instances basées sur Nitro suivantes : • Usage général : A1 | M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6g | M6gd | Mac1 | Mac2 | T3 | T3a | T4g • Optimisé pour le calcul : C5 | C5a | C5ad | C5d | C5n | C6g | C6gd • Mémoire optimisée : R5 | R5a | R5ad | R5d | R5dn | R5n | R6g | R6gd | U-12tb1 | U-18tb1 | U-24tb1 | U-3tb1 | U-6tb1 | U-9TB1 | x2GD | X2ieZN | Z1d • Optimisées en stockage : D3 | D3en | I3en • Calcul accéléré : DI1 | G4ad | G4dn | G5 | G5g | Inf1 | P3dn | P4d | P4de | VT1
4 Kio	Toutes les autres instances basées sur Nitro

Support du système d'exploitation

Le tableau suivant indique les tailles de secteur annoncées par Amazon EBS pour certains systèmes d'exploitation courants.

> **Note**
>
> Cette liste n'est pas exhaustive. Nous vous recommandons de vérifier la taille du secteur physique annoncée par Amazon EBS dans votre système d'exploitation.

Taille du secteur physique annoncée	Operating systems
512 octets	• Amazon Linux avec noyau version 4.14 et antérieures • RHEL 7.9 et versions antérieures • Ubuntu 20.04 et versions antérieures • Windows 7 et versions antérieures • Windows Server 2008 et versions antérieures
4 Kio	• Amazon Linux avec noyau version 5.3 et ultérieure • RHEL8.8 et versions ultérieures • Ubuntu 22.04 et versions ultérieures • Windows 8 et versions ultérieures • Windows Server 2012 et versions ultérieures

AWS NVMe assistance au conducteur

Amazon EBS annonce des secteurs physiques de 4 KiB dotés de la version 1.5.1 et ultérieure AWS NVMe du pilote. Assurez-vous toujours que vous utilisez la dernière version du AWS NVMe pilote.

Tailles de bloc autres que celles par défaut

La taille par défaut du secteur pour les blocs de données logiques est actuellement de 4 KiB. Du fait que certaines charges de travail bénéficient d'une taille de taille inférieure ou supérieure, les systèmes de fichiers prennent en charge des tailles de blocs autres que par défaut et spécifiées au moment du formatage. Les scénarios dans lesquels des tailles de bloc autres que celles par défaut doivent être utilisées (comme les optimisations) ne sont pas couverts par cette documentation, mais le choix de la taille de bloc a des conséquences sur la capacité de stockage du volume. Le tableau suivant indique la capacité de stockage théorique en fonction de la taille des blocs. Cependant, gardez à l'esprit que la limite de taille de volume imposée par EBS (64 TiB pour io2 Block Express) est actuellement égale à la taille maximale autorisée par des blocs de données de 16 Ko.

Taille du bloc	Taille maximale du volume
4 Kio (par défaut)	16 TiO
8 Kio	32 Tio
16 Kio	64 Tio
32 Kio	128 Tio
64 Kio (maximum)	256 TiO

Volumes Amazon EBS et NVMe

Les volumes Amazon EBS sont exposés sous forme de NVMe blocs sur des EC2 instances Amazon basées sur le système AWS Nitro. Pour utiliser pleinement les performances et les fonctionnalités des volumes Amazon EBS exposés sous forme de périphériques en NVMe mode bloc, le AWS NVMe pilote doit être installé sur l' EC2 instance. Le AWS NVMe pilote est installé par défaut sur AMIs tous les systèmes AWS Windows et Linux de dernière génération.

Si vous utilisez une AMI qui ne possède pas le AWS NVMe pilote, vous pouvez l'installer manuellement. Pour plus d'informations, consultez la section AWS NVMe relative aux pilotes dans le guide de EC2 l'utilisateur Amazon.

Instances Linux

Les noms des appareils sont `/dev/nvme0n1`/`dev/nvme1n1`,, etc. Les noms de périphériques que vous spécifiez dans un mappage de périphériques par blocs sont renommés à l'aide de noms de NVMe périphériques (`/dev/nvme[0-26]n1`). Le pilote de périphérique en mode bloc peut attribuer des noms de NVMe périphériques dans un ordre différent de celui que vous avez spécifié pour les volumes dans le mappage de périphériques en mode bloc.

instances Windows

Lorsque vous associez un volume à votre instance, vous incluez un nom d'appareil pour le volume. Ce nom d'appareil est utilisé par Amazon EC2. Le pilote de périphérique de bloc de l'instance attribue le nom réel du volume lors du montage du volume, et le nom attribué peut être différent de celui EC2 utilisé par Amazon.

Table des matières

Associer les volumes Amazon EBS aux noms des NVMe appareils

EBS utilise la virtualisation des E/S à racine unique (SR-IOV) pour fournir des pièces jointes aux volumes sur les instances basées sur Nitro conformément à la spécification. NVMe Ces appareils s'appuient sur des NVMe pilotes standard du système d'exploitation. Habituellement, ces pilotes détectent les périphériques attachés au démarrage de l'instance, puis créent des nœuds de périphériques selon l'ordre dans lequel les périphériques répondent, et non selon la spécification des périphériques dans le mappage de périphérique de stockage en mode bloc.

Instances Linux

Sous Linux, les noms des NVMe périphériques suivent le modèle`/dev/nvme<x>n<y>`, où **<x>**est l'ordre d'énumération et, pour EBS, **<y>**est 1. Lors de démarrages consécutifs de l'instance, il arrive que les périphériques répondent à la détection dans un ordre différent, d'où un changement de nom des périphériques. En outre, le nom de périphérique attribué par le pilote de périphérique de stockage en mode bloc peut être différent du nom spécifié dans le mappage de périphérique de stockage en mode bloc.

Nous vous recommandons d'utiliser des identificateurs stables pour les volumes EBS au sein de votre instance, par exemple :

- Pour les instances basées sur Nitro, les mappages de périphériques en mode bloc spécifiés dans la EC2 console Amazon lorsque vous connectez un volume EBS `AttachVolume` ou pendant des appels d'`RunInstances`API sont capturés dans le champ de données spécifique au fournisseur de l'identification du contrôleur. NVMe Avec Amazon Linux version AMIs ultérieure à la version 2017.09.01, nous fournissons une `udev` règle qui lit ces données et crée un lien symbolique vers le mappage bloc-périphérique.
- L'ID de volume EBS et le point de montage sont stables entre les changements d'état d'instance. Le nom du NVMe périphérique peut changer en fonction de l'ordre dans lequel les périphériques répondent lors du démarrage de l'instance. Nous vous recommandons d'utiliser l'ID de volume EBS et le point de montage pour une identification cohérente des périphériques.

- NVMe L'ID du volume EBS est défini comme numéro de série dans l'identification de l'appareil pour les volumes EBS. Utilisez la commande `lsblk -o +SERIAL` pour répertorier le numéro de série.
- Le format du nom du NVMe périphérique peut varier selon que le volume EBS a été connecté pendant ou après le lancement de l'instance. NVMe les noms de périphérique pour les volumes attachés après le lancement de l'instance incluent le `/dev/` préfixe, tandis que les noms de NVMe périphérique pour les volumes attachés lors du lancement de l'instance n'incluent pas le `/dev/` préfixe.
  - Pour Amazon Linux ou FreeBSD AMI, `sudo ebsnvme-id /dev/nvme0n1 -u` utilisez la commande pour obtenir NVMe un nom d'appareil cohérent.
  - Pour les autres distributions, utilisez la `sudo nvme id-ctrl -v /dev/nvme0n1` commande pour déterminer le nom du NVMe périphérique. Vous devrez peut-être inclure l'option de `--vendor-specific` commande.
- Lors du formatage d'un périphérique, un UUID est généré, qui persiste pendant toute la durée de vie du système de fichiers. Il est possible de spécifier une étiquette de périphérique au même moment. Pour plus d'informations, consultez Rendre un volume Amazon EBS disponible pour utilisation et Démarrez à partir du mauvais volume.

Amazon Linux AMIs

Avec Amazon Linux AMI 2017.09.01 ou version ultérieure (y compris Amazon Linux 2), vous pouvez exécuter la ebsnvme-id commande comme suit pour associer le nom de l' NVMe appareil à un ID de volume et à un nom de périphérique :

L'exemple suivant illustre la commande et la sortie d'un volume attaché lors du lancement de l'instance. Notez que le nom de l' NVMe appareil n'inclut pas le `/dev/` préfixe.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
Volume ID: vol-01324f611e2463981
sda
```

L'exemple suivant illustre la commande et la sortie d'un volume attaché après le lancement de l'instance. Notez que le nom de l' NVMe appareil inclut le `/dev/` préfixe.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux crée également un lien symbolique entre le nom de l'appareil dans le mappage des périphériques en mode bloc (par exemple,`/dev/sdf`) et le nom de l' NVMe appareil.

FreeBSD AMIs

À partir de FreeBSD 12.2-RELEASE, vous pouvez exécuter la commande ebsnvme-id comme indiqué ci-dessus. Transmettez le nom du NVMe périphérique (par exemple,`nvme0`) ou le périphérique de disque (par exemple, `nvd0` ou`da0`). FreeBSD crée également des liens symboliques vers les unités de disque (par exemple,). `/dev/aws/disk/ebs/` *`volume_id`*

Autre Linux AMIs

Avec une version du noyau 4.2 ou ultérieure, vous pouvez exécuter la nvme id-ctrl commande comme suit pour mapper un NVMe périphérique à un ID de volume. Tout d'abord, installez le package en ligne de NVMe commande à l'aide des outils de gestion de packages de votre distribution Linux. `nvme-cli` Pour obtenir des instructions de téléchargement et d'installation pour d'autres distributions, reportez-vous à la documentation correspondante.

L'exemple suivant obtient l'ID du volume et le nom du NVMe périphérique d'un volume qui a été attaché lors du lancement de l'instance. Notez que le nom de l' NVMe appareil n'inclut pas le `/dev/` préfixe. Le nom du périphérique est disponible via l'extension spécifique au fournisseur du NVMe contrôleur (octets 384 : 4095 de l'identification du contrôleur) :

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme0n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : vol01234567890abcdef
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

L'exemple suivant obtient l'ID du volume et le nom du NVMe périphérique pour un volume qui a été attaché après le lancement de l'instance. Notez que le nom de l' NVMe appareil inclut le `/dev/` préfixe.

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme1n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
```

```
sn      : volabcdef01234567890
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

La commande lsblk répertorie les périphériques disponibles ainsi que leurs points de montage (le cas échéant). Vous pouvez ainsi déterminer quel nom de périphérique utiliser. Dans cet exemple, `/dev/nvme0n1p1` est monté comme périphérique racine et `/dev/nvme1n1` est attaché mais pas monté.

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:3   0  100G  0 disk
nvme0n1       259:0   0    8G  0 disk
  nvme0n1p1   259:1   0    8G  0 part /
  nvme0n1p128 259:2   0    1M  0 part
```

instances Windows

Vous pouvez exécuter la **`ebsnvme-id`** commande pour associer le numéro de disque du NVMe périphérique à un ID de volume EBS et à un nom de périphérique. Par défaut, tous les NVMe appareils EBS sont énumérés. Vous pouvez passer un numéro de disque pour énumérer des informations pour un périphérique spécifique. L'`ebsnvme-id`outil est inclus dans le dernier serveur Windows AWS fourni AMIs situé dans`C:\PROGRAMDATA\AMAZON\Tools`.

À partir du package de AWS NVMe pilotes, `1.5.0`, la dernière version de l'`ebsnvme-id`outil est installée par le package de pilotes. La dernière version n'est disponible que dans le package du pilote. Le lien de téléchargement autonome de l'outil `ebsnvme-id` ne recevra plus de mises à jour. La dernière version disponible via le lien autonome est`1.1.0`, qui peut être téléchargée à l'aide du lien ebsnvme-id.zip et en extrayant le contenu de votre EC2 instance Amazon pour y accéder. `ebsnvme-id.exe`

```
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-0d6d7ee9f6e471a7f
Device Name: sda1

Disk Number: 1
Volume ID: vol-03a26248ff39b57cf
Device Name: xvdd

Disk Number: 2
```

```
Volume ID: vol-038bd1c629aa125e6
Device Name: xvde

Disk Number: 3
Volume ID: vol-034f9d29ec0b64c89
Device Name: xvdb

Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe 4
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
```

NVMe Délai d'expiration des opérations d'E/S pour les volumes Amazon EBS

La plupart des systèmes d'exploitation spécifient un délai d'expiration pour les opérations d'E/S soumises aux NVMe appareils.

Instances Linux

Sous Linux, les volumes EBS attachés à des instances basées sur Nitro utilisent le NVMe pilote par défaut fourni par le système d'exploitation. La plupart des systèmes d'exploitation spécifient un délai d'expiration pour les opérations d'E/S soumises aux NVMe appareils. Le délai d'attente par défaut est de 30 secondes. Il peut être modifié à l'aide du paramètre de démarrage `nvme_core.io_timeout`. Pour la plupart des noyaux Linux antérieurs à la version 4.6, ce paramètre est `nvme.io_timeout`.

Si la latence des E/S dépasse la valeur de ce paramètre de délai d'attente, le NVMe pilote Linux échoue et renvoie une erreur au système de fichiers ou à l'application. Selon l'opération d'I/O, le système de fichiers ou l'application peut retenter l'erreur. Dans certains cas, il est possible de remonter le système de fichiers en lecture seule.

Pour bénéficier d'une expérience similaire à celles des volumes EBS attachés aux instances Xen, nous vous recommandons de définir `nvme_core.io_timeout` sur la valeur la plus élevée possible. Pour les noyaux actuels, le maximum est 4294967295, alors que pour les noyaux précédents, le maximum est 255. Selon la version de Linux, il se peut que la temporisation soit déjà réglée à la valeur maximale prise en charge. Par exemple, la temporisation est réglée sur 4294967295 par défaut pour les AMI Linux Amazon 2017.09.01 et ultérieures.

Vous pouvez vérifier la valeur maximale pour votre distribution de Linux en écrivant une valeur plus élevée que la valeur maximale suggérée dans `/sys/module/nvme_core/parameters/io_timeout` et en recherchant l'erreur Numerical result out of range au moment d'enregistrer le fichier.

instances Windows

Sous Windows, le délai d'expiration par défaut est de 60 secondes et le maximum est de 255 secondes. Vous pouvez modifier le paramètre de registre de classe de disque `TimeoutValue` à l'aide de la procédure décrite sur la page Registry Entries for SCSI Miniport Drivers.

NVMe Abort commande pour les volumes Amazon EBS

La `Abort` commande est une commande d' NVMe administration émise pour mettre fin à une commande spécifique précédemment soumise au contrôleur. Cette commande est généralement émise par le pilote de périphérique aux périphériques de stockage qui ont dépassé le seuil de délai d'expiration des opérations d'I/O.

Les types d' EC2 instances Amazon qui prennent en charge la `Abort` commande par défaut mettent fin à une commande spécifique précédemment soumise au contrôleur lorsqu'une `Abort` commande est émise pour les volumes Amazon EBS attachés. EC2 Les instances Amazon qui ne prennent pas en charge la `Abort` commande n'entreprennent aucune action lorsqu'une `Abort` commande est émise pour des volumes Amazon EBS attachés.

La `Abort` commande est prise en charge par :

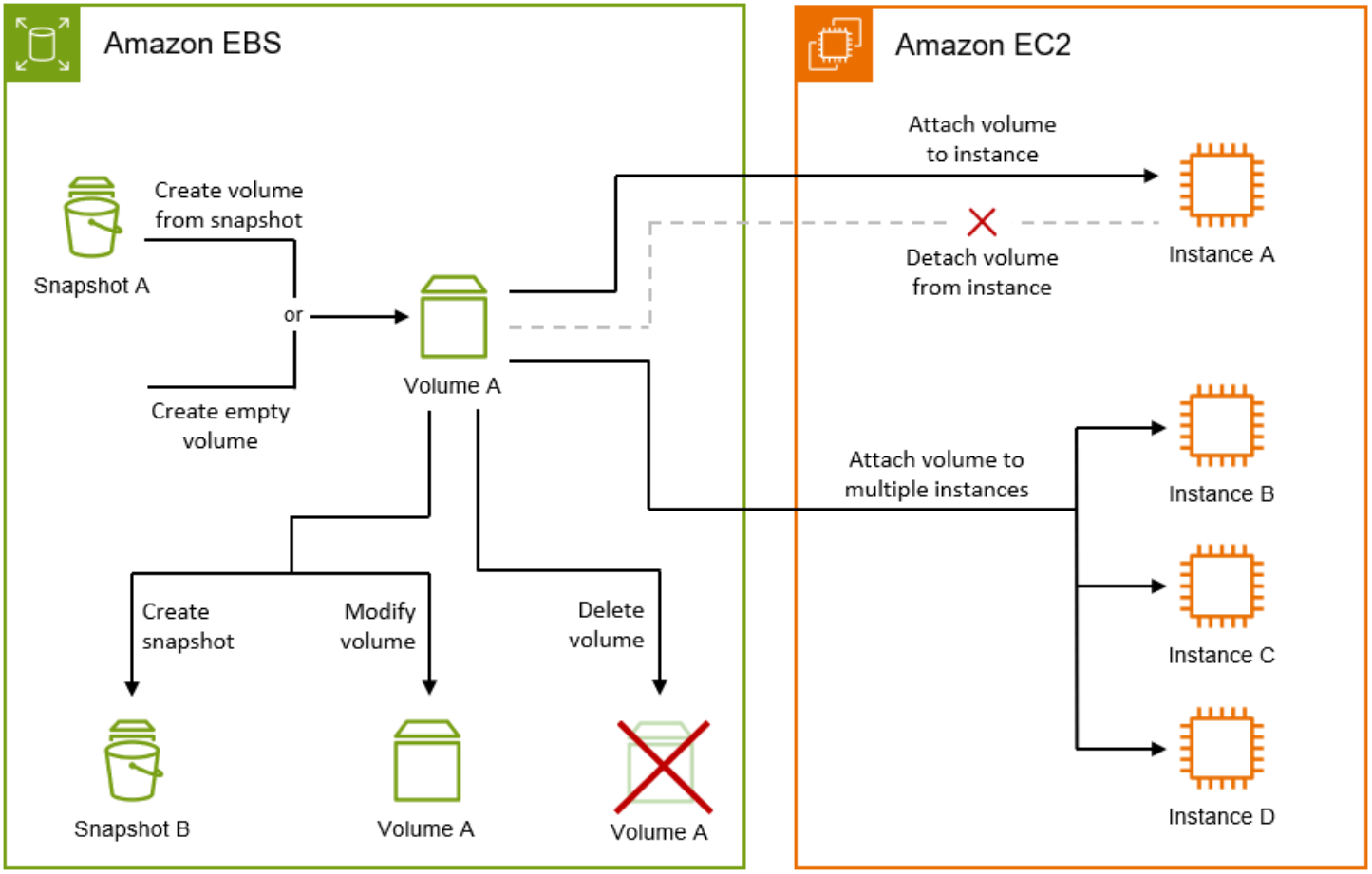
- Appareils Amazon EBS dotés de NVMe la version 1.4 ou supérieure.
- Toutes les EC2 instances Amazon, à l'exception des types d'instances basés sur Xen et des types d'instances basés sur Nitro suivants :
  - Usage général : A1 | M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6g | M6gd | Mac1 | Mac2 | T3 | T3a | T4g
  - Optimisé pour le calcul : C5 | c5a | C5ad | C5d | C5n | C6g | C6gd
  - Mémoire optimisée : R5 | R5a | R5ad | R5d | R5dn | R5n | R6g | R6gd | U-12tb1 | U-18tb1 | U-24tb1 | U-3tb1 | U-6tb1 | U-9TB1 | x2GD | X2ieZN | Z1d
  - Optimisées en stockage : D3 | D3en | I3en
  - Calcul accéléré : DL1 | G4ad | G4dn | G5 | G5g | Inf1 | P3dn | P4d | P4de | VT1

Pour plus d'informations, voir rubrique 5.1 Abort commande de la spécification de base NVM Express.

Cycle de vie des volumes Amazon EBS

Le cycle de vie d'un volume Amazon EBS commence par le processus de création. Vous pouvez créer un volume à partir d'un instantané Amazon EBS ou créer un volume vide. Avant de pouvoir utiliser votre volume, vous devez l'associer à une ou plusieurs EC2 instances Amazon situées dans la même zone de disponibilité que le volume. Vous pouvez associer plusieurs volumes à une instance. Si nécessaire, vous pouvez détacher un volume d'une instance, puis l'attacher à une autre instance. Si vos besoins en stockage changent, vous pouvez modifier la taille ou les performances du volume à tout moment. Vous pouvez créer des point-in-time sauvegardes de vos volumes en créant des instantanés Amazon EBS. Si vous n'avez plus besoin d'un volume, vous pouvez le supprimer pour ne plus avoir à supporter les coûts de stockage associés.

L'image suivante montre les actions que vous pouvez effectuer sur vos volumes dans le cadre de leur cycle de vie.



Vous pouvez également effectuer certaines tâches en vous connectant à l'instance et en exécutant une commande du système d'exploitation. Par exemple, le formatage du volume, le montage du volume, la gestion des partitions et l'affichage de l'espace disque disponible.

Tâches

- Créez un volume Amazon EBS.
- Associer un volume Amazon EBS à une instance Amazon EC2
- Associer un volume EBS à plusieurs EC2 instances à l'aide de l'option Multi-Attach
- Rendre un volume Amazon EBS disponible pour utilisation
- Afficher des informations sur un volume Amazon EBS
- Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes
- Détacher un volume Amazon EBS d'une instance Amazon EC2
- Supprimer un volume Amazon EBS

Créez un volume Amazon EBS.

Vous pouvez créer un volume Amazon EBS, puis l'associer à n'importe quelle EC2 instance de la même zone de disponibilité.

Vous pouvez soit créer un volume vide, soit créer un volume à partir d'un instantané Amazon EBS. Si vous créez un volume à partir d'un instantané, le volume commence comme une réplique exacte du volume utilisé pour créer cet instantané.

Initialisation du volume

Lorsque vous créez un volume à partir d'un instantané, les blocs de stockage de l'instantané doivent être téléchargés depuis Amazon S3 et écrits sur le volume pour que vous puissiez y accéder. Ce processus s'appelle l'initialisation du volume. Pendant ce temps, le volume subira une latence d'E/S accrue. Les performances complètes du volume sont atteintes une fois que tous les blocs de stockage ont été téléchargés et écrits sur le volume. Vous pouvez minimiser l'impact sur les performances de l'initialisation du volume en effectuant l'une des opérations suivantes :

- Utilisez un instantané activé pour une restauration rapide des instantanés. Dans ce cas, le volume est entièrement initialisé lors de sa création et fournit immédiatement des performances optimales. Pour de plus amples informations, veuillez consulter Restauration d'instantané rapide Amazon EBS.

- Initialisez manuellement le volume après sa création. Pour plus d'informations, consultez Initialiser les volumes Amazon EBS.

Les volumes vides offrent leurs performances maximales immédiatement après leur création et ne nécessitent pas d'initialisation.

Chiffrement de volume

L'état de chiffrement du volume dépend de l'activation du chiffrement par défaut sur votre compte et de l'état de chiffrement de l'instantané, si vous choisissez d'en utiliser un. Le tableau suivant récapitule les résultats de chiffrement possibles.

Chiffrement par défaut	Snapshot utilisé ?	Résultat du chiffrement des volumes	Remarque
Désactivé	Non	Chiffrement optionnel	Si vous activez le chiffrement, vous pouvez spécifier la clé KMS à utiliser. Si vous activez le chiffrement mais que vous ne spécifiez pas de clé KMS, le Clé gérée par AWS (`aws/ebs`) est utilisé.
Désactivées	Oui, non crypté	Chiffrement optionnel	Si vous activez le chiffrement, vous pouvez spécifier la clé KMS à utiliser. Si vous activez le chiffrement mais que vous ne spécifiez pas de clé KMS, le Clé gérée par AWS (`aws/ebs`) est utilisé.
Désactivées	Oui, crypté	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, le volume est chiffré à l'aide de la même clé KMS que le snapshot source.
Activées	Non	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.

Chiffrement par défaut	Snapshot utilisé ?	Résultat du chiffrement des volumes	Remarque
Activées	Oui, non crypté	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.
Activées	Oui, crypté	Chiffrement automatique	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, le volume est chiffré à l'aide de la même clé que l'instantané source (console) ou de la clé spécifiée pour le chiffrement par défaut (CLI/API).

Considérations supplémentaires

- Les volumes ne peuvent être attachés qu'à des instances situées dans la même zone de disponibilité.
- Les volumes ne sont prêts à être utilisés qu'une fois qu'ils ont atteint l'`available`état requis.
- Lorsque vous créez un volume à l'aide de la console, `gp3` c'est le type de volume par défaut. Pour les outils de ligne de commande, l'API et le SDK, `gp2` c'est le type de volume par défaut.
- Pour utiliser un volume avec une instance exécutée sur un avant-poste, vous devez créer le volume sur le même avant-poste que l'instance.
- Si vous créez un volume destiné à être utilisé avec une instance Windows et que sa taille est supérieure à 2048 GiB, assurez-vous de configurer le volume pour utiliser les tables de partition GPT. Pour plus d'informations, consultez la section Contraintes de volume Amazon EBS et le support Windows pour les disques de plus de 2 To. .
- Les volumes sont également créés indirectement en lançant une EC2 instance Amazon. L'AMI utilisée pour lancer l'instance ou la demande de lancement d'instance elle-même peut inclure des mappages de périphériques en mode bloc pour les volumes Amazon EBS. Pour plus d'informations, consultez Bloquer les mappages d'appareils.

Utilisez l'une des méthodes suivantes pour créer un volume.

Console

Pour créer un de volumes

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Volumes, puis Create volume.
3. (Clients de l'avant-poste uniquement) Pour l'ARN de l'avant-poste, entrez l'ARN de l' AWS avant-poste sur lequel vous souhaitez créer le volume.
4. Pour Volume type (Type de volume), choisissez le type de volume à créer. Pour plus d'informations sur les types de volumes disponibles, consultezTypes de volume Amazon EBS.
5. Pour Size (Taille), saisissez la taille du volume en Gio. Pour de plus amples informations, veuillez consulter Contraintes de volume Amazon EBS.
6. (Pour *io1*, *io2*, et *gp3* uniquement) Pour les IOPS, entrez le nombre maximum d'opérations d'entrée/sortie par seconde (IOPS) que le volume doit fournir.
7. (*gp3*Uniquement) Pour Débit, entrez le débit que le volume doit fournir, en Mbits/s.
8. Pour Zone de disponibilité, choisissez la zone de disponibilité dans laquelle créer le volume.
9. Pour Snapshot ID, effectuez l'une des opérations suivantes :
   - Pour créer un volume vide, conservez la valeur par défaut (Ne pas créer de volume à partir d'un instantané).
   - Pour créer le volume à partir d'un instantané, sélectionnez le cliché à utiliser.
10. (*io1*et *io2* uniquement) Pour activer le volume pour Amazon EBS Multi-Attach, sélectionnez Enable Multi-Attach. Pour plus d'informations, consultez Associer un volume EBS à plusieurs EC2 instances à l'aide de l'option Multi-Attach.
11. Définissez l'état du chiffrement du volume.
    - Si le chiffrement de votre compte est activé par défaut, le chiffrement est automatique et ne peut pas être désactivé.
    - Si vous avez sélectionné un instantané chiffré, le chiffrement est automatique et ne peut pas être désactivé.
    - Si le chiffrement de votre compte n'est pas activé par défaut et que vous sélectionnez un instantané non chiffré ou que vous n'en sélectionnez pas, le chiffrement est facultatif.
12. (Facultatif) Pour attribuer des balises personnalisées au volume, dans la section Balises, choisissez Ajouter une balise, puis entrez une clé de balise et une paire de valeurs.

13. Choisissez Créer un volume.
14. Pour utiliser le volume, attendez qu'il atteigne son `available` état, puis attachez-le à une EC2 instance Amazon située dans la même zone de disponibilité. Pour de plus amples informations, veuillez consulter Associer un volume Amazon EBS à une instance Amazon EC2 .

Command line

Pour créer un volume à l'aide du AWS CLI

Utilisez la commande create-volume.

Pour créer un volume à l'aide des outils pour Windows PowerShell

Utilisez la commande New-EC2Volume.

Associer un volume Amazon EBS à une instance Amazon EC2

Vous pouvez attacher un volume EBS disponible à l'une de vos instances se trouvant dans la même zone de disponibilité que le volume.

Pour plus d'informations sur l'ajout de volumes EBS à votre instance lors du lancement, consultez la section Mappage des périphériques par blocs d'instance.

Considérations

- Déterminez combien de volumes vous pouvez attacher à votre instance. Le nombre maximal de volumes Amazon EBS que vous pouvez associer à une instance dépend du type et de la taille de l'instance. Pour plus d'informations, consultez la section Limites de volume des instances.
- Déterminez si vous pouvez attacher votre volume à plusieurs instances et activer Multi-Attach. Pour plus d'informations, consultez Associer un volume EBS à plusieurs EC2 instances à l'aide de l'option Multi-Attach.
- Si un volume est chiffré, il ne peut être attaché qu'à une instance prenant en charge le chiffrement Amazon EBS. Pour de plus amples informations, veuillez consulter Types d'instance pris en charge.
- Si un volume possède un code AWS Marketplace produit :
  - Le volume ne peut être attaché qu'à une instance arrêtée.
  - Vous devez être abonné au AWS Marketplace code qui se trouve sur le volume.

- La configuration de l'instance, telle que son type et son système d'exploitation, doit prendre en charge ce AWS Marketplace code spécifique. Par exemple, vous ne pouvez pas prendre un volume sur une instance Windows et l'attacher à une instance Linux.
- AWS Marketplace les codes de produit sont copiés du volume vers l'instance.

Vous pouvez attacher un volume à une instance en utilisant l'une des méthodes suivantes.

Console

Pour attacher un volume EBS à une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume à attacher et choisissez Actions, Attach volume (Attacher un volume).

   > **Note**
   >
   > Vous pouvez attacher uniquement les volumes qui indiquent un état `Available`.

4. Pour Instance, saisissez l'ID de l'instance ou sélectionnez l'instance dans la liste d'options.

   > **Note**
   >
   > - Le volume doit être attaché à une instance dans la même zone de disponibilité.
   > - Si le volume est chiffré, il ne peut être attaché qu'à des types d'instance qui prennent en charge le chiffrement Amazon EBS. Pour de plus amples informations, veuillez consulter EBSChiffrement Amazon.

5. Pour Nom du périphérique, effectuez l'une des opérations suivantes :

   - Pour un volume racine, sélectionnez le nom de périphérique requis dans la section Réservé au volume racine de la liste. Généralement `/dev/sda1` ou `/dev/xvda` pour les instances Linux en fonction de l'AMI, ou `/dev/sda1` pour les instances Windows.
   - Pour les volumes de données, sélectionnez un nom de périphérique disponible dans la section Recommandé pour les volumes de données de la liste.
   - Pour utiliser un nom d'appareil personnalisé, sélectionnez Spécifier un nom d'appareil personnalisé, puis entrez le nom de l'appareil à utiliser.

Ce nom d'appareil est utilisé par Amazon EC2. Le pilote du périphérique de stockage en mode bloc de l'instance peut attribuer un nom de périphérique différent lors du montage du volume. Pour plus d'informations, voir les noms des périphériques sur les instances Linux ou les noms des périphériques pour les volumes sur EC2 les instances.

6. Choisissez Attacher un volume.
7. Connectez-vous à votre instance et montez le volume. Pour de plus amples informations, veuillez consulter Rendre un volume Amazon EBS disponible pour utilisation.

AWS CLI

Pour associer un volume EBS à une instance à l'aide du AWS CLI

Utilisez la commande attach-volume.

Tools for Windows PowerShell

Pour associer un volume EBS à une instance à l'aide des outils pour Windows PowerShell

Utilisez la commande Add-EC2Volume.

> **Note**
>
> - Si vous essayez d'attacher un nombre de volumes supérieur à la limite de volume du type d'instance, la demande échoue. Pour plus d'informations, consultez la section Limites de volume des instances.
> - Dans certaines situations, vous pouvez trouver qu'un volume autre que celui attaché à `/dev/xvda` ou `/dev/sda` est devenu le volume racine de votre instance. Cela peut arriver lorsque vous avez attaché le volume racine d'une autre instance, ou un volume créé à partir de l'instantané d'un volume racine, à une instance avec un volume racine existant. Pour plus d'informations, consultez Démarrage à partir du mauvais volume.

Associer un volume EBS à plusieurs EC2 instances à l'aide de l'option Multi-Attach

Amazon EBS Multi-Attach vous permet d'attacher un volume SSD IOPS provisionnés (`io1` ou `io2`) à plusieurs instances basées sur Nitro situées dans la même zone de disponibilité. Vous pouvez attacher plusieurs volumes activés pour Multi-Attach à une instance ou à un ensemble d'instances. Chaque instance à laquelle le volume est attaché dispose d'une autorisation complète en lecture et en écriture sur le volume partagé. Multi-Attach permet de bénéficier d'une disponibilité d'application plus importante dans les applications qui gèrent des opérations d'écriture simultanée.

Tarification et facturation

L'utilisation d'Amazon EBS Multi-Attach est disponible sans frais supplémentaires. Vous êtes facturé selon les frais standard qui s'appliquent aux volumes SSD IOPS provisionnés (`io1` et `io2`). Pour plus d'informations, consultez la section Tarification d'Amazon EBS.

Table des matières

Considérations et restrictions

- Les volumes compatibles avec l'attachement multiple peuvent être attachés à un maximum de 16 instances créées sur le système Nitro qui se trouvent dans la même zone de disponibilité.
- Les instances Linux prennent en charge l'option Multi-Attach `io1` et les `io2` volumes. Les instances Windows prennent uniquement en charge les `io2` volumes compatibles avec le mode Multi-Attach.
- Le nombre maximal de volumes Amazon EBS que vous pouvez associer à une instance dépend du type et de la taille de l'instance. Pour plus d'informations, consultez la section Limites de volume des instances.
- Multi-Attach est pris en charge exclusivement sur les volumes SSD d'IOPS provisionnés (`io1` et `io2`).

- Multi-Attach pour les volumes `io1` n'est disponible que dans les régions suivantes : USA Est (Virginie du Nord), USA Ouest (Oregon) et Asie-Pacifique (Séoul).

  Multi-Attach pour `io2` est disponible dans toutes les régions prenant en charge `io2`.

  > **Note**
  >
  > Pour améliorer les performances, la cohérence et la durabilité à moindre coût, nous vous recommandons d'utiliser des volumes `io2`.

- Les volumes `io1` compatibles Multi-Attach ne sont pas pris en charge par les instances reposant sur le système Nitro qui prennent uniquement en charge le protocole de réseaux Scalable Reliable Datagram (SRD). Pour utiliser Multi-Attach avec ces types d'instances, vous devez utiliser des volumes `io2` Block Express.
- Les systèmes de fichiers standard, tels que XFS et XFS EXT4, ne sont pas conçus pour être accessibles simultanément par plusieurs serveurs, tels que les EC2 instances. Vous devez utiliser un système de fichiers en cluster pour garantir la résilience et la fiabilité des données pour vos charges de travail de production.
- Les volumes `io2` activés pour Multi-Attach prennent en charge l'isolation d'E/S. Les protocoles d'isolation d'I/O contrôlent l'accès en écriture dans un environnement de stockage partagé afin de maintenir la cohérence des données. Vos applications doivent fournir un ordre d'écriture pour les instances attachées afin de maintenir la cohérence des données. Pour de plus amples informations, veuillez consulter Utiliser les NVMe réservations avec des volumes Amazon EBS compatibles avec Multi-Attach.

  Les volumes `io1` activés pour Multi-Attach ne prennent pas en charge l'isolation d'E/S.
- Les volumes activés pour Multi-Attach ne peuvent pas être créés en tant que volumes de démarrage.
- Les volumes activés pour Multi-Attach peuvent être attachés à un mappage de périphérique de stockage en mode bloc par instance.
- L'attachement multiple ne peut pas être activé lors du lancement de l'instance à l'aide de la EC2 console ou de l' RunInstances API Amazon.
- Les volumes activés pour Multi-Attach présentant un problème au niveau de la couche d'infrastructure Amazon EBS sont indisponibles pour toutes les instances attachées. Les problèmes au niveau d'Amazon EC2 ou de la couche réseau peuvent n'avoir d'impact que sur certaines instances associées.

- Le tableau suivant présente la prise en charge des modifications de volume pour les volumes `io1` et `io2` compatibles Multi-Attach après leur création.

	`io2`Volumes	**`io1`**Volumes
Modifier le type de volume	✗	✗
Modifier la taille du volume	✓	✗
Modifier les IOPS provisionnés	✓	✗
Activer Multi-Attach	✓ *	✗
Désactiver Multi-Attach	✓ *	✗

  * Vous ne pouvez pas activer ou désactiver Multi-Attach lorsque le volume est attaché à une instance.

- Les volumes activés pour Multi-Attach sont supprimés lors de la résiliation de l'instance si la dernière instance attachée est interrompue et si cette instance est configurée pour supprimer le volume lors de la résiliation. Si le volume est attaché à plusieurs instances présentant des paramètres de suppression à la résiliation différents dans leurs mappages de périphérique de stockage en mode bloc, le paramètre de mappage de périphériques de bloc de la dernière instance attachée détermine le comportement de suppression à la résiliation.

  Pour garantir un comportement prévisible en matière de suppression à la résiliation, activez ou désactivez la suppression à la résiliation pour toutes les instances auxquelles le volume est attaché. Pour plus d'informations, consultez la section Préserver les données lorsqu'une instance est mise hors service.

- Vous pouvez surveiller un volume activé par connexion multiple à l'aide CloudWatch des métriques pour les volumes Amazon EBS. Les données sont agrégées dans toutes les instances attachées.

Vous ne pouvez pas surveiller les métriques pour des instances individuelles attachées. Pour de plus amples informations, veuillez consulter CloudWatch Métriques Amazon pour Amazon EBS.

Performances pour les volumes Amazon EBS à connexion multiple

Chaque instance attachée est capable de piloter ses performances IOPS maximales jusqu'aux performances provisionnées maximales du volume. Toutefois, les performances agrégées de toutes les instances attachées ne peuvent pas dépasser les performances provisionnées maximales du volume. Si la demande d'IOPS des instances attachées est supérieure aux IOPS provisionnées du volume, le volume ne dépassera pas ses performances provisionnées.

Par exemple, supposons que vous créez un volume `io2` activé pour Multi-Attach avec `80,000` IOPS provisionnés et que vous l'attachez à une instance `m7g.large` qui prend en charge jusqu'à `40,000` IOPS et à une instance `r7g.12xlarge` qui prend en charge jusqu'à `60,000` IOPS. Chaque instance peut gérer ses IOPS maximum car la valeur est inférieure aux IOPS provisionnés () du volum `80,000`. Toutefois, si les deux instances conduisent simultanément des I/O vers le volume, leurs I/O par seconde combinées ne peuvent pas dépasser les performances provisionnées du volume de `80,000` IOPS.

Pour obtenir des performances cohérentes, il est recommandé d'équilibrer les I/O basées sur les instances attachées parmi les secteurs d'un volume activé pour Multi-Attach.

Pour plus d'informations sur les performances IOPS pour les types d' EC2 instances Amazon, consultez les types d'instances optimisés Amazon EBS dans le guide de EC2 l'utilisateur Amazon.

Activer l'attache multiple pour un volume Amazon EBS

Les volumes activés pour Multi-Attach peuvent être gérés de la même manière que n'importe quel autre volume Amazon EBS. Toutefois, pour utiliser la fonctionnalité Multi-Attach, vous devez l'activer pour le volume. Lorsque vous créez un volume, Multi-Attach est désactivé par défaut.

Après avoir créé un volume activé pour l'attache multiple, vous pouvez l'attacher à une instance de la même manière que vous attachez n'importe quel autre volume EBS. Pour de plus amples informations, veuillez consulter Associer un volume Amazon EBS à une instance Amazon EC2 .

Vous pouvez activer Multi-Attach lors de la création de volumes. Utilisez l'une des méthodes suivantes.

Console

Pour activer Multi-Attach lors de la création du volume

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Choisissez Créer un volume.
4. Pour Type de volume, sélectionnez SSD IOPS provisionnés (**io1**) ou SSD IOPS provisionnés (**io2**).
5. Pour Size (Taille) et IOPS, choisissez la taille de volume requise et le nombre d'I/O par seconde à provisionner.
6. Pour Availability Zone (Zone de disponibilité), choisissez la même zone de disponibilité que celle dans laquelle se trouvent les instances.
7. Pour Amazon EBS Multi-Attach, choisissez Enable Multi-Attach (Activer Multi-Attach).
8. (Facultatif) Pour Snapshot ID (ID d'instantané), choisissez l'instantané à partir duquel créer le volume.
9. Définissez l'état du chiffrement du volume.

   Si l'instantané sélectionné est chiffré, ou si votre compte est activé pour le chiffrement par défaut, le chiffrement est activé automatiquement et vous ne pouvez pas le désactiver. Vous pouvez choisir la clé KMS à utiliser pour chiffrer le volume.

   Si l'instantané sélectionné n'est pas chiffré et que le chiffrement par défaut n'est pas activé pour votre compte, le chiffrement est facultatif. Pour chiffrer le volume, pour Encryption (Chiffrement), choisissez Encrypt this volume (Chiffrer ce volume), puis sélectionnez la clé KMS à utiliser pour chiffrer le volume.

   > **Note**
   >
   > Vous ne pouvez attacher des volumes chiffrés qu'aux instances qui prennent en charge le chiffrement Amazon EBS. Pour de plus amples informations, veuillez consulter EBSChiffrement Amazon.

10. (Facultatif) Pour attribuer des balises personnalisées au volume, dans la section Balises, choisissez Ajouter une balise, puis entrez une clé de balise et une paire de valeurs.
11. Choisissez Créer un volume.

Command line

Pour activer Multi-Attach lors de la création du volume

Utilisez la commande create-volume et spécifiez le paramètre `--multi-attach-enabled`.

```
$ C:\> aws ec2 create-volume --volume-type io2 --multi-attach-enabled --size 100 --
iops 2000 --region us-west-2 --availability-zone us-west-2b
```

Vous pouvez également activer l'option Multi-Attach pour les volumes `io2` après leur création, mais uniquement s'ils ne sont attachés à aucune instance.

> **Note**
>
> Vous ne pouvez pas activer Multi-Attach pour les volumes `io1` après leur création.

Utilisez l'une des méthodes suivantes pour activer Multi-Attach pour un volume `io2` après la création.

Console

Pour activer Multi-Attach après la création

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume, puis Actions et Modify volume (Modifier un volume).
4. Pour Amazon EBS Multi-Attach, choisissez Enable Multi-Attach (Activer Multi-Attach).
5. Sélectionnez Modify.

Command line

Pour activer Multi-Attach après la création

Utilisez la commande modify-volume et spécifiez le paramètre `--multi-attach-enabled`.

```
$ C:\> aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --multi-attach-
enabled
```

Désactiver l'attache multiple pour un volume Amazon EBS

Vous ne pouvez désactiver Multi-Attach pour un volume `io2` que si celui-ci n'est attaché à pas plus d'une instance.

> **Note**
>
> Vous ne pouvez pas désactiver Multi-Attach pour les volumes `io1` après leur création.

Utilisez l'une des méthodes suivantes pour désactiver Multi-Attach pour un volume `io2`.

Console

Pour désactiver Multi-Attach après la création

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume, puis Actions et Modify volume (Modifier un volume).
4. Pour Amazon EBS Multi-Attach, désactivez Enable Multi-Attach (Activer Multi-Attach).
5. Sélectionnez Modify.

Command line

Pour désactiver Multi-Attach après la création

Utilisez la commande modify-volume et spécifiez le paramètre `-no-multi-attach-enabled`.

```
$ C:\> aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --no-multi-attach-
enabled
```

Utiliser les NVMe réservations avec des volumes Amazon EBS compatibles avec Multi-Attach

`io2`Les volumes compatibles avec Multi-Attach prennent en charge les NVMe réservations, qui sont un ensemble de protocoles de clôture de stockage conformes aux normes du secteur. Ces protocoles vous permettent de créer et de gérer des réservations qui contrôlent et coordonnent l'accès de

plusieurs instances à un volume partagé. Les réservations sont utilisées par les applications de stockage partagé pour garantir la cohérence des données.

Rubriques

Prérequis

NVMe les réservations sont prises en charge uniquement avec les `io2` volumes compatibles avec le mode Multi-Attach. Les volumes compatibles Multi-Attach ne peuvent être attachés qu'aux instances construites sur le Système Nitro.

NVMe les réservations sont prises en charge avec les systèmes d'exploitation suivants :

- SUSE Linux Enterprise 12 SP3 et versions ultérieures
- RHEL 8.3 et versions ultérieures
- Amazon Linux 2 et versions ultérieures
- Windows Server 2016 et versions ultérieures

> **Note**
>
> Pour les serveurs Windows pris en charge AMIs datés du 2023.09.13 et versions ultérieures, les NVMe pilotes requis sont inclus. Pour les versions antérieures AMIs, vous devez effectuer la mise à jour vers la version 1.5.0 ou ultérieure du NVMe pilote. Pour plus d'informations, consultez la section AWS NVMe Conducteurs.

Si vous utilisez EC2 Launch v2 pour initialiser vos disques, vous devez passer à la version 2.0.1521 ou ultérieure. Pour plus d'informations, voir Utiliser l'agent EC2 Launch v2.

Activation de l'assistance pour les NVMe réservations

Support pour les NVMe réservations est activé par défaut pour tous les `io2` volumes dotés de l'option Multi-Attach créés après le 18 septembre 2023.

Pour activer la prise en charge des NVMe réservations pour les `io2` volumes existants créés avant le 18 septembre 2023, vous devez détacher toutes les instances du volume, puis rattacher les instances requises. Les NVMe réservations seront activées pour toutes les pièces jointes créées après le détachement de toutes les instances.

Commandes de NVMe réservation prises en charge

Amazon EBS prend en charge les commandes de NVMe réservation suivantes :

Reservation Register

Enregistre, annule ou remplace une clé de réservation. Une clé d'enregistrement est utilisée pour identifier et authentifier une instance. L'enregistrement d'une clé de réservation auprès d'un volume crée une association entre l'instance et le volume. Vous devez enregistrer l'instance auprès du volume pour qu'elle puisse obtenir une réservation.

Reservation Acquire

Acquiert une réservation sur un volume, anticipe une réservation enregistrée sur un espace de noms et annule une réservation enregistrée sur un volume. Les types de réservation suivants peuvent être acquis :

- Réservation Write Exclusive
- Réservation Excusive Access
- Réservation Write Exclusive - Registrants Only
- Réservation Exclusive Access - Registrants Only
- Réservation Write Exclusive - All Registrants
- Réservation Exclusive Access - All Registrants

Reservation Release

Publie ou efface une réservation enregistrée sur un volume.

Reservation Report

Décrit le statut d'enregistrement et de réservation d'un volume.

Tarification

L'activation et l'utilisation de Multi-Attach est disponible sans frais supplémentaires.

Rendre un volume Amazon EBS disponible pour utilisation

Une fois que vous avez attaché un volume Amazon EBS à votre instance, il est exposé en tant que périphérique en mode bloc. Vous pouvez formater le volume avec n'importe quel système de fichiers puis le monter. Après avoir rendu le volume EBS disponible à l'utilisation, vous pouvez y accéder de la même façon que n'importe quel volume. Toutes les données inscrites sur ce système de fichiers le sont sur le volume EBS et sont transparentes pour les applications utilisant cet appareil.

Vous pouvez prendre des instantanés de votre volume EBS à des fins de sauvegarde ou pour servir de base à la création d'un autre volume. Pour de plus amples informations, veuillez consulter Instantanés Amazon EBS.

Si le volume EBS que vous préparez à utiliser est supérieur à 2 Tio, vous devez utiliser un schéma de partitionnement GPT pour accéder à l'ensemble du volume. Pour de plus amples informations, veuillez consulter Contraintes de volume Amazon EBS.

Instances Linux

Formatage et montage d'un volume attaché

Supposons que vous disposiez d'une EC2 instance avec un volume EBS pour le périphérique racine et que vous veniez d'attacher un volume EBS vide à l'instance en utilisant. `/dev/xvda` `/dev/sdf` Utilisez la procédure suivante pour mettre le volume nouvellement attaché à disposition.

Pour formater et monter un volume EBS sous Linux

1. Connectez-vous à votre instance à l'aide de SSH. Pour plus d'informations, consultez Connect to your Linux instance.
2. Le périphérique peut être attaché à l'instance avec un nom de périphérique différent de celui que vous avez spécifié dans le mappage de périphérique de stockage en mode bloc. Pour plus d'informations, consultez les noms des appareils sur les instances Linux. Utilisez la commande lsblk pour voir vos périphériques de disques disponibles et leurs points de montage (le cas échéant) pour vous aider à déterminer quel nom d'appareil utiliser. Le résultat de lsblk supprime le préfixe `/dev/` des chemins d'accès complets à l'appareil.

   Voici un exemple de sortie pour une instance basée sur le système Nitro, qui expose les volumes EBS sous forme NVMe de périphériques en mode bloc. Le périphérique racine est `/dev/nvme0n1`, et il possède deux partitions nommées `nvme0n1p1` et `nvme0n1p128`. Le volume attaché est `/dev/nvme1n1`, et il ne dispose pas de partition ni n'est encore monté.

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  10G  0 disk
nvme0n1       259:1    0   8G  0 disk
-nvme0n1p1    259:2    0   8G  0 part /
-nvme0n1p128  259:3    0   1M  0 part
```

L'exemple ci-dessous représente la sortie pour une instance T2. Le périphérique racine est `/dev/xvda`, et il possède une partition nommée `xvda1`. Le volume attaché est `/dev/xvdf`, et il ne dispose pas de partition ni n'est encore monté.

```
[ec2-user ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0    8G  0 disk
-xvda1  202:1    0    8G  0 part /
xvdf    202:80   0   10G  0 disk
```

3. Déterminez s'il y a un système de fichiers sur le volume. Les nouveaux volumes sont des périphériques de stockage en mode bloc bruts et vous devez créer un système de fichiers sur ces volumes avant de pouvoir les monter et les utiliser. Les volumes créés à partir d'instantanés disposent probablement déjà d'un système de fichiers. Si vous créez un autre système de fichiers par-dessus le système de fichiers existant, l'opération remplace vos données.

   Utilisez l'une des méthodes suivantes ou les deux pour déterminer s'il existe un système de fichiers sur le volume :

   - Utilisez la commande file -s pour obtenir les informations sur un appareil spécifique, telles que son type de système de fichiers. Si le résultat de la commande précédente est simplement `data`, comme dans l'exemple de sortie suivant, il n'y a pas de système de fichiers sur l'appareil.

     ```
     [ec2-user ~]$ sudo file -s /dev/xvdf
     /dev/xvdf: data
     ```

     Si l'appareil possède un système de fichiers, la commande affiche des informations sur le type de système de fichiers. Par exemple, la sortie suivante montre un périphérique racine avec le système de fichiers XFS.

```
[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

- Utilisez la commande lsblk -f pour obtenir des informations sur tous les appareils attachés à l'instance.

  ```
  [ec2-user ~]$ sudo lsblk -f
  ```

  Par exemple, la sortie suivante montre qu'il y a trois appareils attachés aux instances —nvme1n1, nvme0n1, et nvme2n1. La première colonne répertorie les appareils et leurs partitions. La colonne FSTYPE indique le type de système de fichiers pour chaque appareil. Si la colonne est vide pour un appareil spécifique, cela signifie qu'il n'a pas de système de fichiers. Dans ce cas, l'appreil nvme1n1 et la partition nvme0n1p1 sur l'appareil nvme0n1 sont tous deux formatés à l'aide du système de fichiers XFS, tandis que l'appareil nvme2n1 et la partition nvme0n1p128 sur l'appareil nvme0n1 ne disposent pas de systèmes de fichiers.

  ```
  NAME  FSTYPE LABEL UUID      MOUNTPOINT
  nvme1n1         xfs  7f939f28-6dcc-4315-8c42-6806080b94dd
  nvme0n1
  ##nvme0n1p1 xfs     / 90e29211-2de8-4967-b0fb-16f51a6e464c         /
  ##nvme0n1p128
  nvme2n1
  ```

  Si la sortie de ces commandes montre qu'il n'y a pas de système de fichiers sur l'appareil, vous devez en créer un.

4. (Condition) Si vous avez découvert qu'il y a un système de fichiers sur le périphérique à l'étape précédente, ignorez cette étape. Si vous avez un volume vide, utilisez la commande mkfs -t pour créer un système de fichiers sur le volume.

   > **Warning**
   >
   > N'utilisez pas cette commande si vous montez un volume qui contient déjà des données (par exemple, un volume qui a été créé à partir d'un instantané). Sinon, vous formaterez le volume et supprimerez les données existantes.

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
```

Si vous obtenez une erreur indiquant que `mkfs.xfs` est introuvable, utilisez la commande suivante pour installer les outils XFS, puis répétez la commande précédente :

```
[ec2-user ~]$ sudo yum install xfsprogs
```

5. Utilisez la commande mkdir pour créer un répertoire de point de montage pour le volume. Le point de montage est l'endroit où se trouve le volume dans l'arborescence du système de fichiers et où vous lisez et écrivez des fichiers après avoir monté le volume. L'exemple suivant crée un répertoire nommé `/data`.

   ```
   [ec2-user ~]$ sudo mkdir /data
   ```

6. Montez le volume ou la partition dans le répertoire du point de montage que vous avez créé à l'étape précédente.

   Si le volume ne comporte aucune partition, utilisez la commande suivante et spécifiez le nom du périphérique pour monter l'ensemble du volume.

   ```
   [ec2-user ~]$ sudo mount /dev/xvdf /data
   ```

   Si le volume comporte des partitions, utilisez la commande suivante et spécifiez le nom de la partition pour monter une partition.

   ```
   [ec2-user ~]$ sudo mount /dev/xvdf1 /data
   ```

7. Vérifiez les autorisations sur les fichiers de votre nouveau montage de volume pour vous assurer que les utilisateurs et les applications peuvent écrire sur le volume. Pour plus d'informations sur les autorisations sur les fichiers, consultez File security dans Le projet de documentation Linux.
8. Le point de montage n'est pas automatiquement préservé après le redémarrage de votre instance. Pour monter automatiquement ce volume EBS après le redémarrage, suivez la procédure suivante.

Monter automatiquement un volume attaché après le redémarrage

Pour monter un volume EBS attaché à chaque redémarrage du système, ajoutez une entrée pour l'appareil dans le fichier `/etc/fstab`.

Vous pouvez utiliser le nom du périphérique, comme `/dev/xvdf`, dans `/etc/fstab`, mais nous recommandons d'utiliser plutôt l'identificateur universel unique (UUID) de 128 bits de l'appareil. Les noms de périphériques peuvent changer, mais l'UUID persiste pendant toute la durée de vie de la partition. En utilisant l'UUID, vous réduisez les risques que le système devienne impossible à démarrer après une reconfiguration du matériel. Pour plus d'informations, consultez Associer les volumes Amazon EBS aux noms des NVMe appareils.

Pour monter automatiquement un volume attaché après le redémarrage

1. (Facultatif) Créez une sauvegarde de votre fichier `/etc/fstab` que vous pouvez utiliser si vous détruisez ou supprimez accidentellement ce fichier en l'éditant.

   ```
   [ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
   ```

2. Utilisez la commande blkid pour trouver l'UUID du périphérique. Notez l'UUID du périphérique que vous souhaitez monter après le redémarrage. Vous en aurez besoin à l'étape suivante.

   Par exemple, la commande suivante indique que deux périphériques sont montés sur l'instance, et elle indique le UUIDs pour les deux périphériques.

   ```
   [ec2-user ~]$ sudo blkid
   /dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
    PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
   /dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
   ```

   Pour Ubuntu 18.04, utilisez la commande lsblk.

   ```
   [ec2-user ~]$ sudo lsblk -o +UUID
   ```

3. Ouvrez le fichier `/etc/fstab` avec un éditeur de texte tel que nano ou vim.

   ```
   [ec2-user ~]$ sudo vim /etc/fstab
   ```

4. Ajoutez l'entrée suivante à `/etc/fstab` pour monter le périphérique au point de montage spécifié. Les champs sont la valeur UUID renvoyée par blkid (ou lsblk pour Ubuntu 18.04), le

point de montage, le système de fichiers et les options de montage recommandées. Pour plus d'informations sur les champs obligatoires, exécutez `man fstab` pour ouvrir le manuel fstab.

Dans l'exemple suivant, nous montons le périphérique doté de l'UUID `aebf131c-6957-451e-8d34-ec978d9581ae` sur le point de montage `/data` et nous utilisons le système de fichiers `xfs`. Nous utilisons également les indicateurs `defaults` et `nofail`. Nous spécifions `0` pour empêcher le vidage du système de fichiers et 2 pour indiquer qu'il s'agit d'un périphérique non racine.

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae  /data  xfs  defaults,nofail  0  2
```

> **Note**
>
> Si jamais vous démarrez votre instance sans ce volume attaché (par exemple, après avoir déplacé ce volume sur une autre instance), l'option de montage `nofail` permet à l'instance de démarrer même si des erreurs se produisent lors du montage du volume. Les dérivés Debian, y compris les versions Ubuntu antérieures à 16.04, doivent également ajouter l'option de montage `nobootwait`.

5. Pour vérifier que votre entrée fonctionne, exécutez les commandes suivantes pour démonter le périphérique, puis montez tous les systèmes de fichiers dans `/etc/fstab`. S'il n'y a pas d'erreur, le fichier `/etc/fstab` est correct et votre système de fichiers sera monté automatiquement après avoir été redémarré.

```
[ec2-user ~]$ sudo umount /data
[ec2-user ~]$ sudo mount -a
```

Si vous recevez un message d'erreur, traitez les erreurs dans le fichier.

> **Warning**
>
> Des erreurs dans le fichier `/etc/fstab` peuvent rendre un système impossible à démarrer. N'arrêtez pas un système dont le fichier `/etc/fstab` contient des erreurs.

Si vous n'êtes pas sûr de savoir comment corriger des erreurs dans `/etc/fstab` et que vous avez créé un fichier de sauvegarde lors de la première étape de la procédure, vous avez toujours

la possibilité de restaurer votre fichier depuis votre fichier de sauvegarde avec la commande suivante.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

instances Windows

Utilisez l'une des méthodes suivantes pour rendre un volume disponible sur une instance Windows.

PowerShell

Pour que tous les volumes EBS contenant des partitions brutes puissent être utilisés avec Windows PowerShell

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez Connect to your Windows instance.
2. Dans la barre des tâches, ouvrez le menu Démarrer, puis choisissez Windows PowerShell.
3. Utilisez la série de PowerShell commandes Windows fournie dans l' PowerShell invite ouverte. Le script effectue les actions suivantes par défaut :
   1. Arrête le HWDetection service Shell.
   2. Énumère les disques sur lesquels le style de partition est brut.
   3. Crée une nouvelle partition qui couvre la taille maximale prise en charge par le disque et le type de partition.
   4. Attribue une lettre de lecteur disponible.
   5. Formate le système de fichiers en NTFS avec l'étiquette de système de fichiers spécifiée.
   6. Redémarre le HWDetection service Shell.

```
Stop-Service -Name ShellHWDetection
Get-Disk | Where PartitionStyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
 -PassThru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -
FileSystem NTFS -NewFileSystemLabel "Volume Label" -Confirm:$false
Start-Service -Name ShellHWDetection
```

DiskPart command line tool

Pour mettre un volume EBS à la disposition de l'utilisateur avec l'outil de ligne de DiskPart commande

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez Connect to your Windows instance.
2. Déterminez le numéro de disque que vous souhaitez rendre disponible :
    1. Ouvrez le menu Démarrer, puis sélectionnez Windows PowerShell.
    2. Utilisez `Get-Disk` Cmdlet de commande pour récupérer une liste de disques disponibles.
    3. Dans la sortie de la commande, notez laNumérocorrespondant au disque que vous rendez disponible.
3. Créez un fichier de script pour exécuter DiskPart des commandes :
    1. Ouvrez le menu Démarrer et sélectionnezExplorer de fichiers.
    2. Accédez à un répertoire, tel que C:\, pour stocker le fichier de script.
    3. Choisissez ou cliquez avec le bouton droit sur un espace vide dans le dossier pour ouvrir la boîte de dialogue, positionnez le curseur surNouvellepour accéder au menu contextuel, puis choisissezDocument texte.
    4. Nommez le fichier texte `diskpart.txt`.
4. Ajoutez les commandes suivantes au fichier script. Vous devrez peut-être modifier le numéro de disque, le type de partition, l'étiquette du volume et la lettre du lecteur. Le script effectue les actions suivantes par défaut :
    1. Sélectionne le disque 1 pour modification.
    2. Configure le volume pour utiliser la structure de partition MBR (Master Boot Record).
    3. Formate le volume sous la forme d'un volume NTFS.
    4. Définit l'étiquette du volume.
    5. Attribue au volume une lettre de lecteur.

    > **Warning**
    >
    > Si vous montez un volume sur lequel se trouvent déjà des données, ne le reformatez pas, sinon vous supprimerez les données existantes.

```
select disk 1
attributes disk clear readonly
online disk noerr
convert mbr
create partition primary
format quick fs=ntfs label="volume_label"
assign letter="drive_letter"
```

Pour plus d'informations, consultez DiskPart Syntaxe et paramètres.

5. Ouvrez une invite de commande, accédez au dossier dans lequel se trouve le script et exécutez la commande suivante pour rendre un volume disponible sur le disque spécifié :

```
C:\> diskpart /s diskpart.txt
```

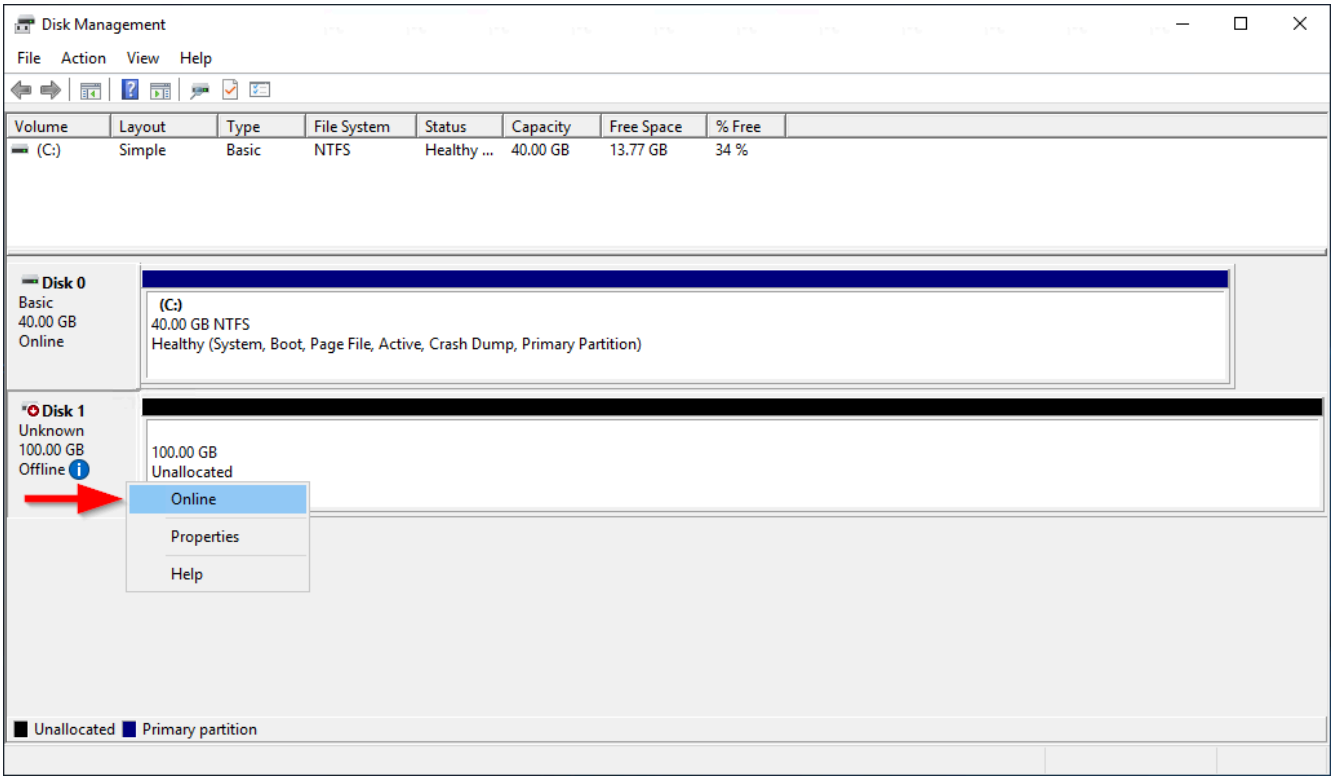
Disk Management utility

Pour rendre un volume EBS disponible à l'utilisation à l'aide de l'utilitaire Gestion des disques

1. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance. Pour plus d'informations, consultez Connect to your Windows instance.
2. Démarrez l'utilitaire Gestion des disques. Dans la barre des tâches, ouvrez le menu contextuel (via un clic droit) du logo Windows et choisissez Gestion des disques.

> **Note**
>
> Sur Windows Server 2008, sélectionnez Démarrer, Outils d'administration, Gestion des ordinateurs et Gestion des disques.

3. Mettez le volume en ligne. Dans le volet inférieur, ouvrez le menu contextuel (avec un clic droit) du panneau de gauche associé au disque du volume EBS. Sélectionnez En ligne.

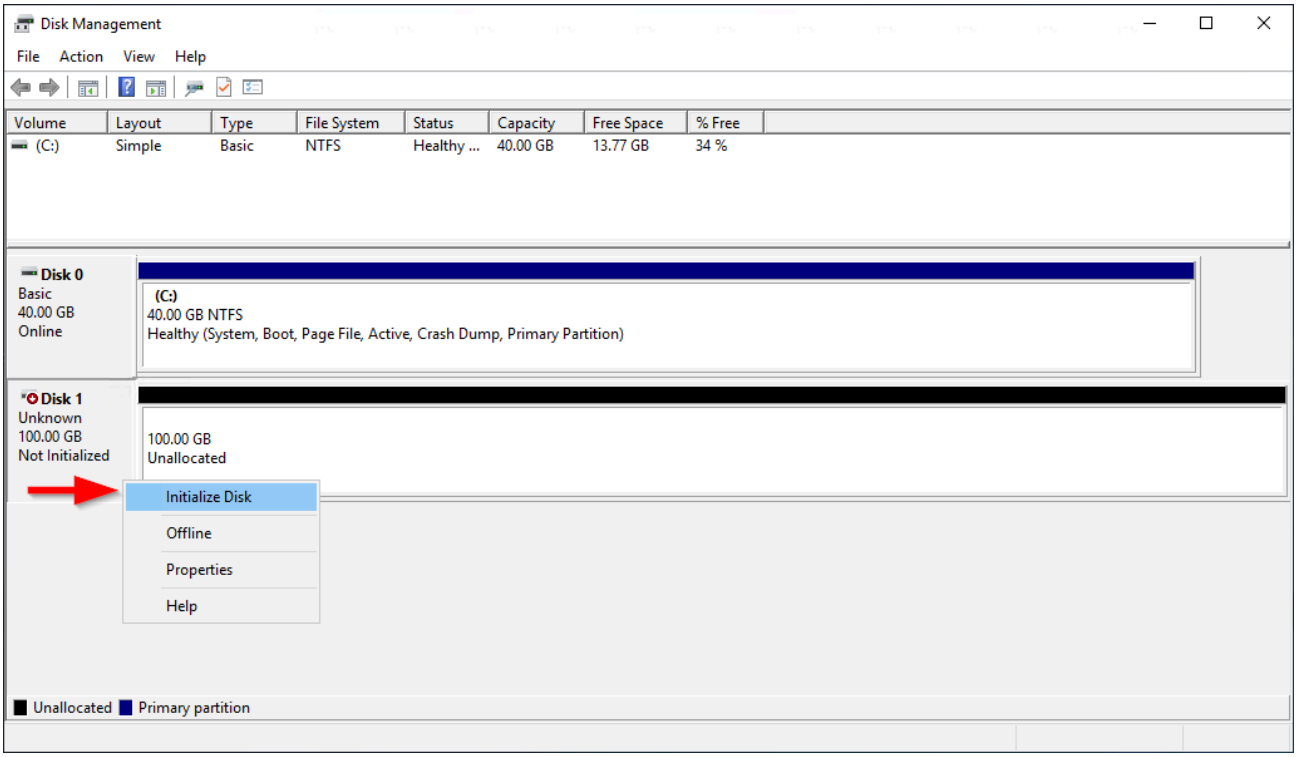


4. (Condition) Si le disque n'est pas initialisé, vous devez l'initialiser avant de pouvoir l'utiliser. Si le disque est déjà initialisé, ignorez cette étape.

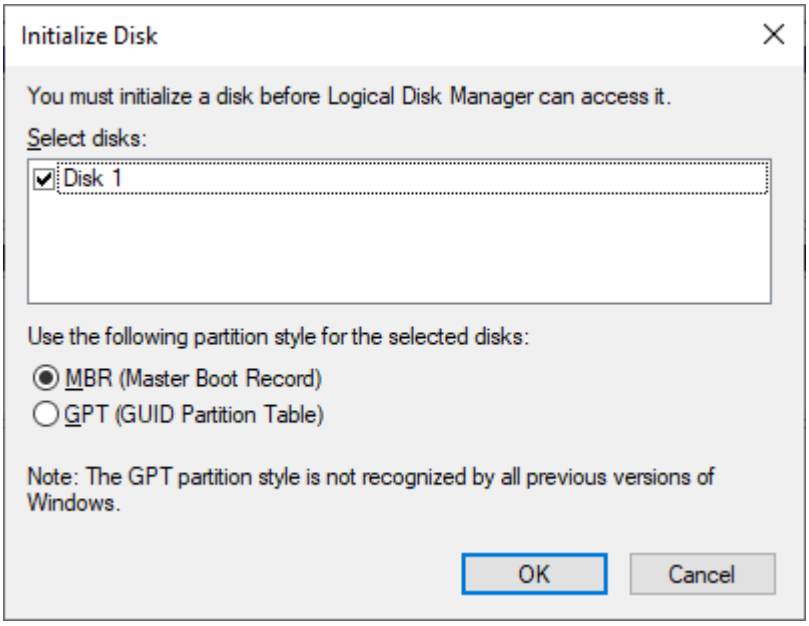
> **Warning**
>
> Si vous montez un volume sur lequel se trouvent déjà des données (par exemple, un ensemble de données public ou un volume créé à partir d'un instantané), ne le reformatez pas. Vous risqueriez de supprimer les données existantes.

Si le disque n'est pas initialisé, lancez-le comme suit :

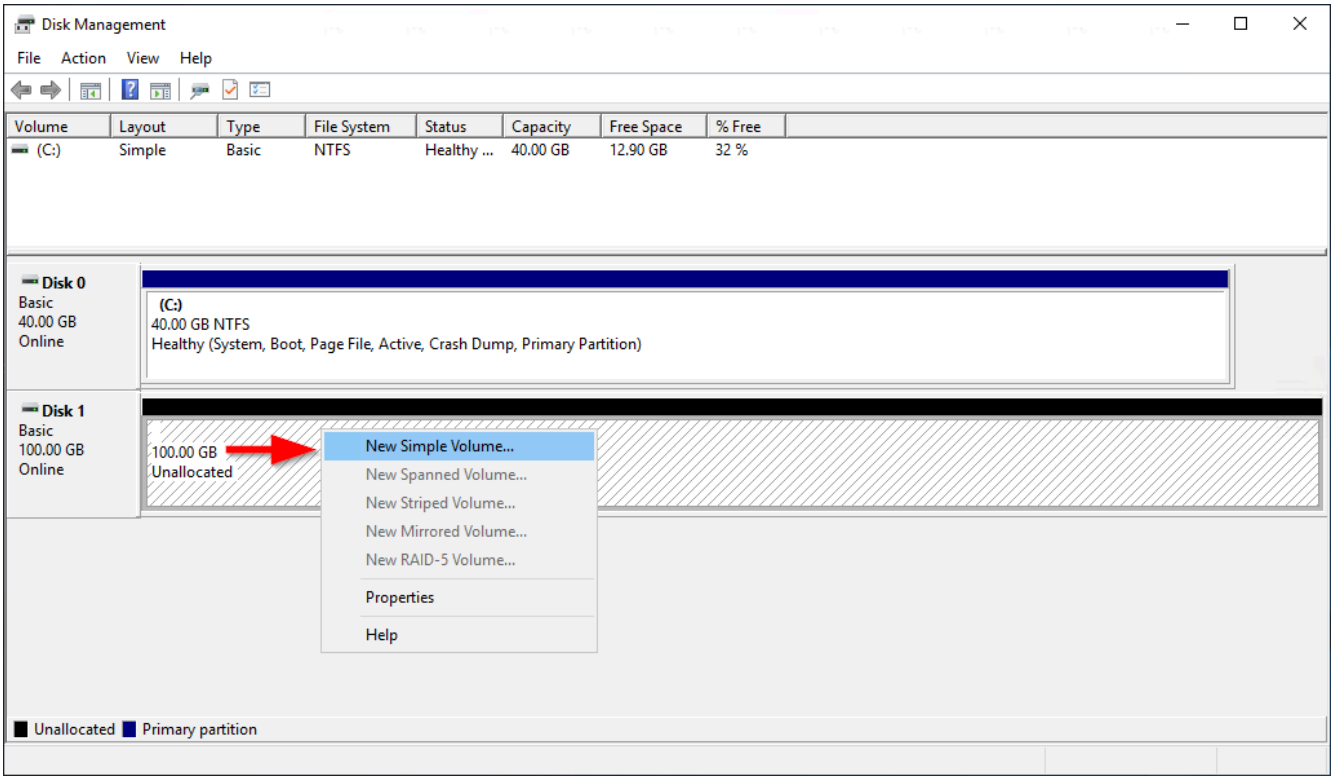
1. Ouvrez le menu contextuel (clic droit) du panneau de gauche du disque, et choisissez Initialiser le disque.



2. Dans la boîte de dialogue Initialiser le disque, sélectionnez un style de partition, puis appuyez sur OK.

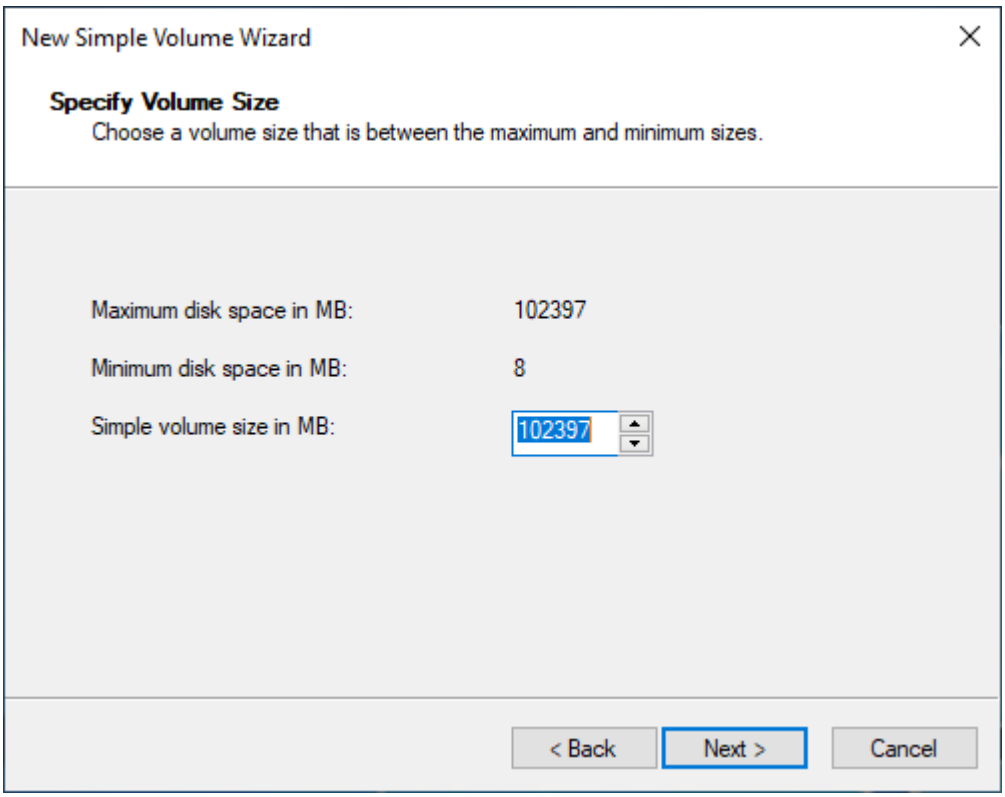


5. Ouvrez le menu contextuel (clic droit) du volet de droite du disque, puis appuyez sur Nouveau volume simple.

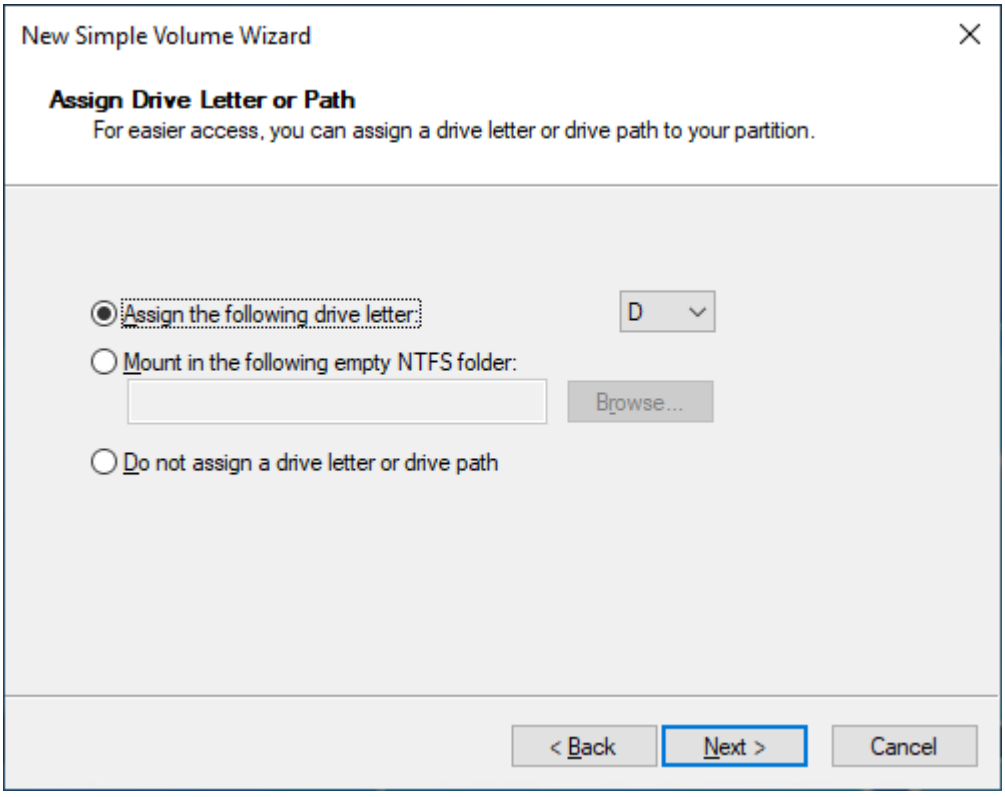


6. DansAssistant Nouveau volume simple, choisissezSuivant.

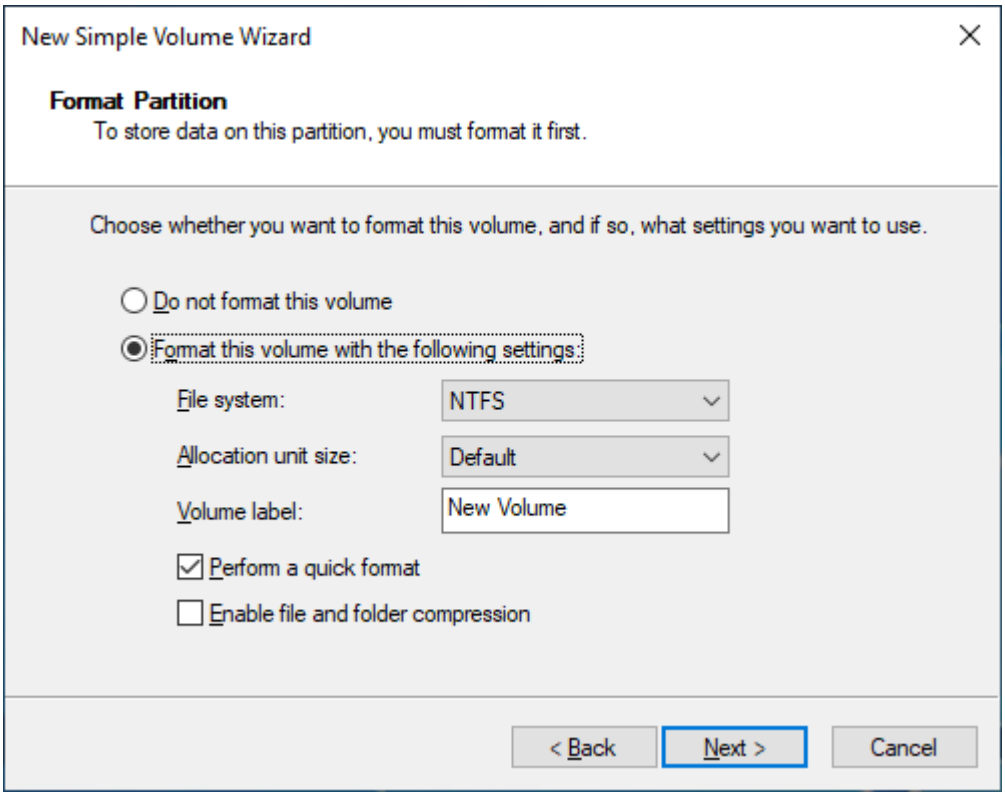
7. Si vous souhaitez modifier la valeur maximale par défaut, spécifiez la valeurTaille simple du volume en Mo, puis choisissezSuivant.



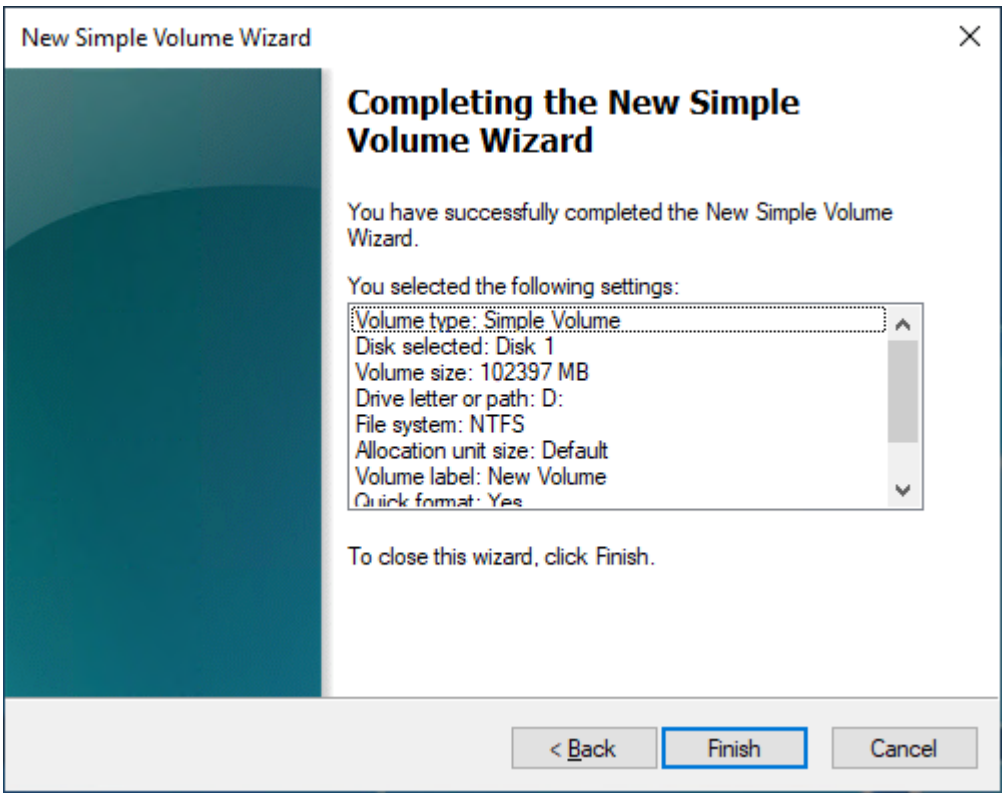
8. Spécifiez une lettre de lecteur préférée, si nécessaire, dans le menu déroulantAttribuez la lettre de lecteur suivante, puis choisissezSuivant.



9. Spécifiez uneÉtiquette du volumeet réglez les paramètres par défaut, le cas échéant, puis choisissezSuivant.



10. Vérifiez vos paramètres, puis choisissezTerminerpour appliquer les modifications et fermer l'Assistant Création d'un volume simple.



Afficher des informations sur un volume Amazon EBS

Vous pouvez visualiser les informations descriptives relatives à vos volumes EBS. Par exemple, vous pouvez afficher des informations sur tous les volumes d'une région spécifique ou des informations détaillées sur un seul volume, notamment sa taille, son type de volume, si le volume est chiffré, la clé KMS utilisée pour chiffrer le volume et l'instance spécifique à laquelle le volume est attaché.

Vous pouvez obtenir des informations supplémentaires sur vos volumes EBS, telles que l'espace disque disponible, à partir du système d'exploitation sur l'instance.

Rubriques

- Afficher des informations sur un volume
- États du volume
- Afficher les métriques de volume
- Afficher l'espace disque disponible

Afficher des informations sur un volume

Vous pouvez afficher des informations sur un volume en utilisant l'une des méthodes suivantes.

Console

Pour afficher des informations sur un volume à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Pour réduire la liste, vous pouvez filtrer vos volumes à l'aide des identifications et des attributs de volume. Choisissez le champ de filtre, sélectionnez une identification ou un attribut de volume, puis sélectionnez la valeur du filtre.
4. Pour afficher des informations supplémentaires sur un volume, sélectionnez son ID.

Pour afficher les volumes EBS qui sont attachés à une instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Instances.
3. Sélectionnez l'instance.
4. Dans l'onglet Storage (Stockage), la section Block devices (Périphériques de bloc) répertorie les volumes attachés à l'instance. Pour afficher des informations sur un volume spécifique, choisissez son ID dans la colonne Volume ID (ID du volume).

Amazon EC2 Global View

Vous pouvez utiliser Amazon EC2 Global View pour consulter vos volumes dans toutes les régions pour lesquelles votre AWS compte est activé. Pour plus d'informations, consultez Amazon EC2 Global View.

AWS CLI

Pour consulter les informations relatives à un volume EBS à l'aide du AWS CLI

Utilisez la commande describe-volumes.

Tools for Windows PowerShell

Pour afficher les informations relatives à un volume EBS à l'aide des Outils pour Windows PowerShell

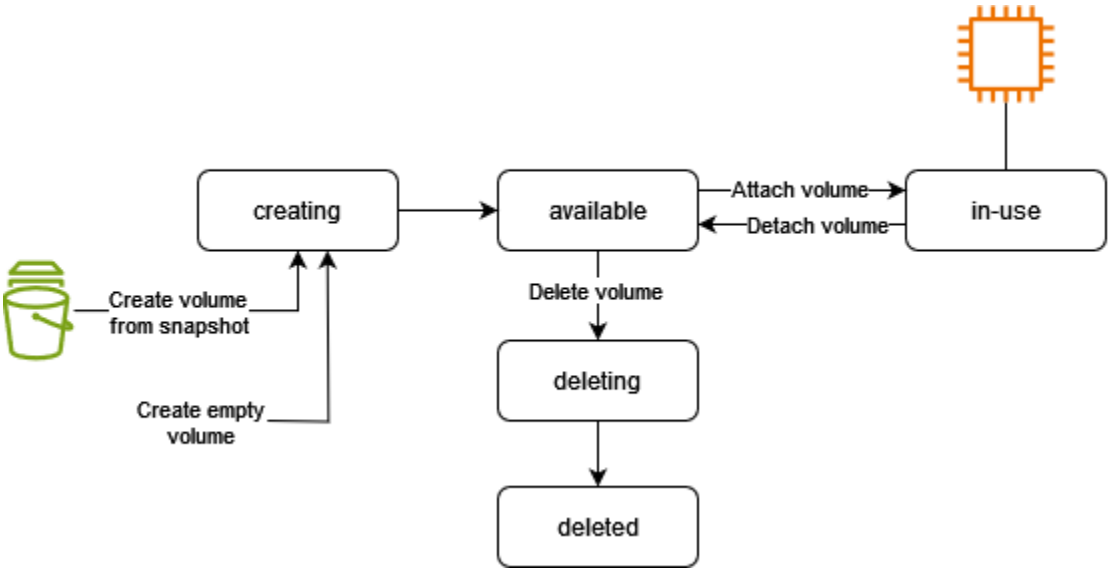
Utilisez la commande Get-EC2Volume.

États du volume

L'état du volume décrit la disponibilité d'un volume Amazon EBS. Vous pouvez consulter l'état du volume dans la colonne État de la page Volumes de la console ou à l'aide de la commande describe-volumes AWS CLI .

Un volume Amazon EBS passe par différents états entre le moment où il est créé et celui où il est supprimé.

L'illustration suivante montre les transitions entre les états de volume. Vous pouvez créer un volume à partir d'un instantané Amazon EBS ou créer un volume vide. Lorsque vous créez un volume, celui-ci passe à l'`creating`état. Une fois que le volume est prêt à être utilisé, il entre dans l'`available`état. Vous pouvez associer un volume disponible à une instance située dans la même zone de disponibilité que le volume. Vous devez détacher le volume avant de l'associer à une autre instance ou de le supprimer. Vous pouvez supprimer un volume lorsque vous n'en avez plus besoin.



Le tableau suivant récapitule les états des volumes.

État	Description
`creating`	Le volume est en cours de création.
`available`	Le volume n'est pas attaché à une instance.

État	Description
`in-use`	Le volume est attaché à une instance.
`deleting`	Le volume est en cours de suppression.
`deleted`	Le volume est supprimé.
`error`	Le matériel sous-jacent associé à votre volume EBS a échoué et les données associées au volume ne peuvent pas être récupérées. Pour plus d'informations sur la façon de restaurer le volume ou de récupérer les données qu'il contient, voir Pourquoi mon volume EBS a-t-il le statut « erreur » ? .

Afficher les métriques de volume

Vous pouvez obtenir des informations supplémentaires sur vos volumes EBS auprès d'Amazon CloudWatch. Pour de plus amples informations, veuillez consulter CloudWatch Métriques Amazon pour Amazon EBS.

Afficher l'espace disque disponible

Vous pouvez obtenir des informations supplémentaires sur vos volumes EBS, telles que l'espace disque disponible, à partir du système d'exploitation sur l'instance.

Instances Linux

Utilisez la commande suivante :

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/xvda1     xfs       8.0G  1.2G  6.9G  15% /
```

instances Windows

Vous pouvez afficher l'espace disque disponible en ouvrant l'explorateur de fichiers et en sélectionnant Ce PC.

Vous pouvez également afficher l'espace disque disponible en utilisant la commande `dir` suivante et en examinant la dernière ligne de la sortie :

```
C:\> dir C:
 Volume in drive C has no label.
 Volume Serial Number is 68C3-8081

 Directory of C:\

03/25/2018  02:10 AM    <DIR>          .
03/25/2018  02:10 AM    <DIR>          ..
03/25/2018  03:47 AM    <DIR>          Contacts
03/25/2018  03:47 AM    <DIR>          Desktop
03/25/2018  03:47 AM    <DIR>          Documents
03/25/2018  03:47 AM    <DIR>          Downloads
03/25/2018  03:47 AM    <DIR>          Favorites
03/25/2018  03:47 AM    <DIR>          Links
03/25/2018  03:47 AM    <DIR>          Music
03/25/2018  03:47 AM    <DIR>          Pictures
03/25/2018  03:47 AM    <DIR>          Saved Games
03/25/2018  03:47 AM    <DIR>          Searches
03/25/2018  03:47 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  18,113,662,976 bytes free
```

Vous pouvez également afficher l'espace disque disponible en utilisant la commande `fsutil` suivante :

```
C:\> fsutil volume diskfree C:
Total # of free bytes        : 18113204224
Total # of bytes             : 32210153472
Total # of avail free bytes  : 18113204224
```

> **Tip**
>
> Vous pouvez également utiliser l' CloudWatch agent pour collecter des métriques d'utilisation de l'espace disque à partir d'une EC2 instance Amazon sans vous connecter à l'instance. Pour plus d'informations, consultez les sections Création du fichier de configuration de l' CloudWatch agent et Installation de l' CloudWatch agent dans le guide de CloudWatch l'utilisateur Amazon. Si vous devez surveiller l'utilisation de l'espace disque pour plusieurs instances, vous pouvez installer et configurer l' CloudWatch agent sur ces instances à l'aide de Systems Manager. Pour plus d'informations, consultez la section Installation de l' CloudWatch agent à l'aide de Systems Manager.

Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes

Amazon EBS Elastic Volumes vous permet d'augmenter la taille du volume, de changer le type de volume ou d'ajuster les performances de vos volumes EBS. Si votre instance prend en charge Elastic Volumes, vous pouvez procéder sans détacher le volume ni redémarrer l'instance. Cela vous permet de continuer à utiliser votre application pendant que les modifications prennent effet.

Aucuns frais supplémentaires ne sont facturés pour modifier la configuration d'un volume. La configuration du nouveau volume vous est facturée une fois que la modification du volume a commencé. Pour plus d'informations, consultez la page Tarification d'Amazon EBS.

Table des matières

Limites

- Il existe des limites au stockage agrégé maximal qui peut être demandé pour les modifications de volume. Pour plus d'informations, consultez Quotas du service Amazon EBS dans le Référence générale d'Amazon Web Services.
- Après avoir modifié un volume, vous devez attendre au moins six heures et veiller à ce que le volume soit à l'état `in-use` ou `available` avant de pouvoir le modifier.
- La modification d'un volume EBS peut prendre quelques minutes à quelques heures, selon les modifications de configuration appliquées. La modification d'un volume EBS d'une taille de 1 Tio peut prendre jusqu'à six heures. Cependant, le même volume peut nécessiter 24 heures ou plus dans d'autres situations. Le temps nécessaire à la modification des volumes n'évolue pas toujours de manière linéaire. Par conséquent, un volume plus important peut prendre moins de temps, et un volume plus petit peut prendre plus de temps.
- Si vous recevez un message d'erreur lorsque vous tentez de modifier un volume EBS ou que vous êtes sur le point de modifier un volume EBS attaché à un type d'instance de la génération précédente, effectuez l'une des actions suivantes :

  - Pour un volume non-racine, détachez le volume de l'instance, appliquez les modifications, puis attachez à nouveau le volume.
  - Pour un volume racine, arrêtez l'instance, appliquez les modifications, puis redémarrez l'instance.
- La durée de modification est augmentée pour les volumes qui ne sont pas entièrement initialisés. Pour plus d'informations, consultez Initialiser les volumes Amazon EBS.
- La nouvelle taille de volume ne peut pas dépasser la capacité prise en charge de son système de fichiers et de son schéma de partitionnement. Pour plus d'informations, consultez Contraintes de volume Amazon EBS.
- Si vous modifiez le type d'un volume, la taille et les performances doivent s'inscrire dans les limites du type de volume cible. Pour plus d'informations, consultez Types de volume Amazon EBS.
- Vous ne pouvez pas réduire la taille d'un volume EBS. Cependant, vous pouvez créer un volume plus petit, puis y faire migrer vos données à l'aide d'un outil au niveau de l'application tel que rsync (instances Linux) ou robocopy (instances Windows).
- `io2`les volumes attachés aux instances basées sur le système Nitro prennent en charge des tailles allant jusqu'à 64 TiB et des IOPS allant jusqu'à 256 000 IOPS. `io2`les volumes attachés à d'autres instances prennent en charge des tailles allant jusqu'à 16 TiB et des IOPS allant jusqu'à 64 000, mais peuvent atteindre des performances allant jusqu'à 32 000 IOPS uniquement.
- Vous ne pouvez pas modifier le type des volumes `io2` activés pour Multi-Attach.
- Vous ne pouvez pas modifier le type de volume, la taille ou les IOPS approvisionnés de volumes `io1` activés pour Multi-Attach.
- Un volume racine de type`io1`,`io2`,`gp2`,`gp3`, ou `standard` ne peut pas être modifié en volume `st1` ou `sc1`, même s'il est détaché de l'instance.
- Si le volume a été attaché avant le 3 novembre 2016 à 23 h 40 UTC, vous devez initialiser la prise en charge d'Elastic Volumes. Pour plus d'informations, consultez Initialisation de la prise en charge d'Elastic Volumes.
- Alors que les instances `m3.medium` prennent pleinement en charge la modification du volume, `m3.large`, `m3.xlarge`, et `m3.2xlarge` peuvent ne pas prendre en charge toutes les fonctionnalités de modification de volume.

Exigences relatives aux modifications de volume Amazon EBS

Les exigences et les limites suivantes s'appliquent lorsque vous modifiez un volume Amazon EBS. Pour en savoir plus sur les exigences générales des volumes EBS, consultez Contraintes de volume Amazon EBS.

Rubriques

- Types d'instance pris en charge
- Système d'exploitation

Types d'instance pris en charge

Elastic Volumes est pris en charge sur les instances suivantes :

- Toutes les instances de la génération actuelle
- Les instances de génération précédente suivantes : C1, C3, C4, G2, I2, M1, M3, M4, R3, and R4

Si votre type d'instance ne prend pas en charge Elastic Volumes, consultez Modifier un volume EBS si Elastic Volumes n'est pas pris en charge.

Système d'exploitation

Les exigences de système d'exploitation suivantes s'appliquent :

Linux

Linux AMIs nécessite une table de partition GUID (GPT) et GRUB 2 pour les volumes de démarrage de 2 TiB (2 048 GiB) ou plus. De AMIs nos jours, de nombreux Linux utilisent encore le schéma de partitionnement MBR, qui ne prend en charge que des tailles de volume de démarrage allant jusqu'à 2 TiB. Si votre instance ne démarre pas avec un volume de démarrage supérieur à 2 Tio, l'AMI que vous utilisez peut être limitée à une taille de volume de démarrage inférieure à 2 Tio. Les volumes autres que ceux de démarrage ne sont pas soumis à cette restriction sur les instances Linux.

Avant de redimensionner un volume de démarrage avec une capacité de plus de 2 Tio, vous pouvez déterminer si le volume utilise un partitionnement MBR ou GPT en exécutant la commande suivante sur votre instance :

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

Une instance Amazon Linux avec un partitionnement GPT renvoie les informations suivantes :

```
GPT fdisk (gdisk) version 0.8.10

  Partition table scan:
    MBR: protective
    BSD: not present
    APM: not present
    GPT: present

  Found valid GPT with protective MBR; using GPT.
```

Une instance SUSE avec un partitionnement MBR renvoie les informations suivantes :

```
GPT fdisk (gdisk) version 0.8.8

  Partition table scan:
    MBR: MBR only
    BSD: not present
    APM: not present
    GPT: not present
```

Windows

Par défaut, Windows initialise les volumes avec une table de partition MBR (Master Boot Record). Comme MBR prend uniquement en charge les volumes dont la taille est inférieure à 2 Tio (2 048 Gio), Windows vous empêche de redimensionner les volumes MBR au-delà de cette limite. Dans ce cas, l'option Extend Volume (Étendre le volume) est désactivée dans l'utilitaire Windows Gestion des disques. Si vous utilisez le AWS Management Console ou AWS CLI pour créer un volume partitionné MBR dont la taille dépasse la limite de taille, Windows ne peut ni détecter ni utiliser l'espace supplémentaire.

Pour contourner cette limite, vous pouvez créer un nouveau volume plus grand avec une table de partition GUID (GPT) et y copier les données du volume MBR d'origine.

Pour créer un volume GPT

1. Créez un nouveau volume vide de la taille souhaitée dans la zone de disponibilité de l' EC2instance et attachez-le à votre instance.

> **Note**
>
> Le nouveau volume ne doit pas être un volume restauré à partir d'un instantané.

2. Connectez-vous au système Windows et ouvrez Gestion des disques (diskmgmt.exe).
3. Ouvrez le menu contextuel (clic droit) pour le disque et choisissez En ligne.
4. Dans la fenêtre Initialiser le disque, sélectionnez le nouveau disque et choisissez Partition GPT (GUID Partition Table), puis OK.
5. Lorsque l'initialisation est terminée, copiez les données du volume d'origine vers le nouveau volume à l'aide d'un outil comme robocopy ou teracopy.
6. Dans Gestion des disques, modifiez les lettres des lecteurs avec les valeurs correspondantes et déconnectez l'ancien volume.
7. Dans la EC2 console Amazon, détachez l'ancien volume de l'instance, redémarrez l'instance pour vérifier qu'elle fonctionne correctement, puis supprimez l'ancien volume.

Demander des modifications de volume Amazon EBS

Avec Elastic Volumes, vous pouvez augmenter de manière dynamique la taille, les performances et le type de vos volumes Amazon EBS sans les détacher.

Utilisez le processus suivant lors de la modification d'un volume :

1. (Facultatif) Avant de modifier un volume contenant des données importantes, une bonne pratique consiste à créer un instantané du volume au cas où vous auriez besoin d'annuler vos modifications. Pour plus d'informations, consultez Créer des instantanés Amazon EBS.
2. Demandez la modification du volume.
3. Surveillez la progression de la modification du volume. Pour plus d'informations, consultez Surveillez la progression des modifications des volumes Amazon EBS.
4. Si la taille du volume a été modifiée, étendez le système de fichiers du volume pour tirer parti de la capacité de stockage accrue. Pour de plus amples informations, veuillez consulter Étendre le système de fichiers après le redimensionnement d'un volume Amazon EBS.

Sommaire

- Modifier un volume EBS si Elastic Volumes n'est pas pris en charge
- Initialiser la prise en charge d'Elastic Volumes (si nécessaire)

Modifier un volume EBS à l'aide d'Elastic Volumes

Considérations

Gardez les points suivants à l'esprit lorsque vous modifiez des volumes :

- Après avoir modifié un volume, vous devez attendre au moins six heures et veiller à ce que le volume soit à l'état `in-use` ou `available` avant de pouvoir le modifier.
- La modification d'un volume EBS peut prendre quelques minutes à quelques heures, selon les modifications de configuration appliquées. La modification d'un volume EBS d'une taille de 1 Tio peut prendre jusqu'à six heures. Cependant, le même volume peut nécessiter 24 heures ou plus dans d'autres situations. Le temps nécessaire à la modification des volumes n'évolue pas toujours de manière linéaire. Par conséquent, un volume plus important peut prendre moins de temps, et un volume plus petit peut prendre plus de temps.
- Vous ne pouvez pas annuler une demande de modification de volume une fois qu'elle a été envoyée.
- Vous pouvez uniquement augmenter la taille du volume. Vous ne pouvez pas réduire la taille d'un volume.
- Vous pouvez augmenter ou diminuer les performances du volume.
- Si vous ne modifiez pas le type de volume, les modifications de taille et de performances du volume doivent s'inscrire dans les limites du type de volume actuel. Si vous modifiez le type de volume, les modifications de taille et de performances du volume doivent respecter les limites du type de volume cible.
- Si vous modifiez le type de volume de gp2 pour gp3, et que vous ne spécifiez pas les performances d'IOPS ou de débit, Amazon EBS fournit automatiquement des performances équivalentes à celles de la source gp2 volume ou référence gp3 performance, la valeur la plus élevée étant retenue.

  Par exemple, si vous modifiez un fichier de 500 GB gp2 volume avec un débit de 250 Mo/s et 1,500 IOPS vers gp3 sans spécifier les performances d'IOPS ou de débit, Amazon EBS met automatiquement en service le volume gp3 avec 3 000 IOPS (référence) IOPS gp3) et 250 Mo/s (pour correspondre à la sourcegp2 débit volumique).

Pour modifier un volume EBS, utilisez l'une des méthodes suivantes.

Console

Pour modifier un volume EBS à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume, puis Actions et Modify volume (Modifier un volume).
4. La fenêtre Modify volume (Modifier un volume) affiche l'ID du volume et la configuration actuelle du volume, notamment le type, la taille, les IOPS et le débit. Définissez les nouvelles valeurs de configuration comme suit :
   - Afin de modifier le type, choisissez une valeur pour Volume type (Type de volume).
   - Pour modifier la taille, saisissez une nouvelle valeur pour Taille.
   - (`gp3`, `io1` et `io2` seulement) Afin de modifier les IOPS, saisissez une nouvelle valeur pour les IOPS.
   - (`gp3` seulement) Afin de modifier le débit, saisissez une nouvelle valeur pour Throughput (Débit).
5. Une fois que vous avez fini de modifier les paramètres du volume, choisissez Modifier. Lorsque vous êtes invité à confirmer l'opération, choisissez Modify (Modifier).
6. **Important**

   Si vous avez augmenté la taille de votre volume, vous devez également étendre la partition du volume pour utiliser la capacité de stockage supplémentaire. Pour de plus amples informations, veuillez consulter Étendre le système de fichiers après le redimensionnement d'un volume Amazon EBS.
7. (Instances Windows uniquement) Si vous augmentez la taille d'un NVMe volume sur une instance dépourvue de AWS NVMe pilotes, vous devez redémarrer l'instance pour permettre à Windows de voir la nouvelle taille du volume. Pour plus d'informations sur l'installation des AWS NVMe pilotes, consultez la section AWS NVMe pilotes.

AWS CLI

Pour modifier un volume EBS à l'aide du AWS CLI

Utilisez la commande modify-volume pour modifier un ou plusieurs paramètres de configuration d'un volume. Par exemple, si vous avez un volume du type gp2 d'une taille de 100 Gio, la commande suivante modifie sa configuration en un volume de type `io1` avec 10 000 IOPS et une taille de 200 Gio.

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-
id vol-1111111111111111
```

Voici un exemple de sortie :

```
{
    "VolumeModification": {
        "TargetSize": 200,
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-1111111111111111",
        "TargetIops": 10000,
        "StartTime": "2017-01-19T22:21:02.959Z",
        "Progress": 0,
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 100
    }
}
```

> **Important**
>
> Si vous avez augmenté la taille de votre volume, vous devez également étendre la partition du volume pour utiliser la capacité de stockage supplémentaire. Pour de plus amples informations, veuillez consulter Étendre le système de fichiers après le redimensionnement d'un volume Amazon EBS.

Modifier un volume EBS si Elastic Volumes n'est pas pris en charge

Si vous utilisez un type d'instance pris en charge, vous pouvez utiliser Elastic Volumes pour modifier dynamiquement la taille, les performances et le type de volume de vos volumes Amazon EBS sans les détacher.

Si vous ne pouvez pas utiliser Elastic Volumes mais que vous devez modifier le volume racine (de démarrage), vous devez arrêter l'instance, modifier le volume, puis redémarrer l'instance.

Une fois que l'instance a démarré, vous pouvez vérifier la taille du système de fichiers pour vérifier que votre instance reconnaît l'espace de volume agrandi. Sur Linux, utilisez la commande df -h pour vérifier la taille du système de fichiers.

```
[ec2-user ~]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/xvda1            7.9G  943M  6.9G  12% /
tmpfs                 1.9G     0  1.9G   0% /dev/shm
```

Si la taille ne reflète pas votre volume nouvellement étendu, vous devez étendre le système de fichiers de votre périphérique pour permettre à votre instance d'utiliser le nouvel espace. Pour de plus amples informations, veuillez consulter Étendre le système de fichiers après le redimensionnement d'un volume Amazon EBS.

Dans le cas des instances Windows, vous devrez peut-être mettre le volume en ligne pour pouvoir l'utiliser. Pour de plus amples informations, veuillez consulter Rendre un volume Amazon EBS disponible pour utilisation. Vous n'avez pas besoin de reformater le volume.

Initialiser la prise en charge d'Elastic Volumes (si nécessaire)

Avant de pouvoir modifier un volume attaché à une instance avant le 3 novembre 2016 à 23 h 40 UTC, vous devez initialiser la prise en charge de modification des volumes par l'une des actions suivantes :

- Détacher et attacher le volume
- Arrêter et démarrer l'instance

Utilisez l'une des procédures suivantes pour déterminer si vos instances sont prêtes pour la modification de volume.

Console

Pour déterminer si vos instances sont prêtes à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Instances.

3. Choisissez l'icône Afficher / Masquer les colonnes (icône d'engrenage). Sélectionnez la colonne d'attribut Heure de lancement, puis choisissez Confirmer.
4. Triez la liste d'instances par colonne d'Heure de lancement. Pour chaque instance démarrée avant la date limite, choisissez l'onglet Stockage et cochez la colonne Heure des pièces jointes pour voir quand ses volumes ont été attachés.

AWS CLI

Pour déterminer si vos instances sont prêtes à l'aide de la CLI

Utilisez la commande describe-instances suivante pour déterminer si le volume a été attaché avant le 3 novembre 2016 à 23 h 40 UTC.

```
aws ec2 describe-instances --query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" --output text
```

```
aws ec2 describe-instances -\-query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" -\-output text
```

Pour chaque instance, la première ligne de la sortie montre son ID et si elle a été démarrée avant la date de coupure (vrai ou faux). La première ligne est suivie d'une ou plusieurs lignes qui montrent si chaque volume EBS a été attaché avant la date de coupure (vrai ou faux). Dans la sortie de l'exemple suivant, vous devez initialiser la modification des volumes pour la première instance car elle a commencé avant la date de coupure et son volume de racine a été attaché avant la date de coupure. Les autres instances sont prêtes car elles ont été démarrées après la date de coupure.

```
i-e905622e              True
True
i-719f99a8              False
True
i-006b02c1b78381e57     False
False
False
i-e3d172ed              False
True
```

Surveillez la progression des modifications des volumes Amazon EBS

Lorsque vous modifiez un volume EBS, il passe par une suite d'états. Le volume passe à l'état `modifying`, à l'état `optimizing` et enfin à l'état `completed`. A ce stade, le volume est prêt à recevoir d'autres modifications.

> **Note**
>
> Dans de rares cas, une AWS panne transitoire peut entraîner un `failed` état. Ceci n'indique pas la santé du volume, mais uniquement l'échec de modification du volume. Si cela se produit, réessayez de modifier le volume.

Lorsque le volume a l'état `optimizing`, ses performances se situent entre les spécifications de configuration source et les spécifications de configuration cible. Les performances de volume transitoires ne seront jamais inférieures aux performances de volume source. Si vous mettez à niveau les opérations d'IOPS, les performances de volume transitoires ne seront jamais inférieures aux performances de volume cible.

Les changements des modifications du volume prennent effet comme suit :

- Les modifications de taille prennent normalement quelques secondes et sont effectives après que le volume soit passé à l'état `0ptimizing`.
- Les modifications de performances (opérations d'IOPS) peuvent prendre quelques minutes à quelques heures et dépendent de la modification de configuration effectuée.
- Dans certains cas, il peut s'écouler plus de 24 heures avant qu'une nouvelle configuration ne soit prise en compte, par exemple lorsque le volume n'a pas été entièrement initialisé. En général, un volume d'1 Tio pleinement utilisé met environ 6 heures à migrer vers une nouvelle configuration de performances.

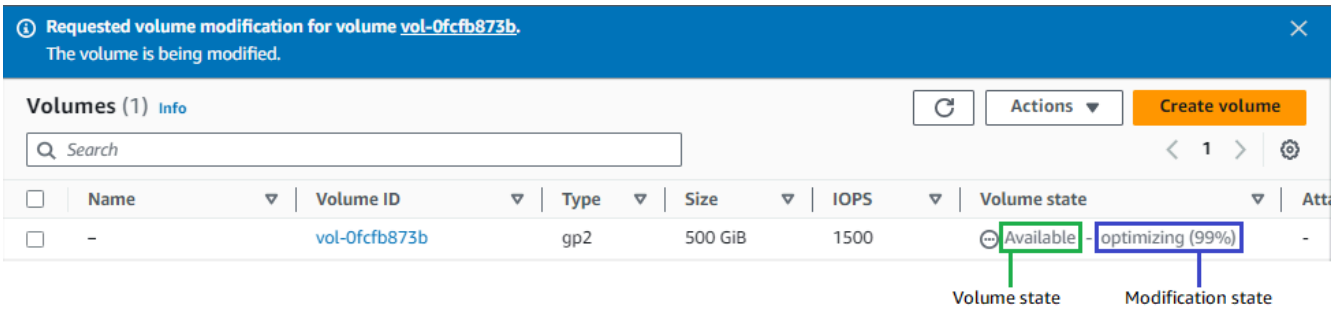
Pour surveiller la progression de la modification d'un volume, utilisez l'une des méthodes suivantes.

Console

Pour suivre la progression d'une modification à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.

3. Sélectionnez le volume.
4. La colonne État du volume et le champ État du volume de l'onglet Détails contiennent des informations au format suivant : *Volume state* - *Modification state* (*Modification progress*%). L'image suivante montre le volume et les états de modification du volume.



Les états de volume possibles sont les suivants : `creating`, `available`, `in-use`, `deleting`, `deleted` et `error`.

Les états de modification possibles sont `modifying`, `optimizing` et `completed`.

Une fois la modification terminée, seul l'état du volume est affiché. L'état de modification et la progression ne sont plus affichés.

AWS CLI

Pour suivre la progression d'une modification à l'aide du AWS CLI

Utilisez la describe-volumes-modificationscommande pour voir la progression d'une ou de plusieurs modifications de volume. L'exemple suivant décrit les modifications de volume de deux volumes.

```
aws ec2 describe-volumes-modifications --volume-
ids vol-1111111111111111 vol-2222222222222222
```

Dans l'exemple de sortie suivant, les modifications de volume sont encore à l'état `modifying`. La progression est présentée en pourcentage.

```
{
    "VolumesModifications": [
        {
            "TargetSize": 200,
            "TargetVolumeType": "io1",
```

```
            "ModificationState": "modifying",
            "VolumeId": "vol-1111111111111111",
            "TargetIops": 10000,
            "StartTime": "2017-01-19T22:21:02.959Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 100
        },
        {
            "TargetSize": 2000,
            "TargetVolumeType": "sc1",
            "ModificationState": "modifying",
            "VolumeId": "vol-2222222222222222",
            "StartTime": "2017-01-19T22:23:22.158Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 1000
        }
    ]
}
```

L'exemple suivant décrit tous les volumes dont l'état de modification est `optimizing` ou `completed`, puis filtre et formate les résultats pour n'afficher que les modifications initiées le 1er février 2017 ou après cette date :

```
aws ec2 describe-volumes-modifications --filters Name=modification-
state,Values="optimizing","completed" --query "VolumesModifications[?
StartTime>='2017-02-01'].{ID:VolumeId,STATE:ModificationState}"
```

Voici un exemple de sortie avec des informations sur deux volumes :

```
[
    {
        "STATE": "optimizing",
        "ID": "vol-06397e7a0eEXAMPLE"
    },
    {
        "STATE": "completed",
        "ID": "vol-ba74e18c2aEXAMPLE"
    }
```

```
]
```

CloudWatch Events console

Avec CloudWatch Events, vous pouvez créer une règle de notification pour les événements de modification de volume. Vous pouvez utiliser votre règle pour générer un message de notification avec Amazon SNS ou appeler une fonction Lambda en réponse aux événements correspondants. Les événements sont générés sur la base du meilleur effort.

Pour suivre la progression d'une modification à l'aide CloudWatch des événements

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Événements, Créer une règle.
3. Pour Créer un modèle d'événement correspondant aux événements par service, choisissez Un modèle d'événement personnalisé.
4. Pour Créer un modèle d'événement personnalisé, remplacez le contenu par ce qui suit et choisissez Enregistrer.

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EBS Volume Notification"
  ],
  "detail": {
    "event": [
      "modifyVolume"
    ]
  }
}
```

Voici un exemple de données d'événement :

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
```

```
   "time": "2017-01-12T21:09:07Z",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```


Étendre le système de fichiers après le redimensionnement d'un volume Amazon EBS

Après avoir augmenté la taille d'un volume EBS, vous devez étendre la partition et le système de fichiers à la nouvelle taille, plus grande. Vous pouvez le faire dès que le volume entre dans l'état `optimizing`.

Avant de commencer

- Créez un instantané du volume, au cas où vous auriez besoin d'annuler vos modifications. Pour de plus amples informations, veuillez consulter Créer des instantanés Amazon EBS.
- Confirmez que la modification du volume a réussi et qu'il est dans l'état `optimizing` ou `completed`. Pour de plus amples informations, veuillez consulter Surveillez la progression des modifications des volumes Amazon EBS.
- Assurez-vous que le volume est attaché à l'instance et qu'il est formaté et monté. Pour de plus amples informations, veuillez consulter Formatage et montage d'un volume attaché.
- (Instances Linux uniquement) Si vous utilisez des volumes logiques sur le volume Amazon EBS, vous devez utiliser Logical Volume Manager (LVM) pour étendre le volume logique. Pour savoir comment procéder, consultez la section Étendre le LV dans l'article Comment utiliser LVM pour créer un volume logique sur la partition d'un volume EBS ? .

Instances Linux

> **Note**
>
> Les instructions suivantes vous guident dans le processus d'extension des systèmes de fichiers XFS et Ext4 pour Linux. Pour plus d'informations sur l'extension d'un autre système de fichiers, consultez sa documentation.

Avant de pouvoir étendre un système de fichiers sous Linux, vous devez étendre la partition, si votre volume en possède une.

Étendre le système de fichiers des volumes EBS

Utilisez la procédure suivante pour étendre le système de fichiers d'un volume redimensionné.

Notez que le nom des périphériques et des partitions diffère pour les instances Xen et les instances basées sur le système Nitro. Pour déterminer si votre instance est basée sur Xen ou Nitro, utilisez la describe-instance-types AWS CLI commande suivante :

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-type instance_type --query
 "InstanceTypes[].Hypervisor"
```

La valeur de `nitro` indique que votre instance est basée sur Nitro. La valeur de `xen` indique que votre instance est basée sur Xen.

Pour étendre le système de fichiers des volumes EBS

1. Connectez-vous à votre instance.
2. Redimensionnez la partition, si nécessaire. Pour ce faire :

   a. Vérifiez si le volume possède une partition. Utilisez la commande lsblk.

      Nitro instance example

      Dans l'exemple de sortie suivant, le volume racine (`nvme0n1`) possède deux partitions (`nvme0n1p1` et `nvme0n1p128`), tandis que le volume supplémentaire (`nvme1n1`) ne possède aucune partition.

      ```
      [ec2-user ~]$ sudo lsblk
      NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
      ```

```
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

Dans l'exemple de sortie suivant, le volume racine (`xvda`) possède une partition (`xvda1`), tandis que le volume supplémentaire (`xvdf`) ne possède aucune partition.

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  24G  0 disk
```

Si le volume possède une partition, poursuivez la procédure à partir de l'étape suivante (2b). Si le volume ne possède aucune partition, ignorez les étapes 2b, 2c et 2d et poursuivez la procédure à partir de l'étape 3.

> **Conseil pour la résolution de problèmes**
>
> Si vous ne voyez pas le volume dans la sortie de la commande, assurez-vous que le volume est attaché à l'instance, et qu'il est formaté et monté.

b. Vérifiez si la partition doit être étendue. Dans la sortie de la commande lsblk de l'étape précédente, comparez la taille de la partition et celle du volume.

   Si la taille de la partition est inférieure à celle du volume, passez à l'étape suivante. Si la taille de la partition est égale à celle du volume, la partition ne peut pas être étendue.

   > **Conseil pour la résolution de problèmes**
   >
   > Si le volume reflète toujours la taille d'origine, confirmez que la modification du volume a réussi.

c. Étendez la partition. Utilisez la growpart commande et spécifiez le nom du périphérique et le numéro de partition.

Nitro instance example

Le numéro de partition est le numéro situé après lep. Par exemple, pour`nvme0n1p1`, le numéro de partition est`1`. Car `nvme0n1p128` le numéro de partition est`128`.

Pour étendre une partition nommée`nvme0n1p1`, utilisez la commande suivante.

> **Important**
>
> Notez l'espace entre le nom du périphérique (`nvme0n1`) et le numéro de la partition (1).

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

Xen instance example

Le numéro de partition est le numéro situé après le nom de l'appareil. Par exemple, pour`xvda1`, le numéro de partition est`1`. Car `xvda128` le numéro de partition est`128`.

Pour étendre une partition nommée`xvda1`, utilisez la commande suivante.

> **Important**
>
> Notez l'espace entre le nom du périphérique (`xvda`) et le numéro de la partition (1).

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
```

> **Conseils pour le dépannage**
>
> - `mkdir: cannot create directory '/tmp/growpart.31171': No space left on device FAILED: failed to make temp dir` : indique qu'il n'y a pas assez d'espace disque libre sur le volume pour que

growpart puisse créer le répertoire temporaire dont il a besoin pour effectuer le redimensionnement. Libérez de l'espace disque, puis recommencez.

- `must supply partition-number` : indique que vous avez spécifié une partition incorrecte. Utilisez la commande lsblk pour confirmer le nom de la partition, et assurez-vous de saisir un espace entre le nom du périphérique et le numéro de la partition.
- `NOCHANGE: partition 1 is size 16773087. it cannot be grown` : indique que la partition couvre déjà la totalité du volume et ne peut pas être étendue. Confirmez que la modification du volume a réussi.

d. Vérifiez que la partition a été étendue. Utilisez la commande lsblk. La taille de la partition devrait maintenant être égale à celle du volume.

Nitro instance example

L'exemple de sortie suivant montre que le volume (`nvme0n1`) et la partition (`nvme0n1p1`) ont la même taille (`16 GB`).

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0  16G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

L'exemple de sortie suivant montre que le volume (`xvda`) et la partition (`xvda1`) ont la même taille (`16 GB`).

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0  16G  0 part /
xvdf    202:80   0  24G  0 disk
```

3. Étendre le système de fichiers.

a. Obtenez le nom, la taille, le type et le point de montage du système de fichiers que vous devez étendre. Utilisez la commande df -hT.

Nitro instance example

L'exemple de sortie suivant montre que le système de fichiers `/dev/nvme0n1p1` a une taille de 8 Go, que son type est `xfs` et que son point de montage est `/`.

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
/dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
...
```

Xen instance example

L'exemple de sortie suivant montre que le système de fichiers `/dev/xvda1` a une taille de 8 Go, que son type est `ext4` et que son point de montage est `/`.

```
[ec2-user ~]$ df -hT
Filesystem      Type   Size    Used   Avail   Use%   Mounted on
/dev/xvda1      ext4   8.0G    1.9G   6.2G    24%    /
/dev/xvdf1      xfs    24.0G   45M    8.0G    1%     /data
...
```

b. Les commandes permettant d'étendre le système de fichiers diffèrent en fonction du type de système de fichiers. Choisissez la commande correcte suivante en fonction du type de système de fichiers que vous avez noté à l'étape précédente.

- [Système de fichiers XFS] Utilisez la commande xfs_growfs et spécifiez le point de montage du système de fichiers que vous avez noté à l'étape précédente.

  Nitro and Xen instance example

  Par exemple, pour étendre un système de fichiers monté sur `/`, utilisez la commande suivante.

  ```
  [ec2-user ~]$ sudo xfs_growfs -d /
  ```

  Conseils pour le dépannage

  - `xfs_growfs: /data is not a mounted XFS filesystem` : indique que vous avez spécifié un point de montage incorrect ou que le système de

fichiers n'est pas XFS. Pour vérifier le point de montage et le type de système de fichiers, utilisez la commande df -hT.

- `data size unchanged, skipping` : indique que le système de fichiers occupe déjà l'ensemble du volume. Si le volume ne comporte pas de partitions, confirmez que la modification du volume a réussi. Si le volume comporte des partitions, assurez-vous que la partition a été étendue comme décrit à l'étape 2.

- [Système de fichiers Ext4] Utilisez la commande resize2fs et spécifiez le nom du système de fichiers que vous avez noté à l'étape précédente.

  Nitro instance example

  Par exemple, pour étendre un système de fichiers monté nommé `/dev/nvme0n1p1`, utilisez la commande suivante.

  ```
  [ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
  ```

  Xen instance example

  Par exemple, pour étendre un système de fichiers monté nommé `/dev/xvda1`, utilisez la commande suivante.

  ```
  [ec2-user ~]$ sudo resize2fs /dev/xvda1
  ```

  Conseils pour le dépannage

  - `resize2fs: Bad magic number in super-block while trying to open /dev/xvda1` : indique que le système de fichiers n'est pas Ext4. Pour vérifier le type de système de fichiers, utilisez la commande df -hT.
  - `open: No such file or directory while opening /dev/xvdb1` : indique que vous avez spécifié une partition incorrecte. Pour vérifier la partition, utilisez la commande df -hT.
  - `The filesystem is already 3932160 blocks long. Nothing to do!` : indique que le système de fichiers occupe déjà l'ensemble du volume. Si le volume ne comporte pas de partitions, confirmez que la modification du volume a réussi. Si le volume comporte des partitions, assurez-vous que la partition a été étendue, comme décrit à l'étape 2.

- [Autre système de fichiers] Consultez la documentation de votre système de fichiers pour obtenir des instructions.

c. Vérifiez que le système de fichiers a été étendu. Utilisez la commande df -hT et confirmez que la taille du système de fichiers est égale à la taille du volume.

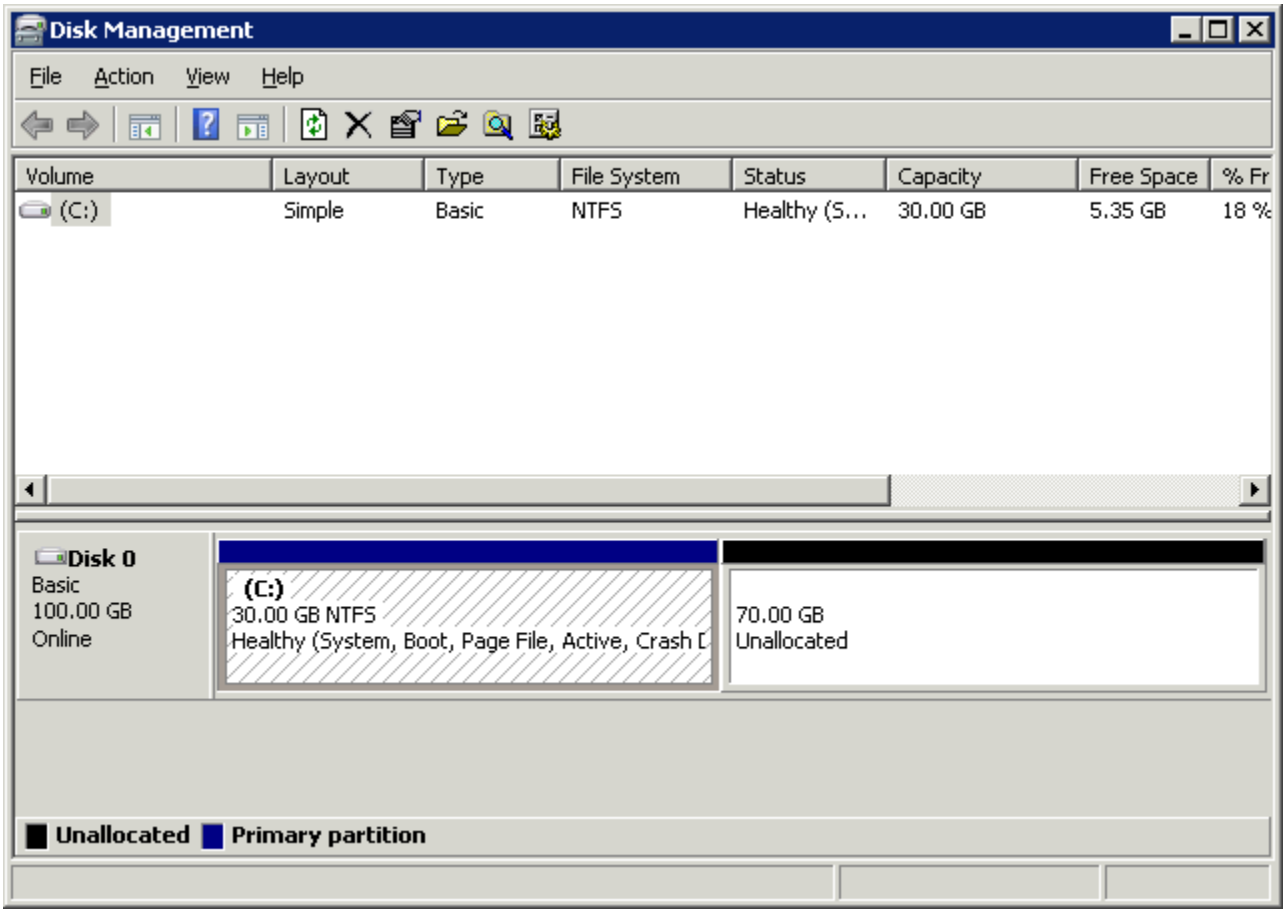
instances Windows

Utilisez l'une des méthodes suivantes pour étendre le système de fichiers sur une instance Windows.

Disk Management utility

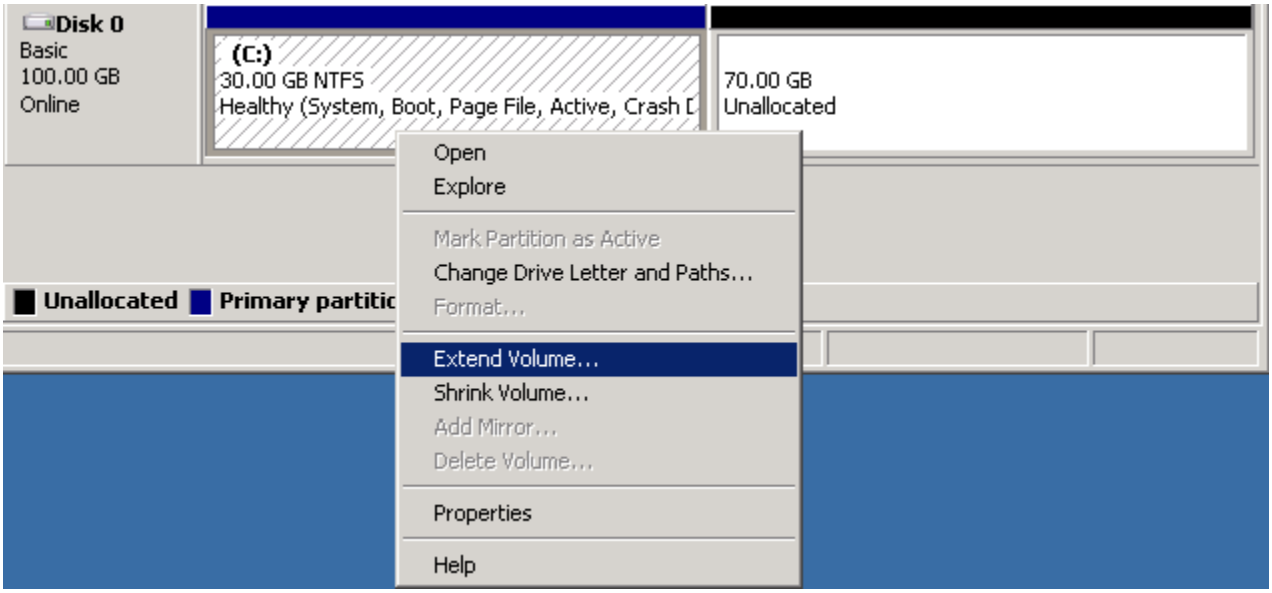
Pour étendre un système de fichiers à l'aide de la gestion des disques

1. Avant d'étendre un système de fichiers qui contient des données critiques, une bonne pratique consiste à créer un instantané du volume qui le contient au cas où vous auriez besoin d'annuler vos modifications. Pour plus d'informations, consultez Créer des instantanés Amazon EBS.
2. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance.
3. Dans la boîte de dialogue Exécuter, saisissez diskmgmt.msc et appuyez sur Entrée. L'utilitaire Gestion des disques s'ouvre.

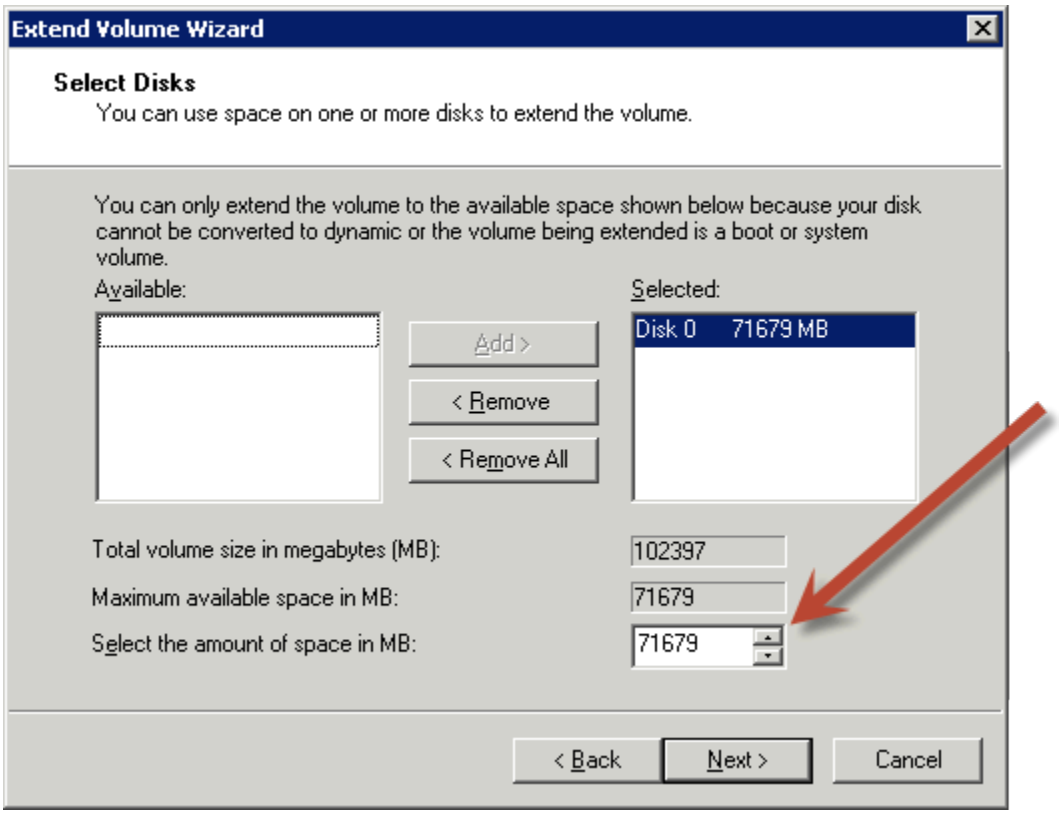


4. Dans le menu Gestion des disques, choisissez Action, Analyser les disques de nouveau.
5. Ouvrez le menu contextuel (clic droit) correspondant au disque étendu et choisissez Extension du volume.

> **Note**
>
> Extension du volume peut être désactivé (grisé) si :
>
> - L'espace non alloué n'est pas adjacent au lecteur. L'espace non alloué doit être adjacent au côté droit du disque que vous souhaitez étendre.
> - Le volume utilise le style de partition MBR (Master Boot Record) et il a déjà une taille de 2 To. Les volumes qui utilisent MBR ne peuvent pas dépasser 2 To.



6. Dans l'Assistant Extension du volume, choisissez Suivant. Pour Select the amount of space in MB (Sélectionner la quantité d'espace en Mo), indiquez le nombre de méga-octets jusqu'auquel vous voulez étendre le volume. En règle générale, vous spécifiez l'espace disponible maximal. Le texte en surbrillance qui figure sous Sélectionné correspond à la quantité d'espace ajoutée, pas à la taille finale du volume. Exécutez l'assistant.



7. Si vous augmentez la taille d'un NVMe volume sur une instance qui ne possède pas le AWS NVMe pilote, vous devez redémarrer l'instance pour permettre à Windows de voir la nouvelle taille du volume. Pour plus d'informations sur l'installation du AWS NVMe pilote, consultez la section AWS NVMe pilotes.

PowerShell

Utilisez la procédure suivante pour étendre un système de fichiers Windows à l'aide de PowerShell.

Pour étendre un système de fichiers à l'aide de PowerShell

1. Avant d'étendre un système de fichiers qui contient des données critiques, une bonne pratique consiste à créer un instantané du volume qui le contient au cas où vous auriez besoin d'annuler vos modifications. Pour plus d'informations, consultez Créer des instantanés Amazon EBS.
2. Connectez-vous à votre instance Windows en utilisant les services Bureau à distance.
3. Exécutez PowerShell en tant qu'administrateur.
4. Exécutez la `Get-Partition` commande. PowerShell renvoie le numéro de partition correspondant pour chaque partition, la lettre du lecteur, le décalage, la taille et le type. Notez la lettre de lecteur de la partition à étendre.
5. Exécutez la commande suivante pour effectuer une nouvelle analyse du disque.

```
"rescan" | diskpart
```

6. Exécutez la commande suivante en utilisant la lettre de lecteur que vous avez notée à l'étape 4 à la place de**<drive-letter>**. PowerShell renvoie la taille minimale et maximale de la partition autorisée, en octets.

```
Get-PartitionSupportedSize -DriveLetter <drive-letter>
```

7. Pour étendre la partition à une quantité spécifiée, exécutez la commande suivante, en entrant la nouvelle taille du volume à la place de **<size>**. Vous pouvez entrer la taille en `KB`, `MB` et `GB`, par exemple `50GB`.

```
Resize-Partition -DriveLetter <drive-letter> -Size <size>
```

Pour étendre la partition à la taille maximale disponible, exécutez la commande suivante.

```
Resize-Partition -DriveLetter <drive-letter> -Size $(Get-PartitionSupportedSize
 -DriveLetter <drive-letter>).SizeMax
```

Les PowerShell commandes suivantes montrent le flux complet de commandes et de réponses permettant d'étendre un système de fichiers à une taille spécifique.

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                      8 MB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin      SizeMax
-------      -------
8388608 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size 50GB
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS
```

Les PowerShell commandes suivantes montrent le flux complet de commandes et de réponses permettant d'étendre un système de fichiers à la taille maximale disponible.

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

 SizeMin      SizeMax
 -------      -------
59047936 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size $(Get-PartitionSupportedSize -DriveLetter D).SizeMax
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                    100 GB IFS
```

Détacher un volume Amazon EBS d'une instance Amazon EC2

Vous devez détacher un volume Amazon Elastic Block Store (Amazon EBS) d'une instance avant de pouvoir l'attacher à une autre instance ou le supprimer. Le détachement d'un volume n'affecte pas les données du volume.

Rubriques

- Considérations
- Démonter et détacher un volume

- Dépannage

Considérations

- Vous pouvez détacher un volume Amazon EBS d'une instance explicitement ou en mettant fin à l'instance. Toutefois, si l'instance est en cours d'exécution, vous devez d'abord démonter le volume à partir de l'instance.
- Si un volume EBS est le volume racine d'une instance, vous devez arrêter l'instance avant de pouvoir détacher le volume.
- Vous pouvez rattacher un volume que vous avez détaché (sans l'avoir démonté), mais celui-ci n'aura peut-être pas le même point de montage. S'il y avait des écritures en cours sur le volume au moment où il a été détaché, les données sur le volume peuvent ne pas être synchronisées.
- Une fois que vous avez détaché un volume, le stockage en volume vous est toujours facturé tant que la quantité de stockage dépasse la limite du niveau AWS gratuit. Vous devez supprimer un volume pour éviter de générer des frais supplémentaires. Pour plus d'informations, consultez Supprimer un volume Amazon EBS.

Démonter et détacher un volume

Utilisez les procédures suivantes pour démonter et détacher un volume d'une instance. Cela peut être utile lorsque vous devez attacher le volume à une autre instance ou lorsque vous devez le supprimer.

Étapes

- Étape 1 : Démonter le volume
- Étape 2 : Détacher le volume de l'instance
- Étape 3 : (instances Windows uniquement) Désinstallez les emplacements des appareils hors ligne

Étape 1 : Démonter le volume

Instances Linux

À partir de votre instance Linux, utilisez la commande suivante pour démonter l'unité `/dev/sdh`.

```
[ec2-user ~]$ sudo umount -d /dev/sdh
```

instances Windows

Depuis votre instance Windows, démontez le volume comme suit.

1. Démarrez l'utilitaire Gestion des disques.
   - (Windows Server 2012 et versions ultérieures) Dans la barre des tâches, cliquez avec le bouton droit sur le logo Windows, puis sélectionnez Disk Management (Gestion des disques).
   - (Windows Server 2008) Sélectionnez Start (Démarrer), Administrative Tools (Outils d'administration), Computer Management (Gestion des ordinateurs) et Disk Management (Gestion des disques).
2. Cliquez avec le bouton droit sur le disque (par exemple, cliquez avec le bouton droit sur Disk 1 (Disque 1)), puis sélectionnez Hors connexion. Attendez que l'état du disque passe à Hors ligne avant d'ouvrir la EC2 console Amazon.

Étape 2 : Détacher le volume de l'instance

Pour détacher le volume de l'instance, utilisez l'une des méthodes suivantes :

Console

Pour détacher un volume EBS à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez un volume à détacher et choisissez Actions, Detach Volume (Détacher le volume).
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Detach.

AWS CLI

Pour détacher un volume EBS d'une instance à l'aide du AWS CLI

Après avoir démonté le volume, utilisez la commande detach-volume.

Tools for Windows PowerShell

Pour détacher un volume EBS d'une instance à l'aide des outils pour Windows PowerShell

Après avoir démonté le volume, utilisez la Dismount-EC2Volumecommande.

Étape 3 : (instances Windows uniquement) Désinstallez les emplacements des appareils hors ligne

Lorsque vous démontez et détachez un volume d'une instance, Windows signale l'emplacement du périphérique comme étant hors connexion. L'emplacement du périphérique reste hors ligne après le rebooting, l'arrêt et le redémarrage de l'instance. Lorsque vous redémarrez l'instance, Windows peut monter l'un des volumes restants à l'emplacement du périphérique hors connexion. Le volume devient indisponible dans Windows. Pour éviter que cela ne se produise et pour vous assurer que tous les volumes sont attachés à des emplacements de périphériques en ligne lors du prochain démarrage de Windows, effectuez les opérations suivantes :

1. Sur l'instance, ouvrez le Gestionnaire de périphériques.
2. Dans le Gestionnaire de périphériques, sélectionnez View (Affichage), Show hidden devices (Afficher les périphériques masqués).
3. Dans la liste des périphériques, développez le nœud Storage controllers (Contrôleurs de stockage).

   Les emplacements de périphériques sur lesquels les volumes détachés ont été montés sont nommés `AWS NVMe Elastic Block Storage Adapter` et ils doivent être grisés.
4. Cliquez avec le bouton droit sur chaque emplacement de périphérique grisé nommé `AWS NVMe Elastic Block Storage Adapter`, sélectionnez Uninstall device (Désinstaller le périphérique) et choisissez Uninstall (Désinstaller).

   > **Important**
   >
   > Ne cochez pas la case Delete the driver software for this device (Supprimer le pilote logiciel pour ce périphérique).

Dépannage

Voici des problèmes courants rencontrés lors du détachement de volumes, ainsi que la façon de les résoudre.

> **Note**
>
> Pour vous prémunir contre la possibilité de perte de données, prenez un instantané de votre volume avant d'essayer de le démonter. Le détachement forcé d'un volume bloqué peut endommager le système de fichiers ou les données qu'il contient ou entraîner une incapacité

d'attacher un volume à l'aide du même nom de périphérique, sauf si vous redémarrez l'instance.

- Si vous rencontrez des problèmes lors du détachement d'un volume via la EC2 console Amazon, il peut être utile d'utiliser la commande describe-volumes CLI pour diagnostiquer le problème. Pour plus d'informations, consultez describe-volumes.
- Si votre volume reste à l'état `detaching`, vous pouvez forcer le détachement en cliquant sur Force Detach (Forcer le détachement). Utilisez cette option uniquement comme dernier recours pour détacher un volume d'une instance en échec, ou si vous détachez un volume avec l'intention de le supprimer. L'instance n'a pas la possibilité de vider les caches du système de fichiers ou les métadonnées du système de fichiers. Si vous utilisez cette option, vous devez effectuer un contrôle du système de fichiers et des procédures de réparation.
- Si vous avez essayé de forcer le volume à se détacher plusieurs fois sur plusieurs minutes et qu'il reste à l'état `detaching`, vous pouvez envoyer une demande d'aide à AWS re:Post. Pour aider à accélérer la résolution d'un problème, incluez l'ID du volume et décrivez les étapes que vous avez déjà effectuées.
- Lorsque vous essayez de détacher un volume qui est toujours monté, le volume peut se bloquer dans l'état `busy` lorsque vous tentez de le détacher. La sortie suivante de la commande describe-volumes présente un exemple de cette condition :

```
"Volumes": [
    {
        "AvailabilityZone": "us-west-2b",
        "Attachments": [
            {
                "AttachTime": "2016-07-21T23:44:52.000Z",
                "InstanceId": "i-fedc9876",
                "VolumeId": "vol-1234abcd",
                "State": "busy",
                "DeleteOnTermination": false,
                "Device": "/dev/sdf"
            }
        ...
    }
]
```

Lorsque vous rencontrez cet état, le détachement peut être retardé indéfiniment jusqu'à ce que vous démontiez le volume, forciez le détachement, redémarriez l'instance ou les trois.

Supprimer un volume Amazon EBS

Vous pouvez supprimer un volume Amazon EBS dont vous n'avez plus besoin. Une fois le volume supprimé, ses données sont perdues et il ne peut être attaché à aucune instance. Ainsi, avant la suppression, vous pouvez stocker un instantané du volume, que vous pourrez utiliser pour recréer le volume ultérieurement.

> **Note**
>
> Vous ne pouvez pas supprimer un volume si celui-ci est attaché à une instance. Pour supprimer un volume, vous devez d'abord le détacher. Pour plus d'informations, consultez Détacher un volume Amazon EBS d'une instance Amazon EC2 .
> Vous pouvez vérifier si un volume est attaché à une instance. Dans la console, sur la page Volumes ,vous pouvez afficher l'état de vos volumes.
>
> - Si un volume est attaché à une instance, son état est `in-use`.
> - Si un volume est détaché d'une instance, son état est `available`. Vous pouvez supprimer ce volume.

Vous pouvez supprimer un volume EBS en employant l'une des méthodes suivantes.

Console

Pour supprimer un volume EBS à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez un volume à supprimer et choisissez Actions, Delete Volume (Supprimer le volume).

> **Note**
>
> Si Delete Volume (Supprimer le volume) est grisé, le volume est attaché à une instance. Vous devez détacher le volume de l'instance avant de pouvoir le supprimer.

4. Dans la boîte de dialogue de confirmation, choisissez Delete (Supprimer).

AWS CLI

Pour supprimer un volume EBS à l'aide du AWS CLI

Utilisez la commande delete-volume.

Tools for Windows PowerShell

Pour supprimer un volume EBS à l'aide des outils pour Windows PowerShell

Utilisez la commande Remove-EC2Volume.

Remplacer un volume Amazon EBS à l'aide d'un instantané

Les instantanés Amazon EBS sont l'outil de sauvegarde préféré sur Amazon en EC2 raison de leur rapidité, de leur commodité et de leur coût. Lorsque vous créez un volume à partir d'un instantané, vous recréez son état à un moment précis dans le temps avec les données sauvegardées intactes jusqu'à ce moment là. En attachant un volume créé à partir d'un instantané à une instance, vous pouvez dupliquer des données dans plusieurs régions, créer des environnements de test, remplacer un volume de production endommagé ou corrompu dans son intégralité ou récupérer des fichiers et des répertoires spécifiques et les transférer vers un autre volume attaché. Pour de plus amples informations, veuillez consulter Instantanés Amazon EBS.

Vous pouvez suivre les procédures ci-après pour remplacer un volume Amazon EBS par un autre volume créé à partir d'un instantané antérieur du volume.

Console

Pour remplacer un volume à l'aide de la console

1. Créez un volume à partir de l'instantané et notez l'ID du nouveau volume. Pour de plus amples informations, veuillez consulter Créez un volume Amazon EBS..

> **Note**
>
> Veillez à créer le volume dans la même zone de disponibilité que votre instance. Les volumes ne peuvent être attachés qu'aux instances de la même zone de disponibilité.

2. Sur la page Instances, sélectionnez l'instance sur laquelle vous souhaitez remplacer le volume et notez l'ID de l'instance.

   Alors que l'instance est toujours sélectionnée, choisissez l'onglet Storage (Stockage). Dans la section Block devices (Périphériques de bloc), recherchez le volume à remplacer et notez le nom du périphérique pour le volume, par exemple `/dev/sda1`.

   Choisissez l'ID du volume.

3. Sur l'écran Volumes, sélectionnez le volume et choisissez Actions, Detach volume (Détacher un volume), Detach (Détacher).

4. Sélectionnez le nouveau volume que vous avez créé à l'étape 1 et choisissez Actions, Attach volume (Attacher un volume).

   Pour Instance et Device name (Nom de périphérique), saisissez l'ID d'instance et le nom de périphérique que vous avez noté à l'étape 2, puis choisissez Attach volume (Attacher le volume).

5. Connectez-vous à votre instance et montez le volume. Pour de plus amples informations, veuillez consulter Rendre un volume Amazon EBS disponible pour utilisation.

AWS CLI

Pour remplacer un volume à l'aide du AWS CLI

1. Créez un volume à partir de l'instantané. Utilisez la commande create-volume. Pour `--snapshot-id`, spécifiez l'ID de l'instantané à utiliser. Pour `--availability-zone`, spécifiez la même zone de disponibilité que l'instance. Configurez les paramètres restants selon les besoins.

> **Note**
>
> Veillez à créer le volume dans la même zone de disponibilité que votre instance. Les volumes ne peuvent être attachés qu'aux instances de la même zone de disponibilité.

```
$ aws ec2 create-volume \
--volume-type volume_type \
--size volume_size \
--snapshot-id snapshot_id \
--availability-zone az_id
```

Notez l'ID du nouveau volume dans la sortie de la commande.

2. Obtenez le nom du périphérique du volume à remplacer. Utilisez la commande describe-instances. Pour `--instance-ids`, spécifiez l'ID de l'instance dont le volume doit être remplacé.

```
$ aws ec2 describe-instances --instance-ids instance_id
```

Dans `BlockDeviceMappings`, dans la sortie de commande, notez `DeviceName` et `VolumeId` pour le volume à remplacer.

3. Détachez le volume à remplacer de l'instance. Utilisez la commande detach-volume. Pour `--volume-id`, spécifiez l'ID du volume à détacher.

```
$ aws ec2 detach-volume --volume-id volume_id
```

4. Attachez le volume de remplacement à l'instance. Utilisez la commande attach-volume. Pour `--volume-id`, spécifiez l'ID du volume de remplacement. Pour `--instance-id`, spécifiez l'ID de l'instance auquel le volume doit être attaché. Pour `--device`, spécifiez le même nom de périphérique que celui que vous avez noté précédemment.

```
$ aws ec2 attach-volume \
--volume-id volume_id \
--instance-id instance_id \
--device device_name
```

5. Connectez-vous à votre instance et montez le volume. Pour de plus amples informations, veuillez consulter Rendre un volume Amazon EBS disponible pour utilisation.

Contrôles de l'état des volumes Amazon EBS

Les contrôles de statut de volume vous permettent de mieux comprendre, suivre et gérer les incohérences potentielles des données d'un volume Amazon EBS. Ils sont destinés à vous fournir les informations dont vous avez besoin pour déterminer si vos volumes Amazon EBS rencontrent des problèmes et pour vous aider à contrôler comment un volume potentiellement incohérent est géré.

Les contrôles de statut de volume sont exécutés automatiquement toutes les cinq minutes et renvoie un statut de réussite ou d'échec. Si tous les contrôles réussissent, le statut du volume est ok. Si un contrôle échoue, le statut du volume est `impaired`. Si le statut est `insufficient-data`, il se peut que les contrôles soient toujours en cours sur le volume. Vous pouvez afficher les résultats des contrôles de statut de volume pour identifier les volumes confrontés à des problèmes et prendre les actions nécessaires.

Lorsqu'Amazon EBS détermine que les données d'un volume sont potentiellement incohérentes, il désactive par défaut les E/S vers le volume à partir de toute EC2 instance attachée, ce qui contribue à empêcher la corruption des données. Une fois que les I/O ont été désactivées, le contrôle de statut de volume suivant échoue et le statut du volume est `impaired`. De plus, vous remarquerez un événement qui vous permet de savoir que les I/O sont désactivées, et que vous pouvez résoudre le statut de défaillance du volume en activant les I/O sur le volume. Nous attendons que vous activiez les E/S pour vous permettre de décider de continuer à autoriser vos instances à utiliser le volume ou d'exécuter un contrôle de cohérence à l'aide d'une commande, telle que fsck (instances Linux) ou chkdsk (instances Windows), avant de le faire.

> **Note**
>
> Le statut du volume s'appuie sur les vérifications de statut du volume et ne reflète pas l'état du volume. Par conséquent, le statut du volume n'indique pas de volumes avec l'état `error` (par exemple, lorsqu'un volume est incapable d'accepter l'I/O). Pour plus d'information sur les états de volume, consultez États du volume.

Si la cohérence d'un volume particulier ne constitue pas un problème et que vous préfèreriez que le volume soit rendu disponible immédiatement s'il rencontre des problèmes, vous pouvez remplacer le comportement par défaut en configurant le volume de façon à activer automatiquement les I/O. Si

vous activez l'attribut de volume Auto-Enable IO (Activation automatique des I/O) (`autoEnableIO` dans l'API), la vérification de l'état du volume continue de se faire. De plus, vous remarquerez un événement qui vous permet de savoir que le volume a été déterminé pour être potentiellement incohérent, mais que ses I/O ont été automatiquement activées. Cela vous permet de vérifier la cohérence du volume ou de le remplacer ultérieurement.

Le contrôle de statut des performances d'I/O compare les performances réelles du volume aux performances attendues. Il vous prévient si le volume se comporte en-deçà des attentes. Cette vérification d'état n'est disponible que pour les volumes SSD IOPS provisionnés (`io1` et `io2`) et les volumes SSD polyvalent (`gp3`) attachés à une instance. La vérification d'état n'est pas valide pour les volumes SSD polyvalent (`gp2`), HDD à débit optimisé (`st1`), HDD à froid (`sc1`), ou magnétique (`standard`). Le contrôle de l'état des performances des E/S est effectué une fois par minute et CloudWatch collecte ces données toutes les 5 minutes. Il peut prendre jusqu'à 5 minutes à partir du moment où vous liez un volume `io1` ou `io2` à une instance pour signaler le statut des performances d'I/O.

> **Important**
>
> Lors de l'initialisation des volumes Provisioned IOPS SSD restaurés à partir des instantanés, les performances du volume peuvent chuter jusqu'à plus de 50 % en dessous du niveau attendu, ce qui entraîne l'affichage par le volume d'un état `warning` dans le contrôle de statut Performances des I/O. Cette situation est attendue et vous pouvez ignorer l'état `warning` des volumes Provisioned IOPS SSD lorsque vous les initialisez. Pour plus d'informations, consultez Initialiser les volumes Amazon EBS.

Le tableau suivant répertorie les statuts des volumes Amazon EBS.

Statut du volume	Statut d'activation des I/O	Statut de performance des I/O (volumes **`io1`**, **`io2`** et **`gp3`** uniquement)
ok	Activé (I/O activées ou I/O activées automatiquement)	Normal (performances du volume telles qu'attendues)
`warning`	Activé (I/O activées ou I/O activées automatiquement)	Dégradé (performances du volume inférieures aux attentes)

Statut du volume	Statut d'activation des I/O	Statut de performance des I/O (volumes **io1**, **io2** et **gp3** uniquement)
		Profondément dégradé (performances du volume bien inférieures aux attentes)
`impaired`	Activé (I/O activées ou I/O activées automatiquement) Désactivé (volume hors connexion et récupération en attente, ou en attente d'activation par l'utilisateur des I/O)	Interrompu (performances du volume profondément impactées) Non disponible (impossible de déterminer les performances d'I/O flottee que les I/O sont désactivées)
`insufficient-data`	Activé (I/O activées ou I/O activées automatiquement) Données insuffisantes	Données insuffisantes

Vous pouvez afficher et utiliser les contrôles de statut à l'aide des méthodes suivantes.

Console

Pour afficher les contrôles de statut

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.

   La colonne Volume Status (Statut du volume) affiche le statut opérationnel de chaque volume.
3. Pour afficher les détails du statut d'un volume spécifique, sélectionnez-le dans la grille et choisissez l'onglet Status checks (Vérifications de l'état).
4. Si vous avez un volume dont la vérification de l'état a échoué (l'état est `impaired`), consultez Travailler avec un volume Amazon EBS endommagé.

Vous pouvez aussi choisir Événements dans le navigateur pour afficher tous les événements de vos instances et volumes. Pour plus d'informations, consultez Événements liés au volume Amazon EBS.

AWS CLI

Pour afficher les informations de statut du volume

Utilisez la commande describe-volume-status.

Pour plus d'informations sur ces interfaces de ligne de commande, consultez Access Amazon EBS.

Tools for Windows PowerShell

Pour afficher les informations de statut du volume

Utilisez la commande Get-EC2VolumeStatus.

Pour plus d'informations sur ces interfaces de ligne de commande, consultez Access Amazon EBS.

Événements liés au volume Amazon EBS

Lorsqu'Amazon EBS détermine que les données d'un volume sont potentiellement incohérentes, il désactive par défaut les E/S vers le volume à partir de toute EC2 instance attachée. Il s'ensuit que le contrôle du statut du volume échoue et qu'un événement de statut de volume est créé indiquant la raison de l'échec.

Pour activer automatiquement les I/O sur un volume avec des incohérences de données potentielles, changez le paramètre de l'attribut de volume Auto-Enabled IO (Activation automatique des I/O) (`autoEnableIO` dans l'API). Pour plus d'informations sur la modification de cet attribut, consultez Travailler avec un volume Amazon EBS endommagé.

Chaque événement inclut une heure de début qui indique l'heure à laquelle l'événement s'est produit, ainsi qu'une durée qui spécifie combien de temps les I/O du volume ont été désactivées. L'heure de fin est ajoutée à l'événement quand les I/O du volume sont activées.

Les événements de statut de volume incluent l'une des descriptions suivantes :

`Awaiting Action: Enable IO`

Les données du volume sont potentiellement incohérentes. Les I/O sont désactivées pour le volume jusqu'à ce que vous les activiez explicitement. La description de l'événement devient IO Enabled après que vous avez explicitement activé les I/O.

`IO Enabled`

Les opérations d'I/O ont été explicitement activées pour ce volume.

`IO Auto-Enabled`

Les opérations d'I/O ont été automatiquement activées sur ce volume après qu'un événement s'est produit. Nous vous recommandons de vérifier leurs incohérences avant de continuer à utiliser les données.

`Normal`

Pour les volumes `io1`, `io2` et `gp3` uniquement. Performances du volume telles qu'attendues.

`Degraded`

Pour les volumes `io1`, `io2` et `gp3` uniquement. Performances du volume inférieures aux attentes.

`Severely Degraded`

Pour les volumes `io1`, `io2` et `gp3` uniquement. Performances du volume bien inférieures aux attentes.

`Stalled`

Pour les volumes `io1`, `io2` et `gp3` uniquement. Performances du volume profondément impactées.

Vous pouvez afficher les événements de vos volumes au moyen des méthodes suivantes.

Console

Pour afficher les événements de vos volumes

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Événements. Tous les volumes et instances ayant des événements sont affichés.

3. Vous pouvez filtrer par volume pour n'afficher que le statut de volume. Vous pouvez aussi filtrer sur des types de statut spécifiques.
4. Sélectionnez un volume pour afficher son événement spécifique.

AWS CLI

Pour afficher les événements de vos volumes

Utilisez la commande describe-volume-status.

Pour plus d'informations sur ces interfaces de ligne de commande, consultez Access Amazon EBS.

Tools for Windows PowerShell

Pour afficher les événements de vos volumes

Utilisez la commande Get-EC2VolumeStatus.

Pour plus d'informations sur ces interfaces de ligne de commande, consultez Access Amazon EBS.

Si vous avez un volume où les I/O sont désactivées, consultez Travailler avec un volume Amazon EBS endommagé. Si vous avez un volume où les performances des I/O sont inférieures à la normale, il peut s'agir d'une condition temporaire due à une action que vous avez prise (par exemple, création d'un instantané d'un volume lors d'une utilisation de pointe, exécution du volume sur une instance qui ne peut pas prendre en charge la bande passante d'I/O requise ou premier accès aux données du volume).

Travailler avec un volume Amazon EBS endommagé

Cette section présente vos options si un volume est dégradé flottee que ses données sont potentiellement incohérentes.

Options

- Option 1 : exécuter un contrôle de cohérence sur le volume attaché à son instance
- Option 2 : exécuter un contrôle de cohérence sur le volume à l'aide d'une autre instance
- Option 3 : supprimer le volume si vous n'en avez plus besoin

Option 1 : exécuter un contrôle de cohérence sur le volume attaché à son instance

L'option la plus simple consiste à activer les E/S, puis à effectuer un contrôle de cohérence des données sur le volume alors que celui-ci est toujours attaché à son EC2 instance Amazon.

Pour exécuter un contrôle de cohérence sur un volume attaché

1. Arrêtez l'utilisation du volume par les applications.
2. Activez les I/O sur le volume. Utilisez l'une des méthodes suivantes.

   Console

   1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
   2. Dans le volet de navigation, sélectionnez Events (Évènements).
   3. Sélectionnez le volume sur lequel vous souhaitez activer les opérations d'I/O.
   4. Choisissez Actions, Enable I/O (Activer les I/O).

   AWS CLI

   Pour activer les E/S pour un volume doté du AWS CLI

   Utilisez la commande enable-volume-io.

   Tools for Windows PowerShell

   Pour activer les E/S d'un volume à l'aide des outils pour Windows PowerShell

   Utilisez la commande Enable-EC2VolumeIO.
3. Vérifiez les données du volume.

   a. Exécutez la commande fsck (instances Linux) ou chkdsk (instances Windows).

   b. (Facultatif) Recherchez dans les journaux des applications journaux système disponibles les messages d'erreur appropriés.

   c. Si le volume est réduit depuis plus de 20 minutes, vous pouvez contacter le AWS Support Center. Sélectionnez Dépannage puis, dans la boîte de dialogue Dépanner les contrôles de statut, sélectionnez Contactez Support pour soumettre une demande de support.

Option 2 : exécuter un contrôle de cohérence sur le volume à l'aide d'une autre instance

Utilisez la procédure suivante pour vérifier le volume en dehors de votre environnement de production.

> **Important**
>
> Cette procédure peut entraîner la perte d'I/O en écriture suspendues quand les I/O du volume ont été désactivées.

Pour exécuter un contrôle de cohérence sur un volume isolé

1. Arrêtez l'utilisation du volume par les applications.
2. Détachez le volume de l'instance. Pour plus d'informations, consultez Détacher un volume Amazon EBS d'une instance Amazon EC2 .
3. Activez les I/O sur le volume. Utilisez l'une des méthodes suivantes.

   Console

   1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
   2. Dans le volet de navigation, sélectionnez Events (Évènements).
   3. Sélectionnez le volume que vous avez détaché à l'étape précédente.
   4. Choisissez Actions, Enable I/O (Activer les I/O).

   AWS CLI

   Pour activer les E/S pour un volume doté du AWS CLI

   Utilisez la commande enable-volume-io.

   Tools for Windows PowerShell

   Pour activer les E/S d'un volume à l'aide des outils pour Windows PowerShell

   Utilisez la commande Enable-EC2VolumeIO.
4. Attachez le volume à une autre instance. Pour plus d'informations, consultez Lancer votre instance etAssocier un volume Amazon EBS à une instance Amazon EC2 .

5. Vérifiez les données du volume.

   a. Exécutez la commande fsck (instances Linux) ou chkdsk (instances Windows).

   b. (Facultatif) Recherchez dans les journaux des applications journaux système disponibles les messages d'erreur appropriés.

   c. Si le volume est réduit depuis plus de 20 minutes, vous pouvez contacter le AWS Support Center. Sélectionnez Dépannage puis, dans la boîte de dialogue de dépannage, sélectionnez Contactez Support pour soumettre une demande de support.

Option 3 : supprimer le volume si vous n'en avez plus besoin

Si vous voulez supprimer le volume de votre environnement, supprimez-le simplement. Pour plus d'informations sur la suppression d'un volume, consultez Supprimer un volume Amazon EBS.

Si vous avez un instantané récent qui sauvegarde les données sur le volume, vous pouvez créer un volume à partir de l'instantané. Pour de plus amples informations, veuillez consulter Créez un volume Amazon EBS..

Activation automatique des E/S pour les volumes Amazon EBS altérés

Lorsqu'Amazon EBS détermine que les données d'un volume sont potentiellement incohérentes, il désactive par défaut les E/S vers le volume à partir de toute EC2 instance attachée. Il s'ensuit que le contrôle du statut du volume échoue et qu'un événement de statut de volume est créé indiquant la raison de l'échec. Si la cohérence d'un volume particulier ne constitue pas un problème et que vous préfèrerez que le volume soit rendu disponible immédiatement s'il rencontre un problème, vous pouvez remplacer le comportement par défaut en configurant le volume de façon à activer automatiquement les I/O. Si vous activez l'attribut de volume Auto-Enabled I/O (I/O activées automatiquement) (`autoEnableIO` dans l'API), les I/O entre le volume et l'instance sont automatiquement réactivées et le contrôle d'état du volume est passé. De plus, vous remarquerez un événement qui vous permet de savoir que le volume se trouvait dans un état potentiellement incohérent, mais que ses I/O ont été automatiquement activées. Quand cet événement se produit, vous devez vérifier la cohérence du volume et le remplacer si nécessaire. Pour plus d'informations, consultez Événements liés au volume Amazon EBS.

Vous pouvez afficher et modifier l'attribut Auto-Enabled I/O (Activation automatique des I/O) d'un volume au moyen des méthodes suivantes.

Amazon EC2 console

Pour afficher l'attribut Auto-Enabled IO d'un volume

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume et choisissez Status Checks (Vérifications de l'état).

   Le champ Auto-Enabled I/O (Activation automatique des I/O) affiche le paramétrage actuel (Enabled (Activé) ou Disabled (Désactivé)) du volume sélectionné.

Pour modifier l'attribut Auto-Enabled IO d'un volume

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume et choisissez Actions, Manage auto-enabled I/O (Gérer les I/O auto-activées).
4. Cochez la case Auto-Enable Volume I/O (Activer automatiquement les I/O du volume) afin d'activer automatiquement les I/O d'un volume dégradé. Pour désactiver la fonction, décochez la case.
5. Choisissez Mettre à jour.

AWS CLI

Pour afficher l'attribut AutoEnable IO d'un volume

Utilisez la commande describe-volume-attribute.

Pour modifier l'attribut autoEnableIO d'un volume

Utilisez la commande modify-volume-attribute.

Pour plus d'informations sur ces interfaces de ligne de commande, consultez Access Amazon EBS.

Tools for Windows PowerShell

Pour afficher l'attribut AutoEnable IO d'un volume

Utilisez la commande Get-EC2VolumeAttribute.

Pour modifier l'attribut autoEnableIO d'un volume

Utilisez la commande Edit-EC2VolumeAttribute.

Pour plus d'informations sur ces interfaces de ligne de commande, consultez Access Amazon EBS.

Tests de défaillance sur Amazon EBS

Utilisez AWS Fault Injection Service l'action Pause I/O pour arrêter temporairement les E/S entre un volume Amazon EBS et les instances auxquelles il est attaché afin de tester la manière dont vos charges de travail gèrent les interruptions d'E/S. Vous pouvez utiliser des expériences contrôlées pour tester votre architecture et votre surveillance, telles que les CloudWatch alarmes Amazon et les configurations de temporisation du système d'exploitation, et améliorer la résilience face aux défaillances de stockage. AWS FIS

Pour plus d'informations AWS FIS, consultez le guide de AWS Fault Injection Service l'utilisateur.

Considérations

Gardez à l'esprit les considérations suivantes pour mettre en pause les E/S de volume :

- Vous pouvez suspendre les E/S pour tous les types de volumes Amazon EBS attachés à des instances créées sur le système Nitro.
- Vous pouvez mettre en pause les E/S pour le volume racine.
- Vous pouvez mettre en pause les E/S pour les volumes activés par Multi-Attach. Si vous mettez en pause les E/S pour un volume activé par Multi-Attach, les E/S sont mises en pause entre le volume et toutes les instances auxquelles il est attaché.
- Pour tester la configuration du délai d'attente de votre système d'exploitation, définissez une durée d'expérience égale ou supérieure à la valeur spécifiée pour `nvme_core.io_timeout`. Pour de plus amples informations, veuillez consulter NVMe Délai d'expiration des opérations d'E/S pour les volumes Amazon EBS.
- Si vous dirigez les E/S vers un volume dont les E/S sont en pause, il se produit ce qui suit :
  - Le statut du volume passe à `impaired` dans les 120 secondes. Pour de plus amples informations, veuillez consulter Contrôles de l'état des volumes Amazon EBS.
  - Les CloudWatch métriques relatives à la longueur de la file d'attente (`VolumeQueueLength`) ne seront pas nulles. Toutes les alarmes et tous les contrôles doivent surveiller une profondeur

de file d'attente non nulle. Pour plus d'informations, voir Mesures relatives aux EBS volumes Amazon.

- Les CloudWatch métriques pour `VolumeReadOps` ou `VolumeWriteOps` seront`0`, ce qui indique que le volume ne traite plus les E/S.

Limites

Gardez à l'esprit les limitations suivantes pour la mise en pause des E/S de volume :

- Les volumes de stockage d'instances ne sont pas pris en charge.
- Les types d'instances basés sur Xen ne sont pas pris en charge.
- Vous ne pouvez pas suspendre les E/S pour les volumes créés sur un avant-poste situé dans AWS Outposts, dans une AWS Wavelength zone ou dans une zone locale.

Vous pouvez effectuer un test de base depuis la EC2 console Amazon, ou vous pouvez effectuer des tests plus avancés à l'aide de la AWS FIS console. Pour plus d'informations sur la réalisation d'expériences avancées à l'aide de la AWS FIS console, consultez les AWS FIS didacticiels du guide de AWS Fault Injection Service l'utilisateur.

Pour effectuer une expérience de base à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Volumes.
3. Sélectionnez le volume pour lequel vous voulez interrompre les E/S et choisissez Actions, Injection de fautes, Interrompre les E/S du volume.
4. Dans le champ Durée, saisissez la durée de la pause des E/S entre le volume et les instances. Le champ situé à côté de la liste déroulante Durée indique la durée au format ISO 8601.
5. Dans la section Accès au service, sélectionnez le rôle de service IAM AWS FIS à assumer pour réaliser l'expérience. Vous pouvez utiliser le rôle par défaut ou un rôle existant que vous avez créé. Pour plus d'informations, consultez Création d'un rôle IAM pour les expériences AWS FIS.
6. Sélectionnez Interrompre les E/S du volume. Lorsque vous y êtes invité, saisissez `start` dans la zone de confirmation et sélectionnez Lancer l'expérience.
7. Surveillez la progression et l'impact de votre expérience. Pour plus d'informations, consultez Surveillance de AWS FIS dans le Guide de l'utilisateur AWS FIS .

Instantanés Amazon EBS

Vous pouvez sauvegarder les données de vos volumes Amazon EBS en créant des point-in-time copies, appelées instantanés Amazon EBS. Un instantané est une sauvegarde incrémentielle, ce qui signifie que nous enregistrons uniquement les blocs du volume qui ont changé depuis le dernier instantané. Cela réduit le temps nécessaire pour créer l'instantané, ainsi que les coûts de stockage en ne dupliquant pas les données.

> **Important**
>
> AWS ne sauvegarde pas automatiquement les données stockées sur vos volumes EBS. Pour garantir la résilience des données et la reprise après sinistre, il est de votre responsabilité de créer régulièrement des instantanés EBS, ou de configurer la création automatique d'instantanés à l'aide d'Automatisez les sauvegardes avec Amazon Data Lifecycle Manager or d'AWS Backup.

Les instantanés sont stockés dans Amazon S3, dans des compartiments S3 auxquels vous ne pouvez pas accéder directement. Vous pouvez créer et gérer vos instantanés à l'aide de la EC2 console Amazon ou de l' EC2 API Amazon. Vous ne pouvez pas accéder à vos instantanés via la console Amazon S3 ou l'API Amazon S3.

Les données des instantanés sont automatiquement répliquées dans toutes les zones de disponibilité de la région. Cela garantit une disponibilité et une durabilité élevées pour les données instantanées et vous permet de restaurer des volumes dans toutes les zones de disponibilité de cette région.

Chaque instantané contient toutes les informations nécessaires à la restauration de vos données (à partir du moment où l'instantané a été pris) sur un nouveau volume EBS. Lorsque vous créez un volume EBS à partir d'un instantané, le nouveau volume commence comme une réplique exacte du volume qui a été utilisé pour créer l'instantané.

Pour plus d'informations, consultez la page produit des Instantanés Amazon EBS.

Événements d'instantané

Vous pouvez suivre l'état de vos instantanés EBS via CloudWatch Events. Pour de plus amples informations, veuillez consulter EBSévénements instantanés.

Tarification des instantanés

Les frais pour vos instantanés sont basés sur la quantité de données stockées. Étant donné que les instantanés sont incrémentiels, la suppression d'un instantané risque de ne pas réduire vos coûts de stockage des données. Les données référencées exclusivement par un instantané sont supprimées lorsque cet instantané est supprimé, mais les données référencées par d'autres instantanés sont conservées. Pour plus d'informations, consultez Volumes et instantanés Amazon Elastic Block Store dans le Guide de l'utilisateur AWS Billing .

Table des matières

Comment fonctionnent les instantanés Amazon EBS

Le premier instantané que vous créez à partir d'un volume est toujours un instantané complet. Il inclut tous les blocs de données écrits sur le volume au moment de la création de l'instantané. Les instantanés suivants du même volume sont des instantanés incrémentiels. Ils incluent uniquement les blocs de données modifiés et nouveaux écrits sur le volume depuis la création du dernier instantané

La taille d'un instantané complet est déterminée par la taille des données sauvegardées, et non par la taille du volume source. De même, les coûts de stockage associés à un instantané complet sont déterminés par la taille de l'instantané, et non par la taille du volume source. Par exemple, vous créez le premier instantané d'un volume Amazon EBS `200 GiB` qui ne contient que `50 GiB` de données. Il en résulte un instantané complet d'une taille de `50 GiB`, et vous êtes facturé pour un stockage d'instantané de `50 GiB`.

De même, la taille et les coûts de stockage d'un instantané incrémentiel sont déterminés par la taille des données écrites sur le volume depuis la création du cliché précédent. En poursuivant cet exemple, si vous créez un deuxième instantané du volume de `200 GiB` après avoir modifié `20 GiB` de données et ajouté `10 GiB` de données, l'instantané incrémentiel a une taille de `30 GiB`. Vous êtes alors facturé pour ce stockage d'instantané supplémentaire de `30 GiB`.

Pour plus d'informations sur la tarification des instantanés, consultez Tarification Amazon EBS.

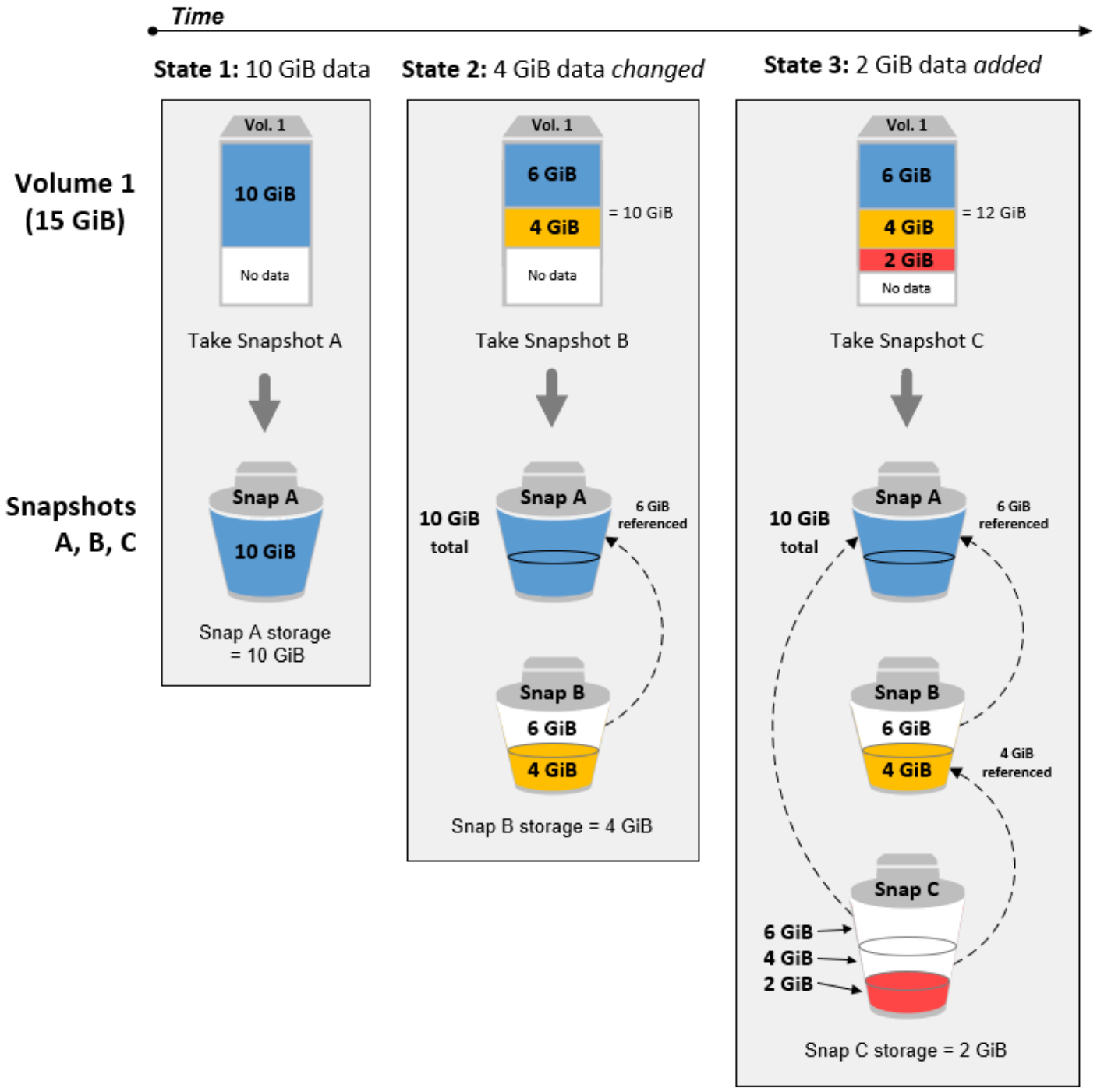
> **Important**
>
> Lorsque vous archivez un instantané incrémentiel, il est converti en instantané complet qui inclut tous les blocs écrits sur le volume au moment de la création de l'instantané. Il est ensuite déplacé vers le niveau Amazon EBS Snapshots Archive. Les instantanés du niveau d'archivage sont facturés à un tarif différent de celui des instantanés du niveau standard. Pour de plus amples informations, veuillez consulter Tarification et facturation pour l'archivage des instantanés Amazon EBS.

Les sections suivantes montrent comment un instantané EBS capture l'état d'un volume à un moment donné et dont des instantanés ultérieurs d'un volume modifié crée un historique de ces modifications.

Plusieurs instantanés d'un même volume

Le diagramme ci-dessous montre le Volume 1, d'une taille de 15 GiB, à trois moments différents. Un instantané de chacun de ces trois états du volume est pris. Le diagramme décrit spécifiquement les éléments suivants :

- Dans l'état State 1, le volume contient 10 GiB de données. Snap A est le premier instantané pris du volume. Snap A est un instantané complet et la totalité des 10 GiB de données est sauvegardée.
- Dans l'état State 2, le volume contient toujours 10 GiB de données, mais seuls 4 GiB ont changé depuis la prise de Snap A. Snap B est un instantané incrémentiel. Il ne doit sauvegarder que les 4 GiB qui ont changé. Les autres 6 GiB de données inchangées, qui sont déjà sauvegardées dans Snap A, sont référencées par Snap B au lieu d'être sauvegardées à nouveau. Ceci est indiqué par la flèche en pointillé.
- Dans l'état State 3, 2 GiB de données ont été ajoutés au volume, pour un total de 12 GiB, après que Snap B a été pris. Snap C est un instantané incrémentiel. Il ne doit sauvegarder que les 2 GiB qui ont été ajoutés après la prise de Snap B. Comme le montrent les flèches en pointillé, Snap C référence également les 4 GiB de données stockées dans Snap B et les 6 GiB de données stockées dans Snap A.
- L'espace de stockage total nécessaire pour les trois instantanés est de 16 GiB. Cela représente 10 Gio pour Snap A, 4 Gio et 2 Gio pour Snap C.



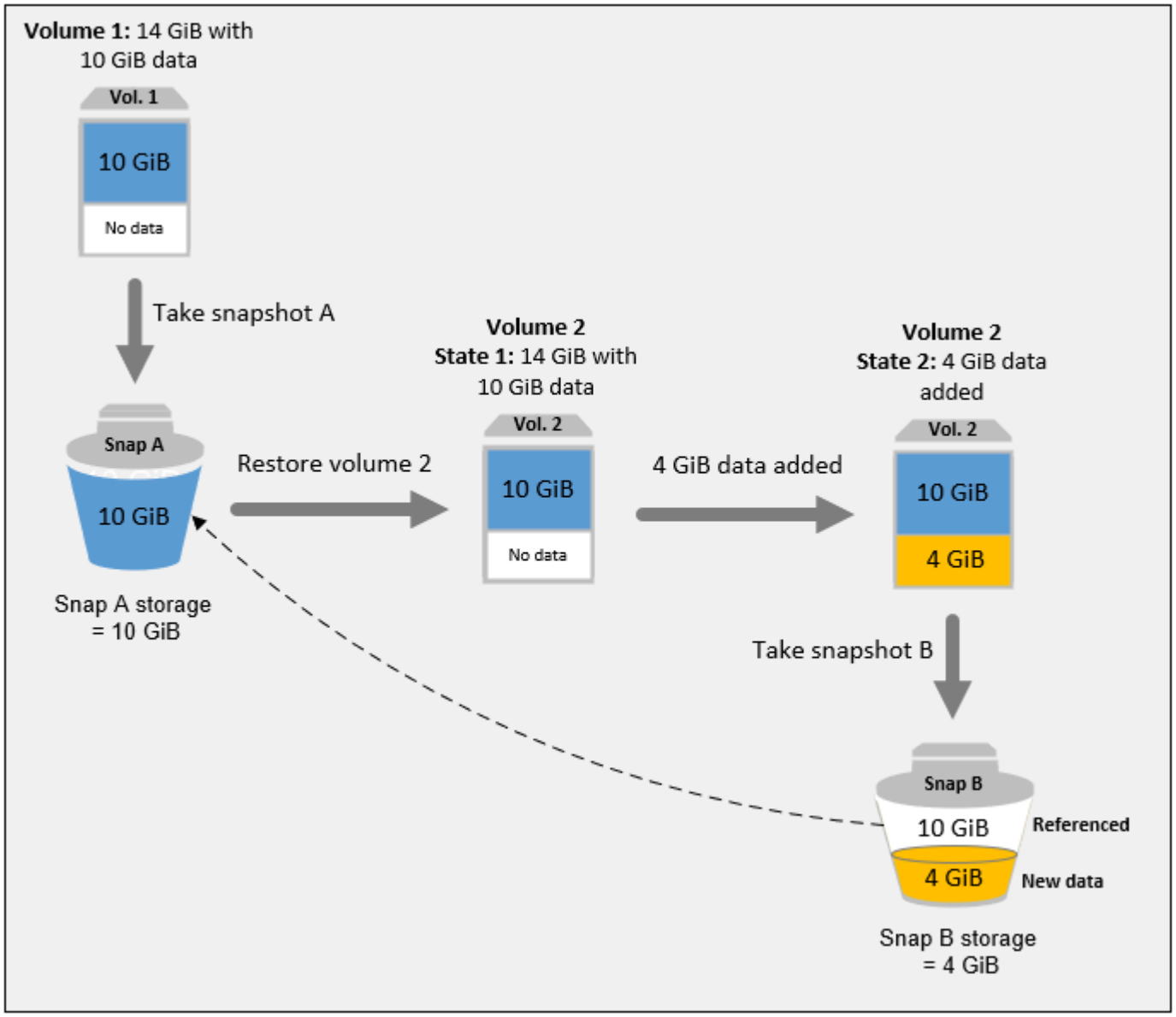
Instantanés incrémentiels de différents volumes

Le diagramme de cette section montre comment les instantanés incrémentiels peuvent être pris à partir de différents volumes.

1. Vol 1, qui a une taille de 14 GiB, contient 10 GiB de données. Snap A étant le premier instantané du volume, il s'agit d'un instantané complet et la totalité des 10 GiB de données est sauvegardée.
2. Vol 2 est créé à partir de Snap A, il s'agit donc d'une réplique exacte de Vol 1 au moment de la prise de l'instantané.
3. Au fil du temps, 4 GiB de données sont ajoutés au Vol 2 et la taille totale de ses données est de 14 GiB.
4. Snap B est pris de Vol 2. Pour Snap B, seuls les 4 GiB de données qui ont été ajoutées après la création du volume à partir de Snap A sont sauvegardées. Les autres 10 GiB de données non modifiées qui avaient déjà été copiés et stockés dans Snap A, sont référencés par Snap B au lieu d'être sauvegardée à nouveau.

   Snap B est un instantané incrémentiel de Snap A, même s'il a été créé à partir d'un volume différent.

> **Important**
>
> Le diagramme suppose que vous possédez Vol 1 et Snap A, et que Vol 2 est chiffré avec la même clé KMS que Vol 1. Si le vol 1 appartenait à un autre AWS compte et que ce compte utilisait Snap A et le partageait avec vous, alors Snap B serait un instantané complet. Ou, si Vol 2 était chiffré avec une clé KMS différente de Vol 1, alors Snap B serait un instantané complet.



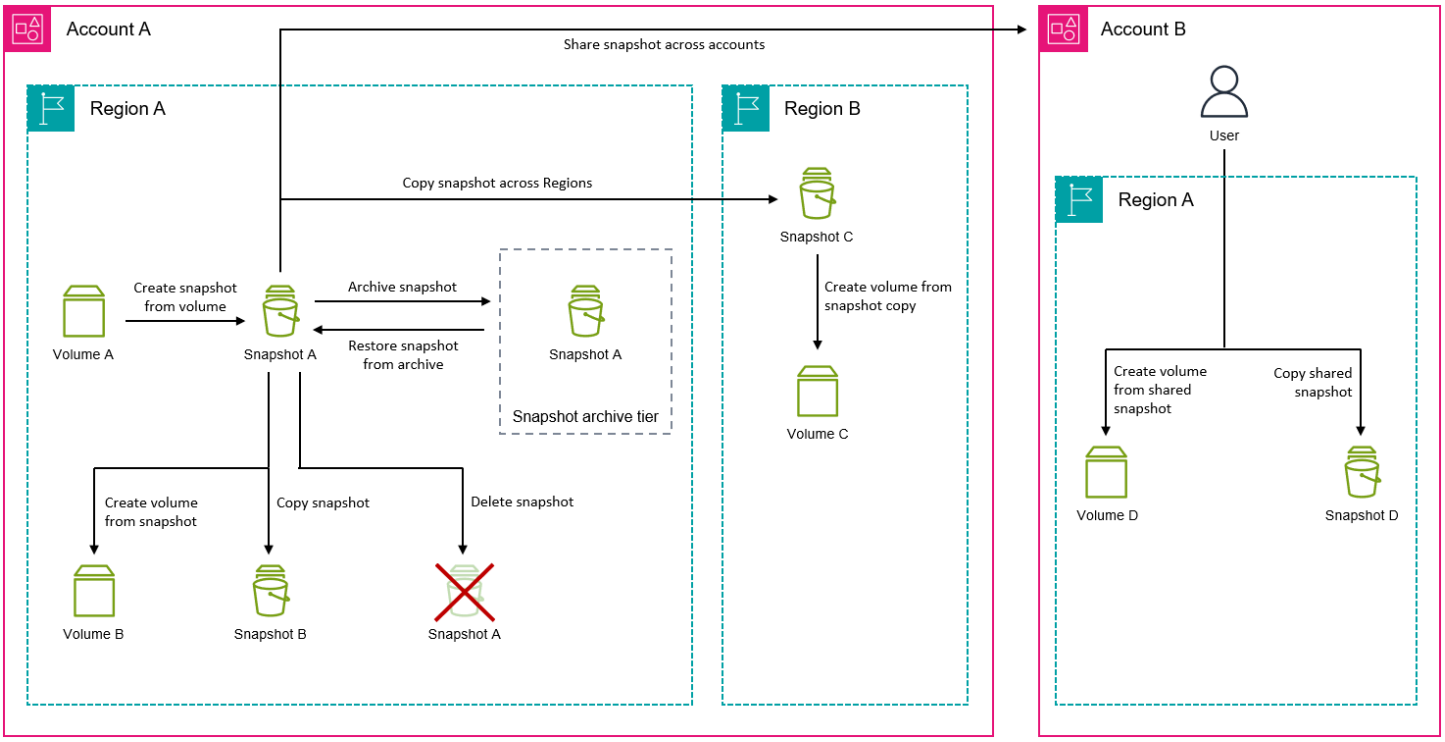
Pour plus d'informations sur la façon dont les données sont gérées lorsque vous supprimez un instantané, consultez Supprimer un instantané Amazon EBS.

Cycle de vie des snapshots Amazon EBS

Le cycle de vie d'un instantané Amazon EBS commence par le processus de création. Vous créez des instantanés à partir de volumes Amazon EBS. Vous pouvez utiliser des instantanés pour restaurer de nouveaux volumes Amazon EBS. Vous pouvez créer des copies d'instantanés dans la même région ou dans différentes régions. Vous pouvez partager des instantanés avec d'autres personnes Comptes AWS, en public ou en privé. Ces comptes peuvent restaurer des volumes à partir des instantanés partagés ou créer des copies des instantanés partagés dans leur propre

compte. Si vous n'avez pas besoin d'un accès immédiat à un instantané, vous pouvez l'archiver pour économiser sur les coûts de stockage.

L'image suivante montre les actions que vous pouvez effectuer sur vos instantanés dans le cadre du cycle de vie des instantanés.



Tâches

- Créer des instantanés Amazon EBS
- Afficher les informations d'instantané Amazon EBS
- Copier un instantané Amazon EBS
- Partager un instantané Amazon EBS avec d'autres comptes AWS
- Archiver des instantanés Amazon EBS
- Supprimer un instantané Amazon EBS

Créer des instantanés Amazon EBS

Vous pouvez créer un instantané Amazon EBS d'un volume Amazon EBS pour créer une point-in-time sauvegarde de ce volume. Vous pouvez soit créer des instantanés de volumes Amazon EBS individuels, soit créer des instantanés multi-volumes de tous les volumes attachés à une instance Amazon ou d'un sous-ensemble de ceux-ci. EC2

La création de snapshots est asynchrone. L'instantané est créé immédiatement, mais il reste dans `pending` cet état jusqu'à ce que toutes les données aient été transférées vers Amazon S3. Cette opération peut prendre plusieurs heures, selon le nombre de blocs modifiés sur le volume. Vous pouvez continuer à utiliser le volume pendant cette période sans affecter le cliché. L'instantané inclut uniquement les données écrites sur le volume au moment où l'instantané a été demandé. Il n'inclut pas les données mises en cache par les applications ou le système d'exploitation.

> **Tip**
>
> Pour garantir des instantanés cohérents et complets, nous vous recommandons de suspendre les écritures sur le volume avant de créer l'instantané. Si vous ne pouvez pas suspendre les écritures sur le volume, nous vous recommandons de démonter le volume, depuis l'instance, avant de créer l'instantané. Vous pouvez remonter et reprendre les écritures une fois que le cliché est entré dans l'`pending`état.
> Si vous créez un instantané d'un volume qui sert de périphérique racine à une EC2 instance Amazon, nous vous recommandons d'arrêter l'instance avant de prendre l'instantané.

Rubriques

Chiffrement des instantanés

Un instantané reçoit automatiquement le même état de chiffrement que le volume à partir duquel il a été créé. Les instantanés créés à partir de volumes non chiffrés ne sont pas chiffrés. Les instantanés créés à partir de volumes chiffrés sont automatiquement chiffrés à l'aide de la même clé KMS que le volume.

> **Tip**
>
> Si vous devez créer un instantané chiffré à partir d'un volume non chiffré, créez d'abord l'instantané non chiffré du volume, puis créez une copie chiffrée de cet instantané.

Destinations d'instantanés

L'emplacement de la ressource source (volume ou instance) détermine l'endroit où vous pouvez créer des instantanés.

- Si la ressource source se trouve dans une région, vous devez créer des instantanés dans la même région que la ressource source.
- Si la ressource source se trouve dans une zone locale, vous pouvez créer des instantanés dans la même zone locale ou dans sa région parente. Pour de plus amples informations, veuillez consulter Instantanés locaux dans des zones locales dédiées.
- Si la ressource source se trouve sur un avant-poste, vous pouvez créer des instantanés sur le même avant-poste ou dans sa région parente. Pour de plus amples informations, veuillez consulter Amazon EBS local snapshots on Outposts.

Automatisation des instantanés

Vous pouvez automatiser la création de snapshots à l'aide d'Amazon Data Lifecycle Manager et AWS Backup.

Considérations relatives à la création d'instantanés

- Nous vous recommandons de ne pas créer d'instantanés de volumes attachés à des EC2 instances Amazon qui sont mises en veille prolongée ou dont l'hibernation est activée. Pour plus d'informations, consultez Comment fonctionne l'hibernation des EC2 instances Amazon.
- Bien que vous puissiez prendre un instantané d'un volume alors qu'un instantané précédent de ce volume est en `pending` état, le fait d'avoir plusieurs instantanés dans `pending` cet état pour le même volume peut entraîner une réduction des performances du volume jusqu'à ce que les instantanés soient terminés.
- Il existe des limites quant au nombre de clichés que vous pouvez avoir dans `pending` cet état et au nombre de clichés simultanés que vous pouvez demander par type de volume. Pour plus

d'informations, consultez la section Quotas pour Amazon EBS. Si vous dépassez l'un de ces quotas, attendez que les instantanés actuels soient terminés, puis réessayez.

Création d'un instantané Amazon EBS d'un volume EBS

Pour créer un instantané d'un volume individuel, appliquez l'une des méthodes suivantes.

Console

Pour créer un instantané avec la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés), Create snapshot (Créer un instantané).
3. Pour Type de ressource, choisissez Volume.
4. Pour Volume ID (ID de volume), sélectionnez le volume à partir duquel créer l'instantané. Le champ Chiffrement indique le volume et l'état de chiffrement de l'instantané obtenu. Il ne peut pas être modifié.
5. (Facultatif) Dans Description, entrez une brève description de l'instantané.
6. Si le volume se trouve sur un avant-poste ou dans une zone locale, le champ Destination du cliché apparaît. Effectuez l'une des actions suivantes :
   - Si le volume se trouve dans une zone locale, choisissez Zone locale pour créer le cliché dans la même zone locale, ou choisissez AWS Région pour créer le cliché dans la région parent de la zone locale.
   - Si le volume se trouve sur un avant-poste, choisissez AWS Outpost, pour créer l'instantané sur le même avant-poste, ou choisissez AWS Region pour créer l'instantané dans la région parent de l'avant-poste.

> **Note**
>
> Si le volume se trouve dans une région, la destination du snapshot n'apparaît pas. L'instantané est automatiquement créé dans la même région que le volume.

7. (Facultatif) Pour attribuer des balises personnalisées à l'instantané, dans la section Balises, choisissez Ajouter une balise, puis entrez la paire clé-valeur. Vous pouvez ajouter jusqu'à 50 balises.
8. Choisissez Créer un instantané.

Command line

Pour créer un instantané à l'aide du AWS CLI

Utilisez la commande create-snapshot.

Pour créer un instantané à l'aide des outils pour Windows PowerShell

Utilisez la commande New-EC2Snapshot.

Créez des instantanés Amazon EBS en plusieurs volumes à partir d'une instance Amazon EC2

Par défaut, lorsque vous créez des instantanés multi-volumes à partir d'une EC2 instance Amazon, Amazon EBS crée des instantanés de tous les volumes Amazon EBS attachés à l'instance. Toutefois, vous pouvez choisir d'exclure le volume racine ou des volumes de données spécifiques si nécessaire.

> **Tip**
>
> Nous vous recommandons de baliser vos instantanés multivolumes afin de pouvoir facilement les identifier et les gérer collectivement. Vous pouvez également copier les balises des volumes source vers les instantanés correspondants afin de définir les métadonnées des instantanés, telles que les politiques d'accès, les informations relatives aux pièces jointes et la répartition des coûts, afin qu'elles correspondent au volume source.

Considérations relatives aux instantanés en plusieurs volumes

- Si tous les instantanés se terminent correctement, un `createSnapshots` CloudWatch événement ayant pour résultat `succeeded` est envoyé à votre AWS compte. Si l'un des instantanés du jeu d'instantanés multivolumes échoue, tous les autres instantanés entrent dans l'`error`état et un `createSnapshots` CloudWatch événement ayant pour résultat `failed` est envoyé à

votre compte. Pour de plus amples informations, veuillez consulter Créer des instantanés () createSnapshots.

- Les instantanés multi-volumes prennent en charge jusqu'à 128 volumes Amazon EBS attachés à une instance, y compris le volume racine, et jusqu'à 127 volumes de données.
- Chaque instantané de l'ensemble d'instantanés en plusieurs volumes est un instantané individuel qui peut être utilisé de la même manière et qui prend en charge les mêmes fonctionnalités qu'un instantané individuel.
- Vous pouvez prendre des instantanés cohérents avec les applications de tous les volumes Amazon EBS attachés à une instance Amazon EC2 Windows à l'aide de documents de commande.AWS Systems Manager

Pour créer des instantanés multivolumes à partir d'une instance, appliquez l'une des méthodes suivantes.

Console

Pour créer des instantanés multi-volumes à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots (Instantanés), Create snapshot (Créer un instantané).
3. Pour Resource type (Type de ressource), choisissez Instance.
4. (Facultatif) Pour Description, saisissez une brève description pour les instantanés. Cette description s'applique à tous les instantanés.
5. Si l'instance se trouve sur un avant-poste ou dans une zone locale, le champ Destination du snapshot apparaît. Effectuez l'une des actions suivantes :
   - Si l'instance se trouve dans une zone locale, choisissez Zone locale pour créer les instantanés dans la même zone locale, ou choisissez AWS Région pour créer les instantanés dans la région parent de la zone locale.
   - Si l'instance se trouve sur un avant-poste, choisissez AWS Outpost pour créer les instantanés sur le même avant-poste, ou choisissez AWS Region pour créer les instantanés dans la région parent de l'avant-poste.

> **Note**
>
> Si l'instance se trouve dans une région, la destination du snapshot n'apparaît pas. L'instantané est automatiquement créé dans la même région que l'instance.

6. (Facultatif) Pour exclure le volume racine de l'instance, sélectionnez Exclure le volume racine.
7. (Facultatif) Pour exclure des volumes de données, sélectionnez Exclure des volumes de données spécifiques. La section Attached data volumes (Volumes de données attachés) répertorie tous les volumes de données qui sont actuellement attachés à l'instance sélectionnée.

   Sélectionnez les volumes de données à exclure. Seuls les volumes qui ne sont pas sélectionnés seront inclus dans l'ensemble d'instantanés multi-volumes.
8. (Facultatif) Pour copier automatiquement les balises des volumes source vers les instantanés correspondants, pour Copier les balises depuis le volume source, sélectionnez Copier les balises.
9. (Facultatif) Pour attribuer des balises personnalisées supplémentaires aux instantanés, dans la section Balises, choisissez Ajouter une balise, puis entrez la paire clé-valeur. Vous pouvez ajouter jusqu'à 50 balises.
10. Choisissez Créer un instantané.

Command line

Pour créer des instantanés en plusieurs volumes à l'aide du AWS CLI

Utilisez la commande create-snapshots.

Pour exclure le volume racine, pour`--instance-specification ExcludeBootVolume`, spécifie`true`. Pour exclure des volumes de données`--instance-specification ExcludeDataVolumes`, pour, spécifiez les volumes IDs de données à exclure.

Pour créer des instantanés en plusieurs volumes à l'aide des Outils pour Windows PowerShell

Utilisez la commande New-EC2SnapshotBatch.

Pour exclure le volume racine, pour`-InstanceSpecification_ExcludeBootVolume`, spécifiez`1`. Pour exclure des volumes de données-`InstanceSpecification_ExcludeDataVolumes`, pour, spécifiez les volumes IDs de données à exclure.

Afficher les informations d'instantané Amazon EBS

Vous pouvez afficher des informations détaillées sur vos instantanés à l'aide de l'une des méthodes suivantes.

Console

Pour afficher des informations sur un instantané à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Pour afficher uniquement les instantanés que vous possédez, dans le coin supérieur gauche de l'écran, choisissez Owned by me (M'appartenant). Vous pouvez également filtrer la liste des instantanés en utilisant des identifications et d'autres attributs d'instantanés. Dans le champ Filter (Filtrer), sélectionnez le champ attribut, puis sélectionnez ou saisissez la valeur de l'attribut. Par exemple, pour afficher uniquement des instantanés chiffrés, sélectionnez Encryption (Chiffrement), puis saisissez `true`.
4. Pour afficher des informations supplémentaires sur un instantané spécifique, choisissez son ID dans la liste.

AWS CLI

Pour afficher les informations relatives aux instantanés à l'aide du AWS CLI

Utilisez la commande describe-snapshots.

Example Exemple 1 : filtre basé sur les balises

La commande suivante décrit les instantanés avec la balise Stack=production.

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Example Exemple 2 : filtre basé sur le volume

La commande suivante décrit les instantanés créés à partir du volume spécifié.

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

Example Exemple 3 : filtre basé sur l'ancienneté des instantanés

Avec le AWS CLI, vous pouvez filtrer JMESPath les résultats à l'aide d'expressions. Par exemple, la commande suivante affiche tous IDs les instantanés créés par votre AWS compte (représentés par*123456789012*) avant la date spécifiée (représentée par*2020-03-31*). Si vous ne spécifiez pas le propriétaire, les résultats incluent tous les instantanés publics.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

La commande suivante affiche tous IDs les instantanés créés dans la plage de dates spécifiée.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]"
 --output text
```

Tools for Windows PowerShell

Pour afficher les informations relatives aux instantanés à l'aide des Outils pour Windows PowerShell

Utilisez la commande Get-EC2Snapshot.

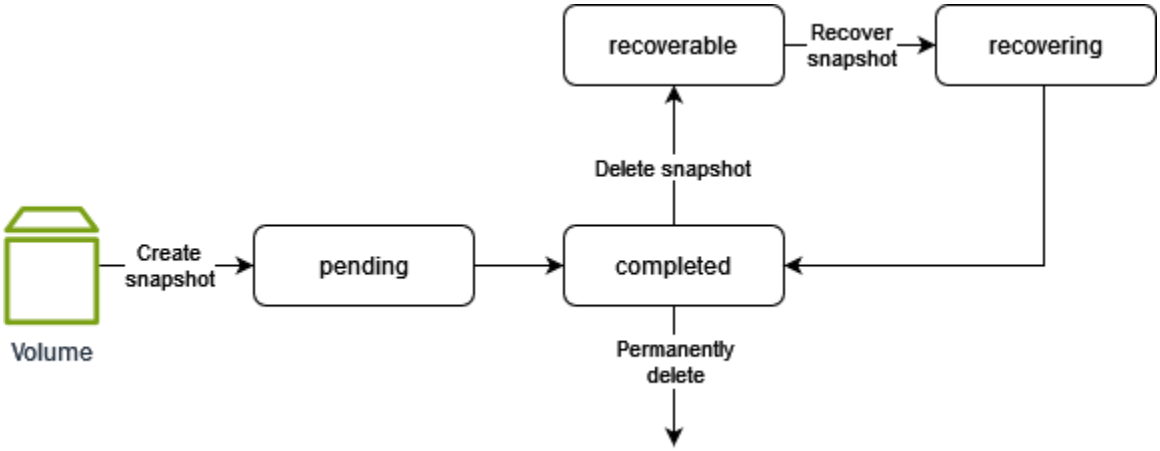
```
PS C:\> Get-EC2Snapshot -SnapshotId snapshot_id
```

États des instantanés

Un instantané Amazon EBS passe par différents états entre le moment où il est créé et celui où il est définitivement supprimé.

L'illustration suivante montre les transitions entre les états des instantanés. Lorsque vous créez un instantané, celui-ci passe à l'`pending`état. Une fois que le cliché est prêt à être utilisé, il passe à l'`completed`état. Lorsque vous avez décidé que vous n'avez plus besoin d'un instantané, vous

pouvez le supprimer. Si vous supprimez un instantané qui correspond à une règle de conservation de la corbeille, il est conservé dans la corbeille et il passe à l'`recoverable`état. Si vous récupérez un instantané depuis la corbeille, il passe à l'`recovering`état puis à l'`completed`état. Dans le cas contraire, il est définitivement supprimé.



Le tableau suivant récapitule les états des instantanés.

État	Description
`pending`	Le processus de création d'un instantané est toujours en cours. Un instantané ne peut pas être utilisé tant qu'il est dans `pending` cet état.
`completed`	Le processus de création d'un instantané est terminé et le cliché est prêt à être utilisé.
`recoverable`	L'instantané se trouve actuellement dans la corbeille. Pour utiliser l'instantané, vous devez d'abord le récupérer depuis la corbeille.
`recovering`	L'instantané est en cours de restauration depuis la corbeille. Une fois l'instantané restauré, il passe à l'`completed` état initial et est prêt à être utilisé.
`error`	Le processus de création d'un instantané a échoué. Un instantané ne peut pas être utilisé s'il est dans `error` cet état.

Copier un instantané Amazon EBS

Une fois que vous avez créé un instantané et qu'il a atteint son `completed` état, vous pouvez le copier d'une AWS région à l'autre, ou au sein de la même région. La copie instantanée est une copie exacte de l'original, mais elle possède un identifiant de ressource unique. Vous pouvez copier des instantanés que vous possédez et des instantanés partagés avec vous, en privé ou en public. Vous devrez peut-être copier un instantané pour les cas d'utilisation suivants :

- Expansion géographique — Vous devez lancer vos applications dans une nouvelle région.
- Migration : vous devez déplacer une application vers une nouvelle région afin d'améliorer la disponibilité ou de minimiser les coûts.
- Reprise après sinistre : vous devez sauvegarder vos données et vos journaux dans des régions secondaires à des fins de redondance des données.
- Chiffrement : vous devez chiffrer un instantané précédemment non chiffré ou rechiffrer un instantané chiffré à l'aide d'une autre clé KMS.
- Copier un instantané partagé : vous devez copier un instantané partagé avec vous.
- Exigences en matière de conservation et d'audit des données : vous devez copier des instantanés chiffrés d'un AWS compte à un autre afin de préserver les données à des fins d'audit ou de conservation des données. L'utilisation d'un autre compte vous protège si votre AWS compte principal est compromis.

Pour copier des instantanés en plusieurs volumes vers une autre AWS région, identifiez tous les instantanés qui font partie de cet ensemble à l'aide des balises que vous avez attribuées lors de la création, puis copiez les instantanés individuellement dans la région requise.

Pour plus d'informations sur la copie d'un instantané Amazon RDS, consultez Copie d'un instantané de base de données dans le Amazon RDS Guide de l'utilisateur.

Tarification

Pour obtenir des informations sur les tarifs relatifs à la copie d'instantanés entre AWS régions et comptes, consultez la section Tarification d'Amazon EBS.

Table des matières

- Copie d'instantané incrémentielle
- Copies temporelles pour les instantanés Amazon EBS
- Chiffrement et copie d'instantanés
- Copie d'un instantané

Considérations relatives à la copie d'instantanés

- Vous pouvez copier des instantanés AWS Marketplace, VM Import/Export et Storage Gateway, mais vous devez vérifier que le snapshot est pris en charge dans la région de destination.
- Il y a une limite de `20` demandes de copie d'instantanés simultanées par Région de destination. Si vous dépassez ce quota, vous recevez une erreur `ResourceLimitExceeded`. Si cette erreur s'affiche, attendez qu'une ou plusieurs des demandes de copie soient terminées avant d'effectuer une nouvelle demande de copie d'instantané.
- Les balises définies par l'utilisateur ne sont pas copiées de l'instantané source vers la copie instantanée. Vous pouvez ajouter des balises définies par l'utilisateur pendant ou après l'opération de copie.
- Les instantanés créés par une opération de copie d'instantané ont un ID de volume arbitraire, tel que `vol-ffff` ou `vol-ffffffff`. Ces volumes arbitraires ne IDs doivent être utilisés à aucune fin.
- Les autorisations au niveau des ressources spécifiées pour l'opération de copie instantanée s'appliquent uniquement à la copie instantanée. Vous ne pouvez pas spécifier d'autorisations au niveau des ressources pour l'instantané source. Pour un exemple, voir Exemple : copie d'instantanés.
- Si vous copiez un instantané activé pour la restauration rapide des instantanés, la copie d'instantané n'est pas automatiquement activée pour la restauration rapide des instantanés. Vous devez explicitement activer la restauration rapide des instantanés pour la copie instantanée.
- Si vous copiez un instantané et le chiffrez dans une nouvelle clé KMS, une copie complète (non incrémentielle) est créée. Cela entraîne des coûts de stockage supplémentaires.
- Si vous copiez un instantané dans une nouvelle région, une copie complète (non incrémentielle) est créée. Cela entraîne des coûts de stockage supplémentaires. Les copies suivantes du même instantané sont incrémentielles.
- Si vous utilisez des transferts de données externes ou interrégionaux, des frais de transfert de EC2 données supplémentaires s'appliqueront. Si vous supprimez des instantanés après le lancement, les données déjà transférées vous seront toujours facturées.

Destinations pour les copies instantanées

L'emplacement de l'instantané source détermine si vous pouvez le copier ou non.

- Si l'instantané source se trouve dans une région, vous pouvez le copier dans cette région, dans une autre région ou dans un avant-poste associé à cette région.
- Si l'instantané source se trouve dans une zone locale, vous ne pouvez pas le copier.
- Si l'instantané source se trouve sur un Outpost, vous ne pouvez pas le copier.

Copie d'instantané incrémentielle

Les opérations de copie instantanée effectuées au sein d'un même compte et d'une même région à l'aide de la même clé KMS sont toujours des copies incrémentielles. Toutefois, si vous chiffrez la copie instantanée à l'aide d'une autre clé KMS, il s'agit d'une copie complète.

Lorsque vous copiez un instantané entre des régions ou des comptes, la copie est une copie incrémentielle si les conditions suivantes sont remplies :

- L'instantané a été préalablement copié dans la région ou le compte de destination.
- La dernière copie d'instantané existe toujours dans la région ou le compte de destination.
- La copie instantanée la plus récente n'a pas été archivée.
- Toutes les copies de l'instantané dans la région ou dans le compte de destination sont soit non chiffrées, soit chiffrées avec la même clé KMS.

> **Tip**
>
> Nous vous recommandons de marquer vos copies instantanées avec l'ID du volume et l'heure de création afin de pouvoir suivre la copie instantanée la plus récente d'un volume dans la région ou le compte de destination.

Pour savoir si vos copies instantanées sont incrémentielles, consultez l'événement CloudWatch CopySnapshot.

Copies temporelles pour les instantanés Amazon EBS

Les copies temporelles peuvent vous aider à répondre aux exigences de conformité ou aux exigences commerciales en matière de réplication des données en garantissant que vos instantanés EBS sont copiés, au sein des AWS régions et entre elles, dans un délai spécifié. La copie d'instantanés basée sur le temps peut également aider les administrateurs de sauvegarde à répondre aux exigences strictes en matière de reprise après sinistre (objectifs de point de restauration et objectifs de temps de restauration), et elle améliore l'agilité du développement en garantissant des temps de copie prévisibles pour les instantanés.

Avec les opérations de copie instantanée basées sur le temps, vous spécifiez une durée d'exécution, comprise entre 15 minutes et 48 heures, pendant laquelle la copie doit être terminée. La durée d'exécution doit être spécifiée par tranches de 15 minutes.

Rubriques

Quotas

Les quotas suivants s'appliquent aux opérations de copie instantanée basées sur le temps :

Quota	Description	Valeur du quota	Ajustable
Quota de débit pour les opérations de copie instantanée	Débit maximal pouvant être atteint par une seule opération de copie instantanée basée sur le temps.	500 Mio/s	Non
Quota de débit cumulé pour les copies de snapshots	Débit cumulé maximal pouvant être atteint par des opérations	2 000 Mbits/s	Oui

Quota	Description	Valeur du quota	Ajustable
	simultanées de copie instantanée basées sur le temps entre une région source et une région de destination.		

Lorsque vous lancez une opération de copie instantanée basée sur le temps, vous spécifiez une durée d'exécution. Le débit utilisé par la demande est déterminé par la taille des données de capture instantanée et la durée d'exécution demandée. Par exemple, si vous copiez un instantané contenant 225 000 MiB (0,214 TiB) de données et que vous demandez une durée d'exécution de 15 minutes, le débit est de 250). MiB/s (225,000 MiB ÷ 15 minutes = 250 MiB/s

Si vous lancez une demande de copie d'instantané basée sur le temps et que votre quota de débit de copie d'instantané cumulé disponible est le suivant :

- supérieur ou égal au débit requis, la copie est terminée dans le délai d'achèvement demandé.
- inférieur au débit requis mais supérieur à zéro, la demande aboutit mais elle prendra plus de temps que ce que vous avez demandé. La copie est terminée en utilisant votre quota de débit disponible.
- zéro (quota atteint), la demande échoue.

Déterminez votre durée de réalisation

La durée d'exécution minimale que vous pouvez demander pour une opération de copie instantanée basée sur le temps est de 15 minutes, et la durée d'exécution maximale que vous pouvez demander est de 48 heures. La durée d'exécution doit être spécifiée par tranches de 15 minutes.

Opérations simultanées de copie d'instantanés basées sur le temps

Vous pouvez effectuer simultanément des opérations de copie d'instantanés basées sur le temps entre les mêmes régions source et de destination, à condition que le débit combiné de toutes les opérations simultanées soit conforme à votre quota de débit cumulé de copies d'instantanés (2 000 Mbits/s par défaut).

Pour déterminer si vous pouvez atteindre la durée d'exécution requise pour vos instantanés existants, divisez la taille combinée de tous vos instantanés par la durée d'exécution requise afin de déterminer le débit requis.

> **Tip**
>
> Si vous ne connaissez pas la taille exacte des données de vos instantanés, vous pouvez plutôt utiliser la taille du volume comme proxy.

```
required throughput rate = combined snapshot size ÷ required completion duration
```

Si le débit requis est inférieur à votre quota de débit cumulé pour les copies d'instantanés, vous pouvez atteindre la durée d'exécution requise. Si le débit requis est supérieur à votre quota de débit cumulé pour les copies d'instantanés, nous vous recommandons de demander une augmentation du quota supérieure d'au moins 10 % au débit requis.

> **Tip**
>
> La EC2 console Amazon fournit un calculateur que vous pouvez utiliser pour vérifier la quantité de données de capture instantanée que vous avez copiées entre deux régions au cours d'une période donnée, ainsi que la durée d'exécution minimale que vous pouvez atteindre pour cette quantité de données, sur la base d'un quota de débit de copies d'instantanés cumulé spécifique. Le calculateur utilise la `SnapshotCopyBytesTransferred` CloudWatch métrique pour calculer les données copiées entre deux régions au cours d'une période. Pour ouvrir le calculateur, dans le panneau de navigation de la EC2 console Amazon, sélectionnez Snapshots, puis choisissez Actions, Lancer le calculateur de durée de copie.

Opérations de copie instantanée individuelles basées sur le temps

Vous pouvez calculer la durée minimale d'exécution d'une opération de copie instantanée individuelle basée sur le temps en divisant la taille des données de capture instantanée par le quota de débit de l'opération de copie instantanée (500 Mbits/s).

> **Tip**
>
> Si vous ne connaissez pas la taille exacte des données de votre instantané, vous pouvez plutôt utiliser la taille du volume comme proxy.

```
minimum completion duration = Max(15 minutes, (snapshot data size ÷ 500 MiB/s)
```

Par exemple, la durée minimale d'exécution d'un instantané contenant 900 000 MiB de données est de 30 minutes.

```
minimum completion duration = Max(15 minutes, (900,000 MiB ÷ 500 MiB/s)
= Max(15 minutes, 30 minutes)
= 30 minutes
```

Considérations

- Vous pouvez lancer des opérations de copie d'instantanés basées sur le temps lorsque vous copiez des instantanés au sein d'une même région ou lorsque vous copiez des instantanés entre régions.
- Si vous lancez deux opérations de copie basées sur le temps pour le même instantané, la durée de fin de la deuxième opération de copie ne commence qu'une fois la première opération de copie terminée.
- Les opérations de copie basées sur le temps ne sont pas prises en charge avec AWS Outposts Local Zones et Wavelength Zones.

Surveillance

Vous pouvez suivre la progression des opérations de copie instantanée basées sur le temps à l'aide de la EC2 console Amazon et du AWS CLI. Dans la console, sélectionnez le cliché puis, dans l'onglet Détails, inspectez le champ Progression. À l'aide du AWS CLI, inspectez l'élément `Progress` de sortie dans la réponse à la commande describe-snapshots.

Vous pouvez vérifier si une opération de copie instantanée basée sur le temps s'est terminée dans le délai d'achèvement demandé en vérifiant la différence entre les heures de début et de fin dans la console ou `StartTime` `CompletionTime` dans la `describe-snapshots` réponse.

Vous pouvez également utiliser l' EventBridge événement `copySnapshot` Amazon pour surveiller le résultat des opérations de copie basées sur le temps. L'événement indique si l'opération est terminée et si la durée d'achèvement demandée a été respectée. Si le délai d'achèvement n'a pas été atteint, l'événement inclut plus d'informations sur la cause. Pour de plus amples informations, veuillez consulter EBSévénements instantanés.

Tarification et facturation

> **Note**
>
> Comme pour les opérations de copie d'instantané standard, si vous copiez un instantané dans une nouvelle région, une copie complète (non incrémentielle) est créée, ce qui entraîne des coûts de stockage supplémentaires. Les copies suivantes du même instantané sont incrémentielles. En outre, si vous utilisez des transferts de données externes ou interrégionaux, des frais de transfert de EC2 données Amazon supplémentaires s'appliqueront.

Des frais supplémentaires s'appliquent pour les opérations de copie instantanée basées sur le temps. Les opérations de copie basées sur le temps sont facturées à un taux basé sur la durée d'exécution demandée, par GiB de données de capture copiées. Les taux fixes sont les suivants :

> **Note**
>
> La durée d'exécution doit être spécifiée par tranches de 15 minutes. La durée minimale d'exécution est de 15 minutes et la durée maximale est de 48 heures.

- 15 minutes — 0,020$ par GiB de données
- 30 minutes et 45 minutes — 0,018$ par GiB de données
- 1 heure à 1 heure 45 minutes — 0,016$ par GiB de données
- 2 heures à 3 heures 45 minutes — 0,014$ par GiB de données
- 4 heures à 7 heures 45 minutes — 0,012$ par GiB de données
- 8 heures à 15 heures 45 minutes — 0,010$ par GiB de données
- 16 heures ou plus : 0,005$ par GiB de données

Par exemple, si vous copiez un instantané contenant 3 000 Go de données avec une durée d'exécution de 8 heures, vous êtes facturé 30$ (0,010$ x 3 000 GiB).

Si vous lancez une opération de copie basée sur le temps, mais que la durée d'achèvement demandée n'est pas atteinte parce que vous avez dépassé un quota, vous êtes facturé sur la base de la durée d'achèvement réelle au lieu de la durée d'achèvement demandée. Par exemple, si vous

demandez une durée d'exécution d'une heure, mais que l'opération se termine en 2 heures, vous êtes facturé sur la base du tarif correspondant à la durée de réalisation de 2 heures.

Si Amazon EBS n'est pas en mesure d'atteindre le délai d'exécution demandé ou si une demande est annulée en raison de problèmes liés au service, aucun frais supplémentaire ne vous sera facturé pour l'opération de copie instantanée basée sur le temps.

Si vous supprimez la copie instantanée alors que l'opération de copie instantanée basée sur le temps est toujours en cours, les données copiées jusque-là vous sont facturées au taux correspondant à la durée d'exécution spécifiée.

Chiffrement et copie d'instantanés

> **Note**
>
> Le chiffrement côté serveur Amazon S3 (AES 256 bits) protège les données d'un instantané en transit pendant une opération de copie.

Vous pouvez créer une copie instantanée chiffrée d'une capture d'écran source non chiffrée. Vous pouvez également chiffrer une copie instantanée à l'aide d'une clé KMS différente de l'instantané source. Cependant, la modification de l'état de chiffrement d'une copie instantanée au cours d'une opération de copie peut entraîner une copie complète (et non incrémentielle), ce qui peut entraîner des frais de transfert de données et de stockage plus élevés.

> **Tip**
>
> Lorsque vous utilisez un instantané chiffré qui est partagé avec vous, nous vous recommandons de le rechiffrer en le copiant et en utilisant une clé KMS dont vous êtes propriétaire. Cela vous protège si la clé KMS d'origine est compromise ou si le propriétaire révoque votre accès, ce qui pourrait vous faire perdre l'accès à l'instantané et aux volumes chiffrés que vous avez créés à partir de celui-ci.

Autorisations pour copier des instantanés chiffrés

Pour copier un instantané chiffré, votre utilisateur doit disposer des autorisations suivantes pour utiliser le chiffrement Amazon EBS.

- • `kms:DescribeKey`
  - `kms:CreateGrant`
  - `kms:GenerateDataKey`
  - `kms:GenerateDataKeyWithoutPlaintext`
  - `kms:ReEncrypt`
  - `kms:Decrypt`
- Pour copier un instantané chiffré partagé depuis un autre AWS compte, vous devez être autorisé à utiliser la clé gérée par le client qui a été utilisée pour chiffrer cet instantané. Pour de plus amples informations, veuillez consulter Partagez la clé KMS utilisée pour chiffrer un instantané Amazon EBS partagé.

Résultats du chiffrement pour les copies instantanées

Le tableau suivant décrit les résultats du chiffrement lorsque vous copiez des instantanés dont vous êtes le propriétaire et des instantanés partagés avec vous.

Chiffrement par défaut pour la région de destination	Aperçu de la source	Résultat du chiffrement des copies instantanées	Remarque
Désactivées	Non chiffré	Chiffrement optionnel	Si vous chiffrez la copie, vous pouvez spécifier la clé KMS à utiliser. Si vous chiffrez la copie sans spécifier de clé KMS, le Clé gérée par AWS (`aws/ebs`) est utilisé.
Désactivées	Chiffré	Chiffré automatiquement	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, le Clé gérée par AWS (`aws/ebs`) est utilisé.
Activées	Non chiffré	Chiffré automatiquement	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.

Chiffrement par défaut pour la région de destination	Aperçu de la source	Résultat du chiffrement des copies instantanées	Remarque
Activées	Chiffré	Chiffré automatiquement	Vous pouvez spécifier la clé KMS à utiliser. Si vous ne spécifiez pas de clé KMS, la clé spécifiée pour le chiffrement par défaut est utilisée.

Copie d'un instantané

Pour copier un instantané, utilisez l'une des méthodes suivantes.

Console

Pour copier un instantané à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané à copier, puis choisissez Actions, Copy snapshot (Copier l'instantané).
4. Pour Description, saisissez une brève description de la copie de l'instantané.

   Par défaut, la description inclut des informations sur l'instantané source afin que vous puissiez distinguer une copie de l'original.
5. Spécifiez la destination de la copie instantanée.

   - Pour copier le cliché dans la même région ou dans une autre région, sélectionnez AWS Région, puis sélectionnez la région de destination.
   - (Clients de l'avant-poste uniquement) Pour copier l'instantané dans un avant-poste, sélectionnez l'AWS avant-poste, puis entrez l'ARN de l'avant-poste de destination.
6. Si vous souhaitez que la copie instantanée soit terminée dans un délai spécifique, sélectionnez Activer la copie basée sur le temps. Pour Durée d'achèvement, entrez la durée d'achèvement requise, par tranches de 15 minutes. Pour plus d'informations, consultez Copies temporelles pour les instantanés Amazon EBS.

Si vous n'avez pas besoin que la copie instantanée soit terminée dans un délai spécifique, n'activez pas la copie basée sur le temps. Dans ce cas, la copie instantanée est réalisée dans la mesure du possible.

7. (Clients de l'avant-poste uniquement) Pour créer la copie instantanée d'un avant-poste dans la région sélectionnée, pour Destination de l'instantané, choisissez AWS Outpost, puis pour Destination Outpost ARN, entrez l'ARN de l'avant-poste vers lequel copier l'instantané. Le champ Destination du cliché apparaît uniquement si vous avez des Outposts dans la région sélectionnée.
8. Spécifiez l'état du chiffrement pour la copie d'instantané.

   Si l'instantané source est chiffré ou si le chiffrement est activé par défaut sur votre compte, la copie instantanée est automatiquement chiffrée. Si l'instantané source n'est pas chiffré et que le chiffrement par défaut n'est pas activé pour votre compte, le chiffrement est facultatif.
9. Choisissez Copy snapshot (Copier un instantané).

> **Note**
>
> Si vous essayez de copier un instantané chiffré sans disposer des autorisations d'utilisation de la clé de chiffrement, l'opération échoue silencieusement. L'état d'erreur ne s'affiche pas sur la console tant que vous n'avez pas actualisé la page.

AWS CLI

Pour copier un instantané à l'aide du AWS CLI

Utilisez la commande copy-snapshot.

Pour copier un instantané à l'aide des Outils pour Windows PowerShell

Utilisez la commande Copy-EC2Snapshot.

> **Note**
>
> Si vous tentez de copier un instantané chiffré sans être autorisé à utiliser la clé de chiffrement, l'opération échoue silencieusement et la copie instantanée reçoit le message d'état « L'ID de clé donné n'est pas accessible ».

Partager un instantané Amazon EBS avec d'autres comptes AWS

Vous pouvez modifier les autorisations d'un instantané si vous souhaitez partager celui-ci avec d'autres comptes AWS . Vous pouvez partager des instantanés publiquement avec tous les autres AWS comptes, ou vous pouvez les partager en privé avec des AWS comptes individuels que vous spécifiez. Les utilisateurs qui bénéficient de votre autorisation peuvent utiliser les instantanés que vous partagez pour créer leurs propres volumes EBS, tandis que votre instantané d'origine reste inchangé.

> **Important**
>
> Lorsque vous partagez un instantané, vous autorisez d'autres personnes à accéder à toutes les données de l'instantané. Partagez vos instantanés uniquement avec les personnes à qui vous faites confiance pour toutes vos données d'instantané.

Pour empêcher le partage public de clichés, vous pouvez activerBloquer l'accès public aux instantanés Amazon EBS.

Rubriques

Avant de partager un instantané

Les considérations suivantes s'appliquent au partage des instantanés :

- Si le blocage de l'accès public pour les instantanés est activé pour la région, les tentatives de partage public des instantanés seront bloquées. Les instantanés peuvent toujours être partagés en privé.
- Les instantanés sont limités à la région dans laquelle ils ont été créés. Pour partager un instantané avec une autre région, copiez l'instantané dans cette région, puis partagez la copie. Pour de plus amples informations, veuillez consulter Copier un instantané Amazon EBS.

- Vous ne pouvez pas partager d'instantanés chiffrés avec l' Clé gérée par AWS par défaut. Vous ne pouvez pas partager d'instantanés chiffrés avec une clé gérée par le client. Pour plus d'informations, consultez Création des clés dans le Guide du développeur AWS Key Management Service .
- Vous ne pouvez partager que des instantanés non chiffrés publiquement.
- Lorsque vous partagez un instantané chiffré, vous devez également partager la clé gérée par le client qui a servi à chiffrer l'instantané. Pour plus d'informations, consultez Partagez la clé KMS utilisée pour chiffrer un instantané Amazon EBS partagé.

Partager un instantané

Vous pouvez partager un instantané à l'aide de l'une des méthodes décrites dans la section.

Console

Pour partager un instantané

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané à partager, puis choisissez Actions, Modify permissions (Modifier des autorisations).
4. Spécifiez les autorisations de l'instantané. Current setting (Paramétrage actuel) indique les autorisations de partage actuelles de l'instantané.
   - Pour partager l'instantané publiquement avec tous les AWS comptes, choisissez Public.
   - Pour partager l'instantané en privé avec des AWS comptes spécifiques, choisissez Privé. Ensuite, dans la section Sharing accounts (Partage de comptes), choisissez Add account (Ajouter un compte), puis saisissez l'ID de compte à 12 chiffres (sans traits d'union) du compte avec lequel partager.
5. Sélectionnez Enregistrer les modifications.

AWS CLI

Les autorisations pour un instantané sont spécifiées à l'aide de l'attribut `createVolumePermission` de l'instantané. Pour qu'un instantané devienne public, définissez le groupe sur `all`. Pour partager un instantané avec un AWS compte spécifique, attribuez à l'utilisateur l'ID du AWS compte.

Pour partager un instantané en mode public

Utilisez la commande modify-snapshot-attribute.

Pour `--attribute`, spécifiez `createVolumePermission`. Pour `--operation-type`, spécifiez `add`. Pour `--group-names`, spécifiez `all`.

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --group-names all
```

Pour partager un instantané en mode privé

Utilisez la commande modify-snapshot-attribute.

Pour `--attribute`, spécifiez `createVolumePermission`. Pour `--operation-type`, spécifiez `add`. Pour`--user-ids`, spécifiez les 12 chiffres IDs des AWS comptes avec lesquels vous souhaitez partager les instantanés.

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --user-ids 123456789012
```

Tools for Windows PowerShell

Les autorisations pour un instantané sont spécifiées à l'aide de l'attribut `createVolumePermission` de l'instantané. Pour qu'un instantané devienne public, définissez le groupe sur `all`. Pour partager un instantané avec un AWS compte spécifique, attribuez à l'utilisateur l'ID du AWS compte.

Pour partager un instantané en mode public

Utilisez la commande Edit-EC2SnapshotAttribute.

Pour `-Attribute`, spécifiez `CreateVolumePermission`. Pour `-OperationType`, spécifiez `Add`. Pour `-GroupName`, spécifiez `all`.

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -GroupName all
```

Pour partager un instantané en mode privé

Utilisez la commande Edit-EC2SnapshotAttribute.

Pour `-Attribute`, spécifiez `CreateVolumePermission`. Pour `-OperationType`, spécifiez `Add`. Pour`UserId`, spécifiez les 12 chiffres IDs des AWS comptes avec lesquels vous souhaitez partager les instantanés.

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -UserId 123456789012
```

Partagez la clé KMS utilisée pour chiffrer un instantané Amazon EBS partagé

Lorsque vous partagez un instantané chiffré, vous devez également partager la clé gérée par le client qui a servi à chiffrer l'instantané. Vous pouvez appliquer des autorisations inter-comptes à une clé gérée par le client lors de sa création ou ultérieurement.

Les utilisateurs de votre clé gérée par le client partagée qui accèdent aux instantanés chiffrés doivent recevoir les autorisations permettant d'exécuter les actions suivantes sur la clé :

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:GenerateDataKeyWithoutPlaintext`
- `kms:ReEncrypt`
- `kms:Decrypt`

> **Tip**
>
> Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour autoriser l'utilisateur à créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée en son nom par un AWS service.

Pour en savoir plus sur le contrôle de l'accès à une clé gérée par le client, consultez Utilisation de stratégies de clé dans AWS KMS dans le Guide du développeur AWS Key Management Service .

Pour partager une clé gérée par le client à l'aide de la AWS KMS console

1. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Choisissez Customer managed keys (Clés gérées par le client) dans le volet de navigation.
4. Dans la colonne Alias choisissez l'alias (lien texte) de la clé gérée par le client que vous avez utilisée pour chiffrer l'instantané. Les détails de la clé s'ouvrent dans une nouvelle page.
5. Dans la section Key policy (Stratégie de clé) s'affiche soit la vue de la stratégie soit la vue par défaut. La vue de la politique affiche le document de la politique de clé. La vue par défaut affiche les sections Key administrators (Administrateurs de clé), Key deletion (Suppression de clé), Key Use (Utilisation de clé) et Other AWS accounts (Autres comptes). L'affichage par défaut s'affiche si vous avez créé la politique dans la console et que vous ne l'avez pas personnalisée. Si l'affichage par défaut n'est pas disponible, vous devez modifier manuellement la politique dans l'affichage de politique. Pour plus d'informations, consultez Affichage d'une stratégie de clé (console) dans le Guide du développeur AWS Key Management Service .

   Utilisez la vue des politiques ou la vue par défaut, selon la vue à laquelle vous pouvez accéder, pour ajouter un ou plusieurs AWS comptes IDs à la politique, comme suit :

   - (Vue de la stratégie) Choisissez Edit (Modifier). Ajoutez un ou plusieurs AWS comptes IDs aux relevés suivants : `"Allow use of the key"` et`"Allow attachment of persistent resources"`. Sélectionnez Enregistrer les modifications. Dans l'exemple suivant, l'ID de AWS compte `444455556666` est ajouté à la politique.

     ```
     {
       "Sid": "Allow use of the key",
       "Effect": "Allow",
       "Principal": {"AWS": [
         "arn:aws:iam::111122223333:user/KeyUser",
         "arn:aws:iam::444455556666:root"
       ]},
       "Action": [
         "kms:Encrypt",
         "kms:Decrypt",
         "kms:ReEncrypt*",
         "kms:GenerateDataKey*",
         "kms:DescribeKey"
       ],
       "Resource": "*"
     ```

```
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

- (Affichage par défaut) Faites défiler la page vers le bas jusqu'à Autres AWS comptes. Choisissez Ajouter d'autres AWS comptes et entrez l'identifiant du AWS compte comme demandé. Pour ajouter un autre compte, choisissez Ajouter un autre AWS compte et entrez l'identifiant du AWS compte. Une fois que vous avez ajouté tous les comptes AWS , choisissez Enregistrer les modifications.

Utilisez les instantanés Amazon EBS partagés avec vous

Pour utiliser un instantané partagé non chiffré

Localisez l'instantané partagé par son ID ou sa description. Vous pouvez utiliser cet instantané comme n'importe quel autre instantané que vous possédez dans votre compte. Par exemple, vous pouvez créer un volume à partir de l'instantané ou le copier dans une autre région.

Pour utiliser un instantané chiffré partagé

Localisez l'instantané partagé par son ID ou sa description. Créez une copie de l'instantané partagé dans votre compte et chiffrez la copie à l'aide d'une clé KMS que vous possédez. Vous pouvez ensuite utiliser la copie pour créer des volumes ou la copier dans différentes régions.

Vous pouvez afficher les instantanés que qui sont partagés avec vous à l'aide de l'une des méthodes suivantes.

Console

Pour afficher les instantanés partagés à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Filtrer les instantanés répertoriés. Dans le coin supérieur gauche de l'écran, choisissez l'une des options suivantes :
   - Instantanés privés — Pour afficher uniquement les instantanés partagés avec vous en mode privé.
   - Instantanés privés — Pour afficher uniquement les instantanés partagés avec vous en mode public.

AWS CLI

Pour afficher les autorisations d'instantané à l'aide de la ligne de commande

Utilisez la commande describe-snapshot-attribute.

Tools for Windows PowerShell

Pour afficher les autorisations d'instantané à l'aide de la ligne de commande

Utilisez la commande Get-EC2SnapshotAttribute.

Déterminer l'utilisation des instantanés que vous partagez

Vous pouvez l'utiliser AWS CloudTrail pour vérifier si un instantané que vous avez partagé avec d'autres est copié ou utilisé pour créer un volume. Les événements suivants sont enregistrés CloudTrail lorsqu'une action est entreprise sur un instantané que vous avez partagé :

- SharedSnapshotCopyInitiated— Un instantané partagé est en cours de copie.
- SharedSnapshotVolumeCreated— Un instantané partagé est utilisé pour créer un volume.

Pour plus d'informations sur l'utilisation CloudTrail, consultez la section Enregistrer les appels d'API Amazon EC2 et Amazon EBS avec AWS CloudTrail.

Archiver des instantanés Amazon EBS

Amazon EBS Snapshots Archive est un niveau de stockage que vous pouvez utiliser pour le stockage à long terme et à faible coût de vos instantanés rarement consultés qui ne nécessitent pas de récupération fréquente ou rapide.

Par défaut, lorsque vous créez un instantané, il est stocké dans le niveau Amazon EBS Snapshot Standard (niveau standard). Les instantanés stockés dans le niveau standard sont incrémentiels. Cela signifie que seuls les blocs du volume qui ont été modifiés après votre dernier instantané sont sauvegardés.

Lorsque vous archivez un instantané, l'instantané incrémentiel est converti en instantané complet et il est déplacé du niveau standard vers le niveau Amazon EBS Snapshots Archive (niveau d'archivage). Les instantanés complets incluent tous les blocs écrits sur le volume au moment de la création de l'instantané.

Lorsque vous devez accéder à un instantané archivé, vous pouvez le restaurer depuis le niveau d'archivage vers le niveau standard, puis l'utiliser de la même manière que n'importe quel autre instantané de votre compte.

Amazon EBS Snapshots Archive offre des coûts de stockage d'instantanés jusqu'à 75 % inférieurs pour les instantanés que vous prévoyez de stocker pendant 90 jours ou plus et auxquels vous n'avez que rarement besoin d'accéder.

Les cas d'utilisation typiques incluent :

- Archivage du seul instantané d'un volume, tel que end-of-project les instantanés
- Archiver des instantanés complets et point-in-time incrémentiels pour des raisons de conformité.
- l'archivage des instantanés incrémentiels mensuels, trimestriels ou annuels.

Rubriques

- Archiver un instantané Amazon EBS
- Restaurer un instantané Amazon EBS archivé
- Modifier la période de restauration d'un instantané Amazon EBS temporairement restauré
- Afficher les instantanés Amazon EBS archivés
- Surveillez l'archivage des instantanés Amazon EBS à l'aide d'Events CloudWatch

Quotas

Cette section décrit les quotas par défaut pour les instantanés archivés et en cours de réalisation.

Quota	Quota par défaut			
Instantanés archivés par volume	25			
Archives simultanées d'instantanés en cours par compte	25			
Restaurations simultanées d'instantanés en cours par compte	5			

Si vous avez besoin de plus que les limites par défaut, remplissez le formulaire Support Center Create Case pour demander une augmentation de limite.

Considérations et limites relatives à l'archivage des instantanés Amazon EBS

Tenez compte des points suivants lorsque vous archivez des instantanés Amazon EBS.

Considérations

- La période d'archivage minimale est de 90 jours. Si vous supprimez ou restaurez définitivement un instantané archivé avant la période d'archivage minimale de 90 jours, vous êtes facturé pour les jours restants dans le niveau d'archivage, arrondi à l'heure la plus proche. Pour plus d'informations, consultez Tarification et facturation pour l'archivage des instantanés Amazon EBS.
- La restauration d'un instantané archivé du niveau d'archivage au niveau standard peut prendre jusqu'à 72 heures, en fonction de la taille de l'instantané.
- Les instantanés archivés sont toujours des instantanés complets. Les instantanés complets incluent tous les blocs écrits sur le volume au moment de la création de l'instantané. L'instantané complet sera probablement plus grand que l'instantané incrémentiel à partir duquel il a été créé. Toutefois, si vous n'avez qu'un instantané incrémentiel d'un volume sur le niveau standard, la taille de l'instantané complet dans le niveau d'archivage sera de la même taille que celle du niveau standard. En effet, le premier instantané pris d'un volume est toujours un instantané complet.
- L'archivage est recommandé pour les instantanés mensuels, trimestriels ou annuels. L'archivage quotidien d'instantanés incrémentiels d'un seul volume peut entraîner des coûts plus élevés par rapport à leur conservation dans le niveau standard.
- Lorsqu'un instantané est archivé, ses données référencées par d'autres instantanés dans sa lignée sont retenues dans le niveau standard. Les coûts de données et de stockage associés aux données référencées retenues sur le niveau standard sont alloués au prochain instantané de la lignée. Cela garantit que les instantanés suivants dans la lignée ne sont pas affectés par l'archivage.
- Si vous supprimez un instantané archivé qui correspond à une règle de rétention de la corbeille, l'instantané archivé est retenu dans la corbeille pendant la période définie dans la règle de rétention. Pour utiliser cet instantané, vous devez d'abord le récupérer depuis la corbeille, puis le restaurer à partir du niveau d'archivage. Pour plus d'informations, voir Corbeille etTarification et facturation pour l'archivage des instantanés Amazon EBS.
- Vous ne pouvez pas utiliser un instantané archivé dans un mappage de périphérique de stockage en mode bloc ou pour créer un volume Amazon EBS.

- Vous pouvez archiver les instantanés créés AWS Backup à l'aide des outils Console AWS Backup APIs, ou en ligne de commande. Pour de plus amples informations, consultez Création d'un plan de sauvegarde dans le Guide du développeur AWS Backup .

Limites

- Vous ne pouvez archiver que les instantanés dont l'état est `completed`.
- Vous ne pouvez archiver que les instantanés dont vous êtes propriétaire dans votre compte. Pour archiver un instantané qui vous est partagé, copiez d'abord l'instantané sur votre compte, puis archivez la copie de l'instantané.
- Avant de pouvoir utiliser un instantané archivé, vous devez d'abord le restaurer au niveau standard. La restauration vers le niveau standard est nécessaire pour créer un volume à partir de l'instantané via les opérations d'API `CreateVolume` et `RunInstances`, ainsi que pour partager ou copier un instantané. Pour de plus amples informations, veuillez consulter Restaurer un instantané Amazon EBS archivé.
- Vous pouvez archiver un instantané associé à un ou plusieurs d'entre eux AMIs uniquement si tous les éléments associés AMIs sont désactivés. Pour plus d'informations, consultez la section Désactiver une AMI.
- Vous ne pouvez pas activer une AMI désactivée si les instantanés associés sont temporairement restaurés. Tous les instantanés associés doivent être définitivement restaurés avant que vous puissiez activer l'AMI.
- Vous ne pouvez pas annuler le processus d'archivage des instantanés ou de restauration des instantanés une fois qu'il a été démarré.
- Vous ne pouvez pas partager les instantanés archivés. Si vous archivez un instantané que vous avez partagé avec d'autres comptes, les comptes avec lesquels l'instantané est partagé perdent l'accès une fois l'instantané archivé.
- Vous ne pouvez pas copier les instantanés archivés. Si vous devez copier un instantané archivé, vous devez d'abord le restaurer.
- Vous ne pouvez pas activer la restauration rapide d'instantané pour un instantané archivé. La restauration rapide d'instantané est automatiquement désactivée lorsqu'un instantané est archivé. Si vous devez utiliser la restauration d'instantané rapide, vous devez l'activer manuellement après la restauration de l'instantané.

Tarification et facturation pour l'archivage des instantanés Amazon EBS

Les instantanés archivés sont facturés au tarif de 0,0125 USD par Go par mois. Par exemple, si vous archivez un instantané de 100 Gio, vous êtes facturé 1,25 USD (100 Gio * 0,0125 USD/Gio) par mois.

Les restaurations d'instantanés sont facturées au tarif de 0,03 USD par Go de données restaurées. Par exemple, si vous restaurez un instantané de 100 Gio à partir du niveau d'archivage, vous êtes facturé une fois 3 USD (100 Gio * 0,03 USD/Gio).

Une fois l'instantané restauré au niveau standard, l'instantané est facturé au tarif standard pour les instantanés de 0,05 USD par Go par mois.

Pour plus d'informations, consultez la section Tarification d'Amazon EBS.

Facturation pour la période d'archivage minimale

La période d'archivage minimale est de 90 jours. Si vous supprimez ou restaurez définitivement un instantané archivé avant la période d'archivage minimale de 90 jours, vous êtes facturé au prorata des frais de stockage du niveau d'archivage pour les jours restants, arrondis à l'heure la plus proche. Par exemple, si vous supprimez ou restaurez définitivement un instantané archivé après 40 jours, vous êtes facturé pour les 50 jours restants de la période d'archivage minimale.

> **Note**
>
> La restauration temporaire d'un instantané archivé avant la période d'archivage minimale de 90 jours n'entraîne pas ces frais.

Restauration temporaire

Lorsque vous restaurez temporairement un instantané, l'instantané est restauré du niveau d'archivage vers le niveau standard, et une copie de l'instantané reste dans le niveau d'archivage. Vous êtes facturé à la fois pour l'instantané dans le niveau standard et pour la copie d'instantané dans le niveau d'archivage pendant la durée de la période de restauration temporaire. Lorsque l'instantané temporairement restauré est retiré du niveau standard, vous n'êtes plus facturé pour celui-ci (niveau standard), et vous êtes facturé pour l'instantané dans le niveau d'archivage uniquement.

Restauration définitive

Lorsque vous restaurez définitivement un instantané, l'instantané est restauré du niveau d'archivage vers le niveau standard, et l'instantané est supprimé du niveau d'archivage. Vous êtes facturé pour l'instantané uniquement dans le niveau standard.

Suppression d'instantanés

Si vous supprimez un instantané pendant qu'il est archivé, vous êtes facturé pour les données de l'instantané qui ont déjà été déplacées vers le niveau d'archivage. Ces données sont soumises à la période d'archivage minimale de 90 jours et facturées en conséquence lors de leur suppression. Par exemple, si vous archivez un instantané de 100 Gio et que vous supprimez l'instantané après que seulement 40 Gio ont été archivés, vous êtes facturé 1,50 USD pour la période d'archivage minimale de 90 jours pour les 40 Gio qui ont déjà été archivés (0,0125 USD par Go par mois * 40 Go * (90 jours * 24 heures) / (24 heures/jour * 30 jours)).

Si vous supprimez un instantané alors qu'il est restauré à partir du niveau d'archivage, la restauration de l'instantané vous sera facturée pour sa taille réelle (taille de l'instantané * 0,03 USD). Par exemple, si vous restaurez un instantané de 100 Gio à partir du niveau d'archivage et que vous supprimez l'instantané à n'importe quel moment avant la fin de sa restauration, vous êtes facturé 3 USD (taille d'instantané de 100 Gio * 0,03 USD).

Corbeille

Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille. Les instantanés archivés qui se trouvent dans la corbeille sont soumis à la période d'archivage minimale de 90 jours et sont facturés en conséquence s'ils sont supprimés par la corbeille avant la période d'archivage minimale. En d'autres termes, si une règle de rétention supprime un instantané archivé de la corbeille avant la période minimale de 90 jours, vous êtes facturé pour les jours restants.

Si vous supprimez un instantané correspondant à une règle de rétention pendant l'archivage de l'instantané, l'instantané archivé est retenu dans la corbeille pendant la période de rétention définie dans la règle de rétention. Il est facturé au tarif des instantanés archivés.

Si vous supprimez un instantané correspondant à une règle de rétention pendant la restauration de l'instantané, l'instantané restauré est retenu dans la corbeille pendant le reste de la période de rétention, et facturé au taux d'instantané standard. Pour utiliser l'instantané restauré, vous devez d'abord le récupérer depuis la corbeille.

Pour plus d'informations, voir Corbeille.

Suivi des coûts

Les instantanés archivés apparaissent dans le fichier AWS Cost and Usage Report avec le même ID de ressource et le même Amazon Resource Name (ARN). Pour plus d'informations, consultez le Guide de l'utilisateur AWS Cost and Usage Report.

Vous pouvez utiliser les types d'utilisation suivants pour identifier les coûts associés :

- `SnapshotArchiveStorage` : frais pour le stockage de données mensuel
- `SnapshotArchiveRetrieval` : frais ponctuels pour les restaurations d'instantanés
- `SnapshotArchiveEarlyDelete` : frais de suppression ou de restauration permanente d'un instantané avant la période d'archivage minimale (90 jours)

Directives et bonnes pratiques pour l'archivage des instantanés Amazon EBS

Cette section fournit des consignes et de bonnes pratiques pour l'archivage des instantanés.

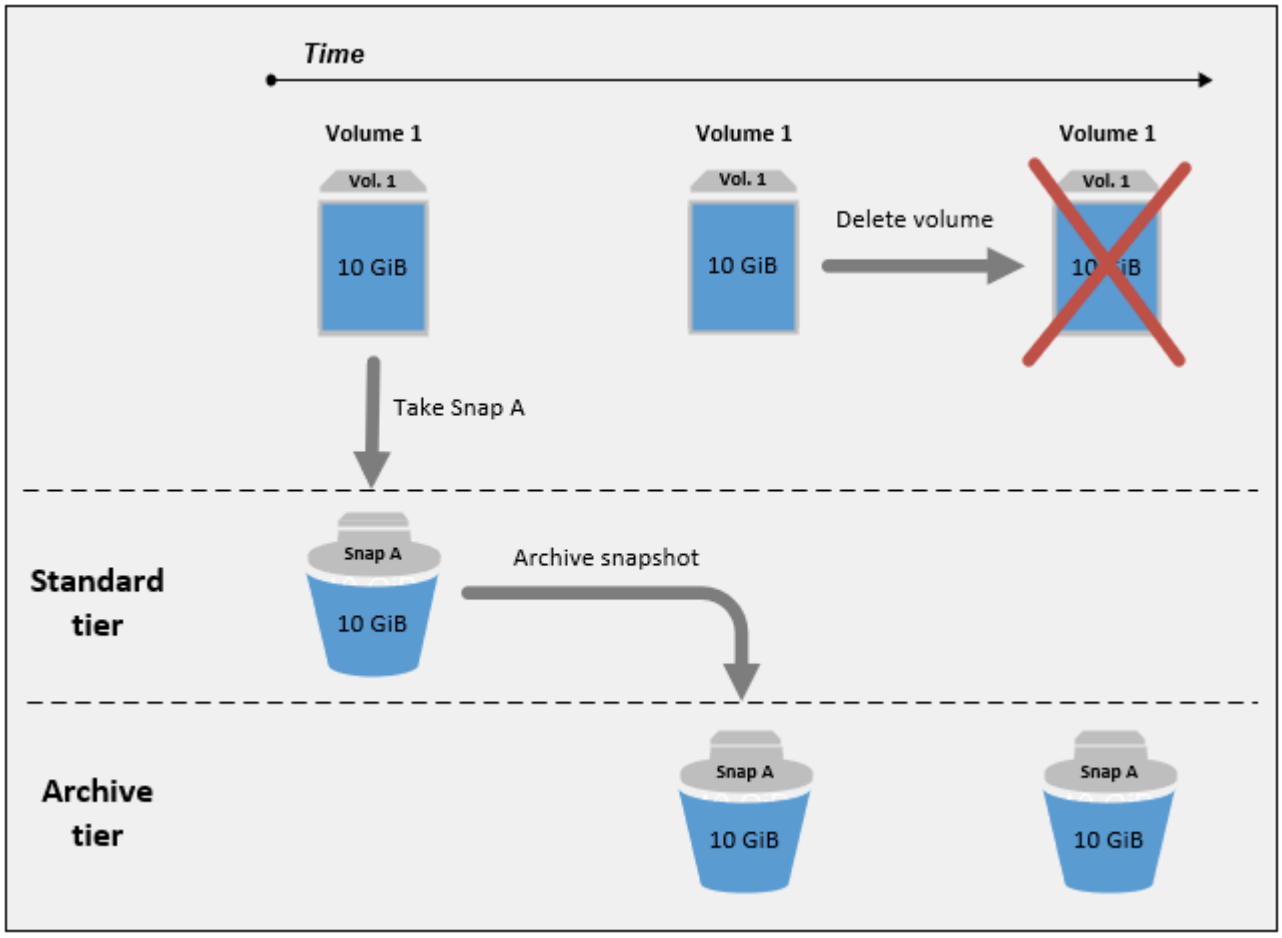
Rubriques

- Archivage du seul instantané d'un volume
- Archivage des instantanés incrémentiels d'un seul volume
- Archivage des instantanés complets pour des raisons de conformité
- Évaluation de la réduction des coûts de stockage de niveau standard

Archivage du seul instantané d'un volume

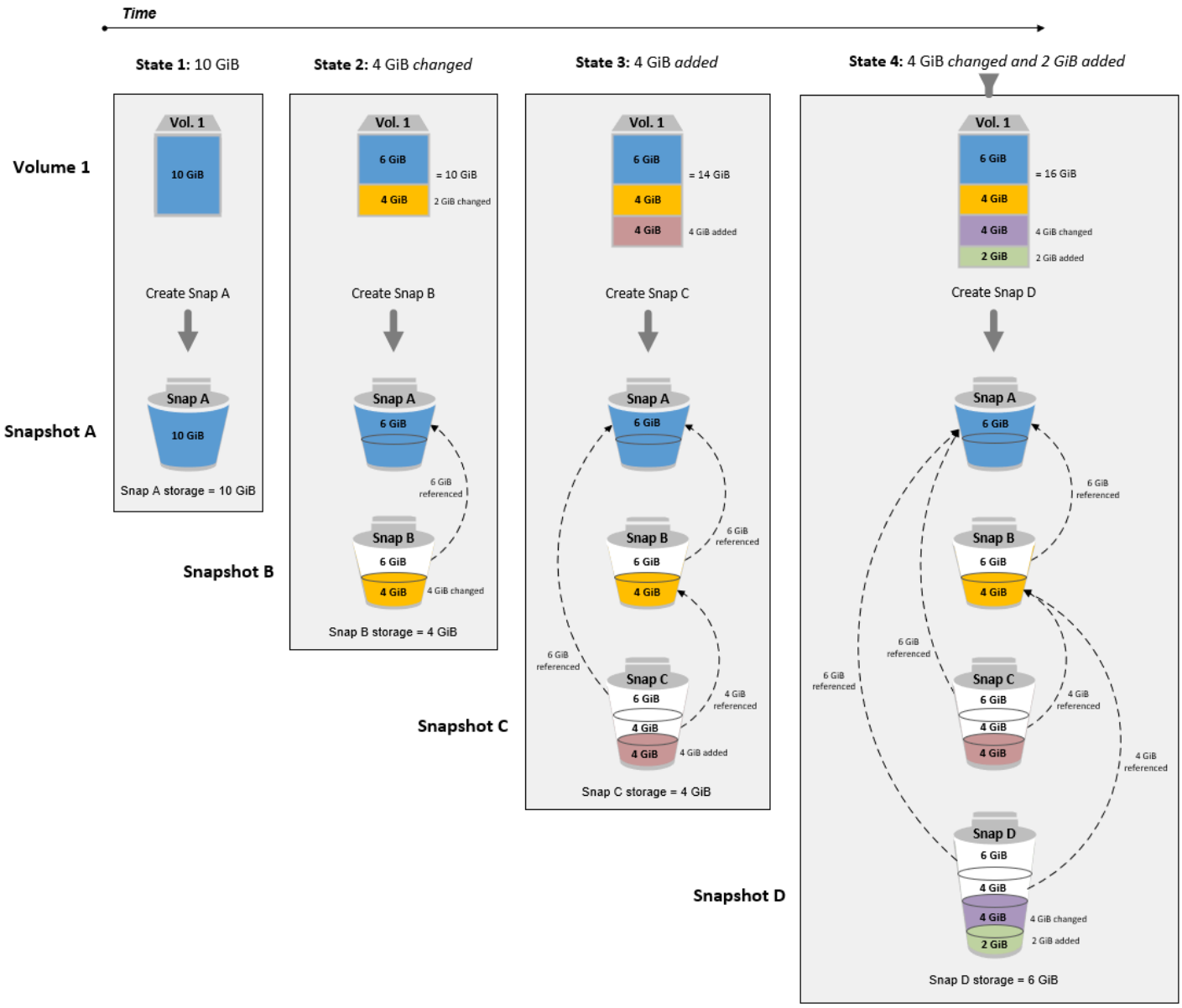
Lorsque vous n'avez qu'un seul instantané d'un volume, l'instantané a toujours la même taille que les blocs écrits sur le volume au moment de la création de l'instantané. Lorsque vous archivez un tel instantané, l'instantané du niveau standard est converti en instantané complet de taille équivalente et il est déplacé du niveau standard vers le niveau d'archivage.

L'archivage de ces instantanés peut vous aider à économiser avec des coûts de stockage réduits. Si vous n'avez plus besoin du volume source, vous pouvez le supprimer pour réduire davantage les coûts de stockage.



Archivage des instantanés incrémentiels d'un seul volume

Lorsque vous archivez un instantané incrémentiel, l'instantané est converti en instantané complet et il est déplacé vers le niveau d'archivage. Par exemple, dans l'image suivante, si vous archivez Snap B, l'instantané est converti en un instantané complet d'une taille de 10 Gio et déplacé vers le niveau d'archivage. De même, si vous archivez Snap C, la taille de l'instantané complet dans le niveau d'archivage est de 14 Gio.



Si vous archivez des instantanés pour réduire vos coûts de stockage dans le niveau standard, n'archivez pas le premier instantané d'un ensemble d'instantanés incrémentiels. Ces instantanés sont référencés par les instantanés suivants dans la lignée des instantanés. Dans la plupart des cas, l'archivage de ces instantanés ne réduira pas les coûts de stockage.

> **Note**
>
> N'archivez pas le dernier instantané d'un ensemble d'instantanés incrémentiels. Le dernier instantané est l'instantané le plus récent d'un volume. Vous aurez besoin de cet instantané

dans le niveau standard si vous souhaitez créer des volumes à partir de celui-ci en cas de corruption ou de perte de volume.

Si vous archivez un instantané qui contient des données référencées par un instantané ultérieur de la lignée, le stockage des données et les coûts de stockage associés aux données référencées sont attribués à l'instantané ultérieur de la lignée. Dans ce cas, l'archivage de l'instantané ne réduira pas le stockage de données ni les coûts de stockage. Par exemple, dans l'image précédente, si vous archivez Snap B, ses 4 Gio de données sont attribués à Snap C. Dans ce cas, vos coûts de stockage globaux augmenteront, car vous engagez des coûts de stockage pour la version complète de Snap B dans le niveau d'archivage, et vos coûts de stockage pour le niveau standard restent inchangés.

Si vous archivez Snap C, votre stockage de niveau standard diminuera de 4 Gio, car les données ne sont référencées par aucun autre instantané ultérieur dans la lignée. De plus, votre stockage de niveau d'archivage augmentera de 14 Gio, car l'instantané est converti en instantané complet.

Archivage des instantanés complets pour des raisons de conformité

Vous devrez peut-être créer des sauvegardes complètes de volumes sur une base mensuelle, trimestrielle ou annuelle pour des raisons de conformité. Pour ces sauvegardes, vous pouvez avoir besoin d'instantanés autonomes sans références en amont ou en aval à d'autres instantanés dans la lignée des instantanés. Les instantanés archivés avec EBS Snapshots Archive sont des instantanés complets, et ils ne contiennent aucune référence à d'autres instantanés de la lignée. En outre, vous devrez probablement retenir ces instantanés pour des raisons de conformité pendant plusieurs années. EBS Snapshots Archive permet d'archiver de manière rentable ces instantanés complets pour une rétention à long terme.

Évaluation de la réduction des coûts de stockage de niveau standard

Si vous souhaitez archiver un instantané incrémentiel pour réduire vos coûts de stockage, vous devez prendre en compte la taille de l'instantané complet dans le niveau d'archivage et la réduction du stockage dans le niveau standard. Cette section explique comment procéder.

Important

Les réponses de l'API sont des données précises au point-in-time moment où APIs elles sont appelées. Les réponses de l'API peuvent différer lorsque les données associées à un instantané changent suite à des modifications de la lignée de ce dernier.

Pour déterminer la réduction du stockage et des coûts de stockage dans le niveau standard, procédez comme suit.

1. Vérifiez la taille de l'instantané complet. Pour déterminer la taille totale de l'instantané, utilisez la list-snapshot-blockscommande. Pour `--snapshot-id`, spécifiez l'ID de l'instantané que vous souhaitez archiver.

```
$  aws ebs list-snapshot-blocks --snapshot-id snapshot_id
```

Ceci renvoie des informations sur l'ensemble des blocs contenus dans l'instantané spécifié. Le `BlockIndex` du dernier bloc renvoyé par la commande indique le nombre de blocs dans l'instantané. Le nombre de blocs multiplié par 512 Kio, qui correspond à la taille du bloc d'instantané, vous donne une approximation proche de la taille de l'instantané complet dans le niveau d'archivage (blocs * 512 Kio = taille de l'instantané complet).

Par exemple, la commande suivante répertorie les blocs pour l'instantané `snap-01234567890abcdef`.

```
$  aws ebs list-snapshot-blocks --snapshot-id snap-01234567890abcdef
```

Voici la sortie de la commande, certains blocs étant omis. La sortie suivante indique que l'instantané comprend environ 16 383 blocs de données. Cela correspond à une taille d'instantané complète d'environ 8 Gio (16 383 * 512 Kio = 7,99 Gio).

```
 {
    "VolumeSize": 8,
    "Blocks": [
        {
            "BlockToken": "ABgBAeShfa5RwG+RiWUg2pwmnCU/
YMnV7fGMxLbCWfEBEUmmuqac5RmoyVat",
            "BlockIndex": 0
        },
        {
            "BlockToken": "ABgBATdTONyThPUAbQhbUQXsn5TGoY/
J17GfE83j9WN7siupavOTw9E1KpFh",
            "BlockIndex": 1
        },
        {
            "BlockToken": "EBEUmmuqXsn5TGoY/QwmnCU/YMnV74eKE2TSsn5TGoY/
E83j9WQhbUQXsn5T",
```

```
            "BlockIndex": 4
        },
        .....
        {
            "BlockToken": "yThPUAbQhb5V8xpwmnCU/
YMnV74eKE2TSFY1sKP/4r05y47WETdTONyThPUA",
            "BlockIndex": 12890
        },
        {
            "BlockToken":
 "ABgBASHKD5V8xEbaRKdxdkZZS4eKE2TSFYlMG1sKP/4r05y47WEHqKaNPcLs",
            "BlockIndex": 12906
        },
        {
            "BlockToken": "ABgBARROGMUJo6P9X3CFHQGZNQ7av9B6vZtTTqV89QqC
+SkO0HWMlwkGXjnA",
            "BlockIndex": 16383
        }
    ],
    "VolumeSize": 8,
    "ExpiryTime": 1637677800.845,
    "BlockSize": 524288
}
```

2. Cherchez le volume source à partir duquel l'instantané que vous voulez archiver a été créé. Utilisez la commande describe-snapshots. Pour `--snapshot-id`, spécifiez l'ID de l'instantané que vous souhaitez archiver. Le paramètre de réponse `VolumeId` indique l'ID du volume source.

```
$ aws ec2 describe-snapshots --snapshot-id snapshot_id
```

Par exemple, la commande suivante renvoie des informations sur l'instantané `snap-09c9114207084f0d9`.

```
$ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
```

Voici la sortie de la commande, qui indique que l'instantané `snap-09c9114207084f0d9` a été créé à partir du volume `vol-0f3e2c292c52b85c3`.

```
{
    "Snapshots": [
        {
```

```
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        }
    ]
}
```

3. Cherchez tous les instantanés créés à partir du volume source. Utilisez la commande describe-snapshots. Spécifiez le filtre `volume-id`, et pour la valeur du filtre, spécifiez l'ID du volume de l'étape précédente.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

Par exemple, la commande suivante renvoie tous les instantanés créés à partir du volume `vol-0f3e2c292c52b85c3`.

```
$ aws ec2 describe-snapshots --filters "Name=volume-id,
 Values=vol-0f3e2c292c52b85c3"
```

Voici la sortie de la commande, qui indique que trois instantanés ont été créés à partir du volume `vol-0f3e2c292c52b85c3`.

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-14T08:57:39.300Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
```

```
            "SnapshotId": "snap-08ca60083f86816b0"
        },
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-15T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        },
        {
            "Description": "01",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T07:50:08.042Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-024f49fe8dd853fa8"
        }
    ]
}
```

4. En utilisant la sortie de la commande précédente, triez les instantanés par leur date de création, du plus ancien au plus récent. Le paramètre de réponse `StartTime` pour chaque instantané indique sa date de création, au format UTC.

   Par exemple, les instantanés renvoyés à l'étape précédente, organisés par date de création, du plus ancien au plus récent, sont les suivants :

   1. `snap-08ca60083f86816b0` (le plus ancien, créé avant l'instantané que vous souhaitez archiver)
   2. `snap-09c9114207084f0d9` (l'instantané à archiver)
   3. `snap-024f49fe8dd853fa8` (le plus récent, créé après l'instantané que vous souhaitez archiver)

5. Identifiez les instantanés créés immédiatement avant et après l'instantané que vous souhaitez archiver. Dans ce cas, vous souhaitez archiver l'instantané `snap-09c9114207084f0d9`, qui était le deuxième instantané incrémentiel créé dans l'ensemble de trois instantanés. L'instantané `snap-08ca60083f86816b0` a été créé immédiatement avant, et l'instantané `snap-024f49fe8dd853fa8` a été créé immédiatement après.
6. Cherchez les données non référencées dans l'instantané que vous voulez archiver. Tout d'abord, recherchez les blocs qui diffèrent entre l'instantané créé immédiatement avant l'instantané que vous souhaitez archiver et l'instantané que vous souhaitez archiver. Utilisez la commande list-changed-blocks. Pour `--first-snapshot-id`, spécifiez l'ID de l'instantané créé immédiatement avant celui que vous souhaitez archiver. Pour `--second-snapshot-id`, spécifiez l'ID de l'instantané que vous souhaitez archiver.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-
snapshot-id snapshot_to_archive
```

Par exemple, la commande suivante affiche les index de blocs pour les blocs qui sont différents entre l'instantané `snap-08ca60083f86816b0` (créé avant celui que vous souhaitez archiver) et l'instantané `snap-09c9114207084f0d9` (celui que vous souhaitez archiver).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-
snapshot-id snap-09c9114207084f0d9
```

Voici la sortie de la commande, certains blocs étant omis.

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1rOVeFbWXsH3W4z/",
            "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAcfL
+EfmQmlNgstqrFnYgsAxR4SDSO4LkNLYOOChGBWcfJnpn90E9XX1",
            "SecondBlockToken": "ABgBAdX0mtX6aBAt3EBy
+8jFCESMpig7csKjbO2Ocd08m2iNJV2Ue+cRwUqF",
```

```
            "BlockIndex": 5
        },
        {
            "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUi3MKZmEMxs2wC3AmM/
fc6yCOAMb65",
            "SecondBlockToken":
 "ABgBAdewWkHKTcrhZmsfM7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVnOqPxmx9r7Wf6O+i
+ltZ0dwPpGN39ijztLn",
            "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRclnV
+bKjViu/9UESTcW7CD9w4J2td",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken":
 "ABgBAZBfEv4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICGlFmZCyJXzE4r3",
            "SecondBlockToken":
 "ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVCldnpc91zBiNmSfW9ouIlbeXWy",
            "BlockIndex": 15
        },
        .....
        {
            "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5VO5Q3rEEA
+ku50P498hjnTAgMhLG",
            "BlockIndex": 13171
        },
        {
            "SecondBlockToken":
 "ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
            "BlockIndex": 13172
        },
        {
            "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWiOujOAKcauOnUFCO
+eZ5ASVdWLXWWC04ijfoDTpTVZ",
            "BlockIndex": 13173
        },
        {
            "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6tOvMoLBLJ14LKvavw4IiB1d0iykWe6b",
            "BlockIndex": 13174
        },
```

```
        {
            "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
            "BlockIndex": 13175
        }
    ],
    "ExpiryTime": 1637648751.813,
    "VolumeSize": 8
}
```

Ensuite, utilisez la même commande pour rechercher des blocs différents entre l'instantané que vous souhaitez archiver et l'instantané créé immédiatement après. Pour `--first-snapshot-id`, spécifiez l'ID de l'instantané que vous souhaitez archiver. Pour `--second-snapshot-id`, indiquez l'ID de l'instantané créé immédiatement après l'instantané que vous souhaitez archiver.

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-
snapshot-id snapshot_created_after
```

Par exemple, la commande suivante affiche les index de blocs des blocs qui sont différents entre l'instantané `snap-09c9114207084f0d9` (celui que vous souhaitez archiver) et l'instantané `snap-024f49fe8dd853fa8` (créé après celui que vous souhaitez archiver).

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-
snapshot-id snap-024f49fe8dd853fa8
```

Voici la sortie de la commande, certains blocs étant omis.

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
            "SecondBlockToken":
 "ABgBASEvi9x8Om7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAeL0mtX6aBAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
```

```
            "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLkO",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken":
 "ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
            "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrxOqGy4PKZ9SAAHaZ2HQBM9fQQU0+EXxQjVGv37",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken":
 "ABgBAbRlitCVI7c6hGsT4ckkKCw6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
            "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyvOwpozYII6UNCT",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken": "ABgBAd+yxCO26I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
            "SecondBlockToken": "ABgBAcPpnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
            "BlockIndex": 18
        },
        .....
        {
            "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV03lU/lKCW
+CTxFl3cQ5p2f2h1njpuUiGbqKGUa",
            "BlockIndex": 13190
        },
        {
            "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ
+iSlWVpBIshmeyeS5FD/M0i64U+a9",
            "BlockIndex": 13191
        },
        {
            "SecondBlockToken": "ABgBAZ8DhMk+rROXa4dZlNK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
            "BlockIndex": 13192
        },
        {
            "SecondBlockToken":
 "ABgBATh6MBVE904l6sqOC27s1nVntFUpDwiMcRWGyJHy8sIgGL5yuYXHAVty",
```

```
            "BlockIndex": 13193
        },
        {
            "SecondBlockToken":
 "ABgBARuZykaFBWpCWrJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn61OQyy+giN",
            "BlockIndex": 13194
        }
    ],
    "ExpiryTime": 1637692677.286,
    "VolumeSize": 8
}
```

7. Comparez la sortie renvoyée par les deux commandes lors de l'étape précédente. Si le même index de bloc apparaît dans les deux sorties de commande, cela indique que le bloc contient des données non référencées.

   Par exemple, la sortie de commande de l'étape précédente indique que les blocs 4, 5, 13 et 14 sont uniques à l'instantané `snap-09c9114207084f0d9` et qu'ils ne sont référencés par aucun autre instantané dans la lignée des instantanés.

   Pour déterminer la réduction du stockage de niveau standard, multipliez le nombre de blocs apparaissant dans les deux sorties de commande par 512 Kio, soit la taille du bloc d'instantané.

   Par exemple, si 9 950 index de blocs apparaissent dans les deux sorties de commandes, cela indique que vous allez diminuer le stockage standard d'environ 4,85 GiB (9 950 blocs * 512 KiB = 4,85 GiB).

8. Déterminez les coûts de stockage liés au stockage des blocs non référencés dans le niveau standard pendant 90 jours. Comparez cette valeur avec le coût de stockage de l'instantané complet, décrit à l'étape 1, dans le niveau d'archivage. Vous pouvez déterminer vos économies de coûts en comparant les valeurs, en supposant que vous ne restaurez pas l'instantané complet à partir du niveau d'archivage pendant la période minimale de 90 jours. Pour de plus amples informations, veuillez consulter Tarification et facturation pour l'archivage des instantanés Amazon EBS.

Autorisations IAM requises pour l'archivage des instantanés Amazon EBS

Par défaut, les utilisateurs ne sont pas autorisés à utiliser l'archivage des instantanés. Pour permettre aux utilisateurs d'utiliser l'archivage des instantanés, vous devez créer des politiques

IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Pour plus d'informations, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Pour utiliser l'archivage des instantanés, les utilisateurs ont besoin des autorisations suivantes.

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`
- `ec2:RestoreSnapshotTier`

Les utilisateurs de la console peuvent avoir besoin d'autorisations supplémentaires telles que `ec2:DescribeSnapshots`.

Pour archiver et restaurer des instantanés chiffrés, les AWS KMS autorisations supplémentaires suivantes sont requises.

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`

Voici un exemple de politique IAM qui autorise les utilisateurs IAM à archiver, restaurer et afficher des instantanés chiffrés et non chiffrés. Elle inclut l'autorisation `ec2:DescribeSnapshots` pour les utilisateurs de la console. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

> **Tip**
>
> Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour autoriser l'utilisateur à créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée en son nom par un AWS service, comme indiqué dans l'exemple suivant.

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

```
            "ec2:DescribeSnapshotTierStatus",
            "ec2:ModifySnapshotTier",
            "ec2:RestoreSnapshotTier",
            "ec2:DescribeSnapshots",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
    }]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Archiver un instantané Amazon EBS

Vous pouvez archiver n'importe quel instantané qui se trouve dans l'état `completed` et dont vous êtes propriétaire dans votre compte. Vous ne pouvez pas archiver les instantanés qui se trouvent dans l'état `pending` ou `error`, ou ceux qui sont partagés avec vous. Pour de plus amples

informations, veuillez consulter Considérations et limites relatives à l'archivage des instantanés Amazon EBS.

Si le cliché est associé à un ou plusieurs d'entre eux AMIs, vous devez d'abord désactiver ceux qui y sont associés AMIs avant de pouvoir archiver le cliché. Pour plus d'informations, consultez la section Désactiver une AMI.

Les instantanés archivés conservent leur ID d'instantané, leur état de chiffrement, leurs autorisations AWS Identity and Access Management (IAM), les informations sur le propriétaire et les balises de ressources. Toutefois, la restauration rapide d'instantané et le partage d'instantané sont automatiquement désactivés une fois celui-ci archivé.

Vous pouvez continuer à utiliser l'instantané pendant que l'archivage est en cours de traitement. Dès que l'état de hiérarchisation de l'instantané passe à `archival-complete`, vous ne pouvez plus l'utiliser.

Vous pouvez archiver un instantané en utilisant l'une des méthodes suivantes.

Console

Pour archiver un instantané

Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

1. Dans le panneau de navigation, choisissez Snapshots.
2. Dans la liste des instantanés, sélectionnez l'instantané à archiver, puis choisissez Actions, Archive snapshot (Archiver l'instantané).
3. Pour confirmer, choisissez Archive snapshot (Archiver l'instantané).

AWS CLI

Pour archiver un instantané

Utilisez la commande . modify-snapshot-tier AWS CLI Pour `--snapshot-id`, spécifiez l'ID de l'instantané à archiver. Pour `--storage-tier`, spécifiez `archive`.

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snapshot_id \
--storage-tier archive
```

Par exemple, la commande suivante archive l'instantané `snap-01234567890abcedf`.

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--storage-tier archive
```

Voici la sortie de cette commande. Le paramètre de réponse `TieringStartTime` indique la date et l'heure à laquelle le processus d'archivage a été lancé, au format UTC (AAAA-MM-JJTHH:MM:SSZ).

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

Restaurer un instantané Amazon EBS archivé

Avant de pouvoir utiliser un instantané archivé, vous devez d'abord le restaurer au niveau standard. L'instantané restauré possède les mêmes ID d'instantané, état de chiffrement, autorisations IAM, informations sur le propriétaire et identifications de ressources qu'avant son archivage. Une fois restauré, vous pouvez l'utiliser de la même manière que n'importe quel autre instantané de votre compte. L'instantané restauré est toujours un instantané complet.

Lorsque vous restaurez un instantané, vous pouvez choisir de le restaurer de façon permanente ou temporaire.

Si vous restaurez un instantané de façon permanente, il est déplacé définitivement du niveau d'archivage vers le niveau standard. L'instantané demeure restauré et prêt à être utilisé jusqu'à ce que vous le réarchiviez manuellement ou que vous le supprimiez manuellement. Lorsque vous restaurez définitivement un instantané, il est supprimé du niveau d'archivage.

Si vous restaurez temporairement un instantané, il est copié du niveau d'archivage vers le niveau standard pendant une période de restauration que vous spécifiez. L'instantané demeure restauré et prêt à être utilisé pendant la période de restauration uniquement. Pendant la période de restauration, une copie de l'instantané reste dans le niveau d'archivage. Une fois la période expirée, l'instantané est automatiquement supprimé du niveau standard. Vous pouvez augmenter ou diminuer la période de restauration ou changer le type de restauration pour le rendre permanent à tout moment pendant la période de restauration. Pour de plus amples informations, veuillez consulter Modifier la période de restauration d'un instantané Amazon EBS temporairement restauré.

Si vous restaurez des instantanés associés à une AMI désactivée et que vous avez l'intention d'utiliser cette AMI, vous devez d'abord restaurer définitivement tous les instantanés associés, puis réactiver une AMI désactivée avant de pouvoir l'utiliser. Vous ne pouvez pas activer une AMI si les instantanés associés sont temporairement restaurés. Vous pouvez utiliser la commande suivante pour rechercher tous les instantanés associés à une AMI.

```
aws ec2 describe-images --image-id ami_id \
  --query Images[*].BlockDeviceMappings[*].Ebs[].SnapshotId[]
```

Vous pouvez restaurer un instantané en utilisant l'une des méthodes suivantes.

Console

Pour restaurer un instantané à partir de l'archive

Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

1. Dans le panneau de navigation, choisissez Snapshots.
2. Dans la liste des instantanés, sélectionnez l'instantané à archiver, puis choisissez Actions, Restore snapshot (Restaurer l'instantané).
3. Spécifiez le type de restauration à effectuer. Pour Restore type (Type de restauration), effectuez l'une des opérations suivantes :
   - Pour restaurer définitivement l'instantané, sélectionnezPermanent.
   - Pour restaurer temporairement l'instantané, sélectionnez Temporary (Temporaire), puis pour Temporary restore period (Période de restauration temporaire), saisissez le nombre de jours de restauration de l'instantané.
4. Pour confirmer, choisissez Restore snapshot (Restaurer l'instantané).

AWS CLI

Pour restaurer définitivement un instantané archivé

Utilisez la commande . restore-snapshot-tier AWS CLI Pour `--snapshot-id`, spécifiez l'ID de l'instantané à restaurer et incluez l'option `--permanent-restore`.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--permanent-restore
```

Par exemple, la commande suivante restaure définitivement l'instantané `snap-01234567890abcedf`.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--permanent-restore
```

Voici la sortie de cette commande.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Pour restaurer temporairement un instantané archivé

Utilisez la commande . restore-snapshot-tier AWS CLI Omettez l'option `--permanent-restore`. Pour `--snapshot-id`, spécifiez l'ID de l'instantané à restaurer, et pour `--temporary-restore-days`, spécifiez le nombre de jours de restauration de l'instantané.

`--temporary-restore-days` doit être spécifié en jours. La plage autorisée est 1–180. Si vous ne spécifiez aucune valeur, la valeur par défaut est le jour 1.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--temporary-restore-days number_of_days
```

Par exemple, la commande suivante restaure temporairement l'instantané `snap-01234567890abcedf` pour une période de restauration de 5 jours.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--temporary-restore-days 5
```

Voici la sortie de cette commande.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 5,
    "IsPermanentRestore": false
```

```
}
```

Modifier la période de restauration d'un instantané Amazon EBS temporairement restauré

Lorsque vous restaurez temporairement un instantané, vous devez spécifier le nombre de jours pendant lesquels l'instantané doit rester restauré dans votre compte. Une fois la période expirée, l'instantané est automatiquement supprimé du niveau standard.

Vous pouvez modifier la période de restauration d'un instantané temporairement restauré à tout moment.

Vous pouvez choisir d'augmenter ou de diminuer la période de restauration, ou de changer le type de restauration de type temporaire à permanent.

Si vous modifiez la période de restauration, la nouvelle période de restauration est effective à partir de la date actuelle. Par exemple, si vous spécifiez une nouvelle période de restauration de 5 jours, l'instantané restera restauré pendant cinq jours à compter de la date actuelle.

> **Note**
>
> Vous pouvez mettre fin prématurément à une restauration temporaire en fixant la période de restauration à 1 jour.

Si vous changez le type de restauration de temporaire à permanent, la copie de l'instantané est supprimée du niveau d'archivage et l'instantané reste disponible dans votre compte jusqu'à ce que vous le réarchiviez ou que vous le supprimiez manuellement.

Vous pouvez modifier la période de restauration d'un instantané en utilisant l'une des méthodes suivantes.

Console

Pour modifier la période de restauration ou le type de restauration

Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

1. Dans le panneau de navigation, choisissez Snapshots.

2. Dans la liste des instantanés, sélectionnez l'instantané à archiver, puis choisissez Actions, Restore snapshot from archive (Restaurer l'instantané depuis une archive).
3. Pour Restore type (Type de restauration), effectuez l'une des opérations suivantes :
   - Pour passer du type de restauration temporaire à permanent, sélectionnez Permanent.
   - Pour augmenter ou diminuer la période de restauration, conservez Temporary (Temporaire), puis pour Temporary restore period (Période de restauration temporaire), saisissez la nouvelle période de restauration en jours.
4. Pour confirmer, choisissez Restore snapshot (Restaurer l'instantané).

AWS CLI

Pour modifier la période de restauration ou le type de restauration

Utilisez la commande . restore-snapshot-tier AWS CLI Pour `--snapshot-id`, spécifiez l'ID de l'instantané que vous avez précédemment temporairement restauré. Pour passer du type de restauration temporaire à permanent, spécifiez `--permanent-restore` et omettez `--temporary-restore-days`. Pour augmenter ou diminuer la période de restauration, omettez `--permanent-restore` et pour `--temporary-restore-days`, spécifiez la nouvelle période de restauration en jours.

Exemple : augmenter ou diminuer la période de restauration

La commande suivante modifie la période de restauration de l'instantané `snap-01234567890abcedf` pour `10` jours.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--temporary-restore-days 10
```

Voici la sortie de cette commande.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 10,
    "IsPermanentRestore": false
}
```

Exemple : changer le type de restauration en mode permanent

La commande suivante change le type de restauration pour l'instantané `snap-01234567890abcedf` de temporaire à permanent.

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--permanent-restore
```

Voici la sortie de cette commande.

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

Afficher les instantanés Amazon EBS archivés

Vous pouvez afficher les informations sur le niveau de stockage pour les instantanés en utilisant l'une des méthodes suivantes.

Console

Pour afficher les informations de niveau de stockage pour un instantané

Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

1. Dans le panneau de navigation, choisissez Snapshots.
2. Dans la liste des instantanés, sélectionnez l'instantané et choisissez l'onglet Storage tier (Niveau de stockage).

   L'onglet fournit les informations suivantes :

   - Last tier change started on (Dernier changement de niveau démarré le) : date et heure auxquelles la dernière archive ou restauration a démarré.
   - Tier change progress (Progrès du changement de niveau) : la progression de la dernière action d'archivage ou de restauration, sous forme de pourcentage.
   - Storage tier (Niveau de stockage) : niveau de stockage de l'instantané. Toujours `archive` pour les instantanés archivés, et `standard` pour les instantanés stockés sur le niveau standard, y compris les instantanés temporairement restaurés.

- Tiering status (Statut de hiérarchisation) : état de la dernière action d'archivage ou de restauration.
- Archive completed on (Archivage terminée le) : date et heure auxquelles l'archivage s'est terminé.
- Temporary restore expires on (La restauration temporaire expire le) : date et heure auxquelles un instantané restauré temporairement doit expirer.

AWS CLI

Pour afficher les informations d'archivage relatives à un instantané archivé

Utilisez la commande . describe-snapshot-tier-status AWS CLI Spécifiez le filtre `snapshot-id` et pour la valeur du filtre, spécifiez l'ID de l'instantané. Pour afficher tous les instantanés archivés, vous pouvez également omettre le filtre.

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snapshot_id"
```

La sortie comprend les paramètres de réponse suivants :

- `Status` : état de l'instantané. Toujours `completed` pour les instantanés archivés. Seuls les instantanés qui sont dans l'état `completed` peuvent être archivés.
- `LastTieringStartTime` : date et heure auxquelles le processus d'archivage a commencé, au format UTC (AAAA-MM-JJTHH:MM:SSZ).
- `LastTieringOperationState` : état actuel du processus d'archivage. Les états possibles incluent : `archival-in-progress` | `archival-completed` | `archival-failed` | `permanent-restore-in-progress` | `permanent-restore-completed` | `permanent-restore-failed` | `temporary-restore-in-progress` | `temporary-restore-completed` | `temporary-restore-failed`
- `LastTieringProgress` : progression du processus d'archivage des instantanés, sous forme de pourcentage.
- `StorageTier` : niveau de stockage de l'instantané. Toujours `archive` pour les instantanés archivés, et `standard` pour les instantanés stockés sur le niveau standard, y compris les instantanés temporairement restaurés.
- `ArchivalCompleteTime` : date et heure à laquelle le processus d'archivage s'est terminé, au format UTC (AAAA-MM-JJTHH:MM:SSZ).

Exemple

La commande suivante affiche des informations sur l'instantané `snap-01234567890abcedf`.

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snap-01234567890abcedf"
```

Voici la sortie de cette commande.

```
{
    "SnapshotTierStatuses": [
        {
            "Status": "completed",
            "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
            "LastTieringProgress": 100,
            "Tags": [],
            "VolumeId": "vol-01234567890abcedf",
            "LastTieringOperationState": "archival-completed",
            "StorageTier": "archive",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890abcedf",
            "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
        }
    ]
}
```

Pour afficher les instantanés de niveau standard et archivés

Utilisez la commande describe-snapshots AWS CLI . Pour `--snapshot-ids`, spécifiez l'ID de l'instantané à afficher.

```
$ aws ec2 describe-snapshots --snapshot-ids snapshot_id
```

Par exemple, la commande suivante affiche des informations sur l'instantané `snap-01234567890abcedf`.

```
$ aws ec2 describe-snapshots --snapshot-ids snap-01234567890abcedf
```

Voici la sortie de cette commande. Le paramètre de réponse `StorageTier` indique si l'instantané est actuellement archivé. `archive` indique que l'instantané est actuellement archivé et stocké

dans le niveau d'archivage, et `standard` indique que l'instantané n'est actuellement pas archivé et qu'il est stocké dans le niveau standard.

Dans l'exemple de sortie suivant, seul `Snap A` est archivé. `Snap B` et `Snap C` ne le sont pas.

En outre, le paramètre de réponse `RestoreExpiryTime` est renvoyé uniquement pour les instantanés temporairement restaurés à partir de l'archive. Il indique la date à laquelle les instantanés restaurés temporairement doivent être automatiquement retirés du niveau standard. Il n'est pas renvoyé pour les instantanés qui sont restaurés de façon permanente.

Dans l'exemple de sortie suivant, `Snap C` est temporairement restauré, et il sera automatiquement supprimé du niveau standard au 2021-09-19T21:00:00.000Z (19 septembre 2021 à 21 h 00 UTC).


```
{
    "Snapshots": [
        {
            "Description": "Snap A",
            "Encrypted": false,
            "VolumeId": "vol-01234567890aaaaaa",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-09-07T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890aaaaaa",
            "StorageTier": "archive",
            "Tags": []
        },
        {
            "Description": "Snap B",
            "Encrypted": false,
            "VolumeId": "vol-09876543210bbbbbb",
            "State": "completed",
            "VolumeSize": 10,
            "StartTime": "2021-09-14T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09876543210bbbbbb",
            "StorageTier": "standard",
            "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
            "Tags": []
        },
```

```
        {
            "Description": "Snap C",
            "Encrypted": false,
            "VolumeId": "vol-054321543210cccccc",
            "State": "completed",
            "VolumeSize": 12,
            "StartTime": "2021-08-01T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-054321543210cccccc",
            "StorageTier": "standard",
            "Tags": []
        }
    ]
}
```

Pour afficher uniquement les instantanés stockés dans le niveau d'archivage ou le niveau standard

Utilisez la commande describe-snapshots AWS CLI . Incluez l'option `--filter`, pour le nom du filtre, spécifiez `storage-tier`, et pour la valeur du filtre, spécifiez `archive` ou `standard`.

```
aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive|standard"
```

Par exemple, la commande suivante n'affiche que les instantanés archivés.

```
aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

Surveillez l'archivage des instantanés Amazon EBS à l'aide d'Events CloudWatch

Amazon EBS émet des événements liés aux actions d'archivage des instantanés. Vous pouvez utiliser AWS Lambda Amazon CloudWatch Events pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Les événements suivants sont disponibles :

- `archiveSnapshot` : émis lorsqu'une action d'archivage d'un instantané réussit ou échoue.

  Voici un exemple d'événement émis lorsqu'une action d'archivage d'instantané réussit.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Snapshot Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "2021-05-25T13:12:22Z",
   "region": "us-east-1",
   "resources": [
     "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
   ],
   "detail": {
     "event": "archiveSnapshot",
     "result": "succeeded",
     "cause": "",
     "request-id": "123456789",
     "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
     "startTime": "2021-05-25T13:12:22Z",
     "endTime": "2021-05-45T15:30:00Z",
     "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
```

Voici un exemple d'événement émis lorsqu'une action d'archivage d'instantané échoue.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
```

```
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `permanentRestoreSnapshot` : émis lorsqu'une action de restauration permanente réussit ou échoue.

  Voici un exemple d'événement émis lorsqu'une action de restauration permanente réussit.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}
```

  Voici un exemple d'événement émis lorsqu'une action de restauration permanente échoue.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `temporaryRestoreSnapshot` : émis lorsqu'une action de restauration permanente réussit ou échoue.

  Voici un exemple d'événement émis lorsqu'une action de restauration temporaire réussit.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

Voici un exemple d'événement émis lorsqu'une action de restauration temporaire échoue.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `restoreExpiry` : émis lorsque la période de restauration d'un instantané temporairement restauré expire.

  Voici un exemple.

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
```

```
    "event": "restoryExpiry",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```


Supprimer un instantané Amazon EBS

Une fois que vous n'avez plus besoin d'un instantané Amazon EBS d'un volume, vous pouvez le supprimer. La suppression d'un instantané n'a aucun effet sur le volume. La suppression d'un volume n'a aucun effet sur les instantanés créés à partir de celui-ci.

Rubriques

- Considérations relatives à la suppression des instantanés
- Comment fonctionne la suppression d'instantanés incrémentiels
- Suppression d'un instantané
- Supprimer des instantanés en plusieurs volumes

Considérations relatives à la suppression des instantanés

Les considérations suivantes s'appliquent à la suppression des instantanés :

- Vous ne pouvez pas supprimer un instantané de l'appareil racine d'un volume EBS utilisé par une AMI enregistrée. Cette considération s'applique même si l'AMI enregistrée est obsolète ou désactivée. Vous devez commencer par annuler l'inscription de l'AMI avant de pouvoir supprimer l'instantané. Pour plus d'informations, consultez Désenregistrer votre AMI.
- Vous ne pouvez pas supprimer un instantané géré par le AWS Backup service via Amazon EC2. Utilisez-le plutôt AWS Backup pour supprimer les points de restauration correspondants dans le coffre de sauvegarde. Pour plus d'informations, consultez Suppression des sauvegardes dans le Guide du développeur AWS Backup .

- Vous pouvez créer, conserver et supprimer les instantanés manuellement, ou vous pouvez utiliser Amazon Data Lifecycle Manager pour les gérer à votre place. Pour plus d'informations, consultez Amazon Data Lifecycle Manager.
- Même si vous pouvez supprimer un instantané qui est toujours en cours, l'instantané doit être terminé avant que la suppression prenne effet. Cela pourrait prendre beaucoup de temps. En outre, si vous avez atteint votre limite d'instantanés simultanés et que vous tenez de prendre un instantané supplémentaire, vous pouvez obtenir une erreur `ConcurrentSnapshotLimitExceeded`. Pour plus d'informations, consultez les Quotas de service pour Amazon EBS dans le Référence générale d'Amazon Web Services.
- Si vous supprimez un instantané conforme à une règle de conservation de la corbeille, le cliché est conservé dans la corbeille au lieu d'être immédiatement supprimé. Pour plus d'informations, consultez la section Corbeille.
- Vous ne pouvez pas supprimer les instantanés associés à une sauvegarde AMIs EBS désactivée. Pour plus d'informations, consultez la section Désactiver une AMI.
- Vous ne pouvez pas supprimer les instantanés partagés avec vous.
- Si vous supprimez un instantané partagé dont vous êtes le propriétaire, tous les comptes avec lesquels il est partagé n'y ont plus accès.

Comment fonctionne la suppression d'instantanés incrémentiels

Si vous effectuez régulièrement des instantanés d'un volume, les instantanés sont incrémentiels. Cela signifie que seuls les blocs qui ont changé sur l'appareil depuis le dernier instantané sont enregistrés dans le nouvel instantané. Bien que les instantanés soient enregistrés de manière incrémentielle, le processus de suppression de l'instantané prévoit que vous ayez uniquement besoin de conserver l'instantané le plus récent pour créer le volume.

Si des données étaient présentes sur un volume stocké dans un instantané ou une série d'instantanés précédents et que ces données sont supprimées ultérieurement de ce volume, elles sont toujours considérées comme des données uniques d'instantanés antérieurs. Les données uniques sont uniquement supprimées de la séquence d'instantanés si tous les instantanés qui référencent les données uniques sont supprimés.

Lorsque vous supprimez un instantané, seules les données référencées exclusivement par cet instantané sont supprimées. Les données uniques ne sont supprimées que si tous les instantanés qui les référencent sont supprimés. La suppression d'instantanés précédents d'un volume n'a aucune

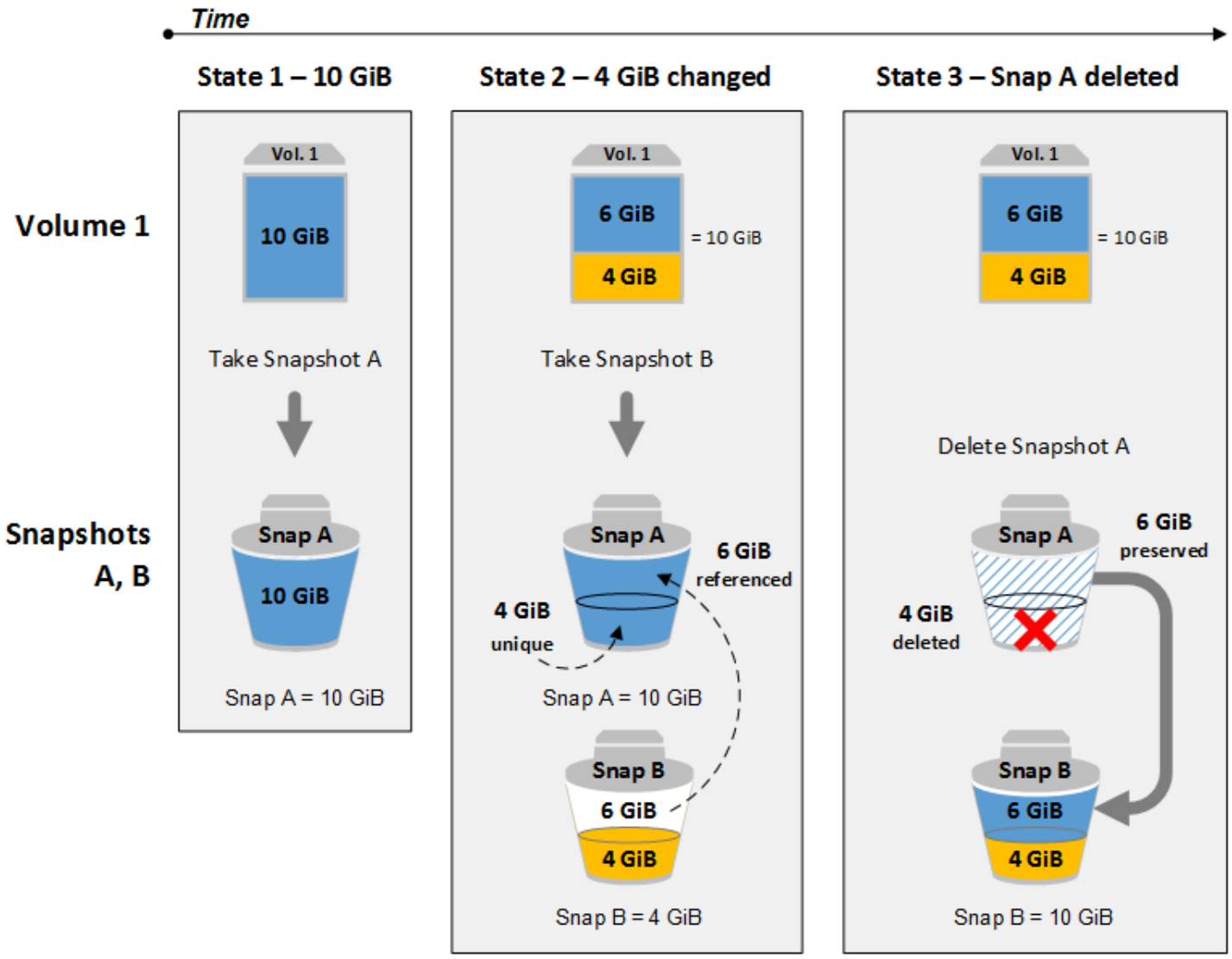
répercussion sur votre capacité à créer des volumes à partir d'instantanés ultérieurs de ce même volume.

La suppression d'un instantané ne réduit pas les coûts de stockage des données de votre organisation. D'autres instantanés peuvent faire référence aux données de cet instantané et les données référencées sont toujours conservées. Si vous supprimez un instantané contenant des données utilisées par un instantané ultérieur, les coûts associés aux données référencées sont alloués à l'instantané ultérieur. Pour plus d'informations sur la façon dont les instantanés stockent les données, consultez Comment fonctionnent les instantanés Amazon EBS et l'exemple ci-dessous.

Dans le graphique suivant, Volume 1 est affiché à trois moments différents. Un instantané a capturé chacun des deux premiers états, et dans le troisième, un instantané a été supprimé.

- Dans l'état 1, le volume contient 10 GiB de données. Comme Snap A est le premier instantané pris du volume, la totalité des 10 Gio de données doit être copiée. Dans cet état, le stockage de 10 GiB de données instantanées vous est facturé.
- Dans l'état 2, le volume contient toujours 10 GiB de données, mais 4 GiB ont changé. Snap B ne stocke que les 4 GiB modifiés après la prise de Snap A, et il fait référence aux 6 GiB de données inchangées déjà stockées dans Snap A. Dans cet état, le stockage de 14 GiB de données instantanées vous est facturé (10 Go pour Snap A + 4 GiB pour Snap B).
- Dans l'état 3, le volume est inchangé mais le Snap A est supprimé. Étant donné que les 6 Go de données inchangées du Snap A sont toujours référencés par le Snap B, ces données sont conservées et associées au Snap B. Les 4 Go de données uniques du Snap A sont supprimés car ils ne sont plus référencés par d'autres instantanés. Dans cet état, vous êtes facturé pour le stockage de 10 Go de données de capture instantanée (6 Go de données conservées dans le Snap A + 4 Go de données dans le Snap B).

Suppression d'un instantané avec certaines de ses données référencées par un autre instantané



Suppression d'un instantané

Pour supprimer un instantané, utilisez l'une des méthodes suivantes.

Console

Pour supprimer un instantané avec la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané que vous souhaitez supprimer, puis choisissez Actions, Delete snapshot (Supprimer l'instantané).
4. Sélectionnez Delete (Supprimer).

AWS CLI

Pour supprimer un instantané à l'aide du AWS CLI

Utilisez la commande delete-snapshot.

Tools for Windows PowerShell

Pour supprimer un instantané à l'aide des Outils pour Windows PowerShell

Utilisez la commande Remove-EC2Snapshot.

> **Conseil pour la résolution de problèmes**
>
> Si un `Failed to delete snapshot` message d'erreur indique que l'instantané est actuellement utilisé par une AMI, vous devez désenregistrer l'AMI associée avant de pouvoir supprimer l'instantané. Vous ne pouvez pas supprimer les instantanés associés à une AMI. Si vous utilisez la console et que l'AMI associée est désactivée, vous devez sélectionner le filtre d'images désactivées à l'AMIsécran pour désactiver l'affichage AMIs.

Supprimer des instantanés en plusieurs volumes

Pour supprimer des instantanés multi-volumes, récupérez tous les instantanés de votre ensemble multi-volume en utilisant l'étiquette que vous avez appliquée à l'ensemble lorsque vous avez créé les instantanés. Ensuite, supprimez individuellement les instantanés.

Vous ne vous verrez pas empêché de supprimer des instantanés individuels dans l'ensemble d'instantanés multi-volumes. Si vous supprimez un instantané alors qu'il se trouve à l'état `pending state`, seul cet instantané est supprimé. Les autres instantanés de l'ensemble d'instantanés multi-volumes sont toujours terminés avec succès.

Restauration d'instantané rapide Amazon EBS

La restauration d'instantané rapide (FSR) Amazon EBS vous permet de créer un volume à partir d'un instantané entièrement initialisé à la création. Elle élimine les temps de latence liés aux opérations d'I/O sur un bloc lors du premier accès à ce dernier. Les volumes créés avec la restauration rapide d'instantané fournissent instantanément la totalité des performances allouées.

Pour commencer, activez la restauration d'instantané rapide pour des instantanés spécifiques dans des zones de disponibilité déterminées. Chaque paire d'instantanés/zones de disponibilité fait référence à une seule restauration d'instantané rapide. Lorsque vous créez un volume à partir d'un de ces instantanés dans l'une de ses zones de disponibilité activées, le volume est restauré à l'aide de la restauration d'instantané rapide.

Vous devez explicitement activer la restauration rapide des instantanés pour chaque instantané. Par exemple, si vous créez un nouvel instantané à partir d'un volume restauré à partir d'un instantané activé pour la restauration rapide des instantanés, le nouvel instantané n'est pas automatiquement activé pour une restauration rapide des instantanés. Si vous copiez un instantané activé pour la restauration rapide des instantanés, la copie d'instantané n'est pas automatiquement activée pour la restauration rapide des instantanés.

Le nombre de volumes que vous pouvez restaurer avec la totalité des bénéfices en matière de performance de la fonction de restauration d'instantané rapide est déterminé par les crédits de création de volume associés à l'instantané. Pour plus d'informations, consultez Crédits de création de volumes Amazon EBS Fast Snapshot Restore.

Vous pouvez activer la restauration d'instantané rapide pour les instantanés que vous possédez et pour les instantanés publics et privés qui sont partagés avec vous.

Table des matières

Considérations

- La restauration rapide des instantanés n'est pas prise en charge avec AWS Outposts Local Zones et Wavelength Zones.
- La restauration rapide des instantanés peut être activée sur des instantanés d'une taille inférieure ou égale à 16 Tio.

- Pour les volumes approvisionnés avec des performances allant jusqu'à 64 000 IOPS et un MiB/s throughput receive the full performance benefit of fast snapshot restore. For volumes provisioned with performance greater than 64,000 IOPS or 1,000 MiB/s débit de 1 000, nous vous recommandons d'initialiser le volume pour bénéficier de toutes ses performances.
- Vous pouvez activer jusqu'à 5 instantanés pour une restauration d'instantané rapide par région. Le quota s'applique aux instantanés que vous possédez et aux instantanés qui sont partagés avec vous. Si vous activez la restauration d'instantané rapide pour un instantané partagé avec vous, elle est comptabilisée dans votre quota de restauration d'instantané rapide. Elle n'est pas comptabilisée dans le quota de restauration rapide du propriétaire de l'instantané.
- Amazon EBS émet des CloudWatch événements Amazon lorsque l'état de restauration rapide d'un instantané change. Pour de plus amples informations, veuillez consulter EBSévénements de restauration rapide des instantanés.

Tarification et facturation

Vous êtes facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée pour un instantané dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure.

Par exemple, si vous activez la restauration d'instantané rapide pour un instantané dans `US-East-1a` pendant un mois (30 jours), vous êtes facturé 540 USD (1instantané x 1 AZ x `720` heures x `$0.75` par heure). Si vous activez la restauration rapide des instantanés pour deux instantanés au `us-east-1a` cours de la même période et `us-east-1c` pour la même période, vous êtes facturé 3 240 $ (2instantanés x `720` heures 3 AZs x par heure). `us-east-1b` `$0.75`

Si vous activez la restauration d'instantané rapide pour un instantané public ou privé partagé avec vous, votre compte est facturé ; le propriétaire de l'instantané ne l'est pas. Lorsqu'un instantané partagé avec vous est supprimé ou non partagé par son propriétaire, la restauration d'instantané rapide est désactivée pour l'instantané dans votre compte et la facturation est arrêtée.

Pour plus d'informations, consultez la section Tarification d'Amazon EBS.

Crédits de création de volumes Amazon EBS Fast Snapshot Restore

Le nombre de volumes qui reçoivent la totalité des bénéfices en matière de performances de la fonction de restauration d'instantané rapide est déterminé par les crédits de création de volume associés à l'instantané. Il y a un compartiment de crédits par instantané et par zone de disponibilité. Chaque volume que vous créez à partir d'un instantané pour lequel la fonction de restauration

d'instantané rapide est activée consomme un crédit du compartiment de crédits. Vous devez disposer d'au moins un crédit dans le compartiment pour créer un volume initialisé à partir de l'instantané. Si vous créez un volume mais qu'il y a moins d'un crédit dans le compartiment, le volume est créé sans bénéficier d'une restauration d'instantané rapide.

Lorsque vous activez la restauration d'instantané rapide pour un instantané partagé avec vous, vous obtenez un compartiment de crédit distinct pour l'instantané partagé dans votre compte. Si vous créez des volumes à partir de l'instantané partagé, les crédits sont consommés à partir de votre compartiment de crédit ; ils ne sont pas consommés à partir du compartiment de crédit du propriétaire de l'instantané.

La taille du compartiment de crédits et sa vitesse de recharge dépendent de celles de l'instantané, ce qui n'est pas le cas de la taille des volumes créés à partir de l'instantané.

Lorsque vous activez la restauration d'instantané rapide pour un instantané, le compartiment de crédits ne contient aucun crédit au départ et se recharge à une vitesse définie jusqu'à ce qu'il atteigne sa capacité de crédits maximale. De plus, au fur et à mesure que vous consommez des crédits, le compartiment de crédits se recharge jusqu'à ce qu'il atteigne sa capacité de crédits maximale.

La vitesse de rechargement de chaque compartiment de crédits est calculée comme suit :

```
MIN (10, (1024 ÷ snapshot_size_gib))
```

Et la taille du compartiment de crédits est calculée comme suit :

```
MAX (1, MIN (10, (1024 ÷ snapshot_size_gib)))
```

Par exemple, si vous activez la restauration d'instantané rapide pour un instantané d'une taille de `128 GiB`, la vitesse de rechargement est de `0.1333` crédits par minute.

```
MIN (10, (1024 ÷ 128))
 = MIN (10, 8)
 = 8 credits per hour
 = 0.1333 credits per minute
```

Et la taille maximale du compartiment de crédits est de 8 crédits.

```
MAX (1, MIN (10, (1024 ÷ 128)))
 = MAX (1, MIN (10, 8))
```

```
= MAX (1, 8)
= 8 credits
```

Dans cet exemple, lorsque vous activez la restauration d'instantané rapide, le compartiment de crédits ne contient aucun crédit au départ. Après 8 minutes, le compartiment de crédits dispose de suffisamment de crédits pour créer un volume initialisé (`0.1333 credits × 8 minutes = 1.066 credits`). Lorsque le compartiment de crédits est plein, vous pouvez créer simultanément 8 volumes initialisés (8 crédits). Lorsque le compartiment est en dessous de sa capacité maximale, il se recharge à une vitesse de `0.1333` crédits par minute.

Vous pouvez utiliser CloudWatch des indicateurs pour surveiller la taille de vos tranches de crédits et le nombre de crédits disponibles dans chaque tranche. Pour de plus amples informations, veuillez consulter Métriques de restauration d'instantané rapide.

Après que vous avez créé un volume à partir d'un instantané avec la fonction de restauration d'instantané rapide activée, vous pouvez décrire le volume à l'aide de describe-volumes et vérifier le champ `fastRestored` e la sortie pour déterminer si le volume a été créé comme volume initialisé à l'aide de la restauration d'instantané rapide.

Configurer la restauration rapide des instantanés pour un instantané Amazon EBS

La restauration d'instantané rapide est désactivée par défaut pour un instantané. Vous pouvez activer ou désactiver la restauration d'instantané rapide pour les instantanés que vous possédez et pour ceux qui sont partagés avec vous. Lorsque vous activez ou désactivez la restauration d'instantané rapide pour un instantané, les modifications s'appliquent uniquement à votre compte.

> **Note**
>
> Lorsque vous activez la restauration d'instantané rapide pour un instantané, votre compte est facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure.

Lorsque vous supprimez un instantané que vous possédez, la restauration d'instantané rapide est automatiquement désactivée pour cet instantané dans votre compte. Si vous avez activé la restauration d'instantané rapide pour un instantané partagé avec vous et que le propriétaire de

l'instantané le supprime ou l'annule, la restauration d'instantané rapide est automatiquement désactivée pour l'instantané partagé dans votre compte.

Si vous avez activé la restauration rapide d'instantané pour un instantané partagé avec vous et que celui-ci est chiffré à l'aide d'une clé CMK personnalisée, la restauration rapide d'instantané n'est pas automatiquement désactivée pour l'instantané lorsque le propriétaire de ce dernier révoque votre accès à la clé CMK personnalisée. Vous devez désactiver manuellement la restauration d'instantané rapide pour cet instantané.

Utilisez la procédure suivante pour activer ou désactiver la restauration rapide d'instantané pour un instantané que vous possédez ou pour un instantané partagé avec vous.

Console

Pour activer ou désactiver la restauration d'instantané rapide

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané, puis choisissez Actions, Manage fast snapshot restore (Gérer la restauration d'instantané rapide).
4. La section Paramètres de restauration rapide d'instantané répertorie toutes les zones de disponibilité dans lesquelles vous pouvez activer la restauration rapide des instantanés pour l'instantané sélectionné. Le paramètre de volume Current status (État actuel) indique si la restauration d'instantané rapide est actuellement activée ou désactivée pour chaque zone.

   Pour activer la restauration d'instantané rapide dans une zone où elle est actuellement désactivée, sélectionnez la zone, choisissez Enable (Activer), puis pour confirmer, choisissez Enable (Activer).

   Pour désactiver la restauration d'instantané rapide dans une zone où elle est actuellement activée, sélectionnez la zone, puis choisissez Disable (Désactiver).
5. Lorsque vous avez apporté les modifications requises, choisissez Close (Fermer).

AWS CLI

Pour gérer la restauration rapide des instantanés à l'aide du AWS CLI

- enable-fast-snapshot-restores
- disable-fast-snapshot-restores

- describe-fast-snapshot-restores

> **Note**
>
> Après avoir activé la restauration rapide d'instantané pour un instantané, il passe à l'état `optimizing`. Les instantanés qui ont l'état `optimizing` offrent certains avantages en termes de performances lors de leur utilisation pour restaurer des volumes. Ils commencent à fournir tous les avantages de performances de la restauration d'instantané rapide uniquement après leur passage l'état `enabled`.

Vérifiez l'état de restauration rapide d'un instantané Amazon EBS

La restauration d'instantané rapide pour un instantané peut être dans l'un des états suivants.

- `enabling` — Une demande d'activation de la fonction de restauration d'instantané rapide a été effectuée.
- `optimizing` — La fonction de restauration d'instantané rapide est en cours d'activation. L'optimisation d'un instantané prend 60 minutes par Tio. Les instantanés dans cet état offrent quelques avantages en termes de performances lors de la restauration de volumes.
- `enabled` — La fonction de restauration d'instantané rapide est activée. Les instantanés qui affichent cet état et qui disposent de suffisamment de crédits de création de volume offrent tous les avantages en termes de performances lors de la restauration de volumes.
- `disabling` — Une demande de désactivation de la fonction de restauration d'instantané rapide a été faite ou une demande d'activation de la fonction de restauration d'instantané rapide a échoué.
- `disabled` — La fonction de restauration d'instantané rapide est désactivée. Vous pouvez réactiver la fonction de restauration d'instantané rapide lorsque vous le souhaitez.

Suivez la procédure suivante afin d'afficher l'état de la restauration d'instantané rapide pour un instantané que vous possédez ou pour un instantané partagé avec vous.

Console

Pour afficher l'état de la restauration d'instantané rapide à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané.
4. Sous l'onglet Details (Détails), Fast Snapshot Restore (Restauration d'instantané rapide) indique l'état de la restauration d'instantané rapide.

AWS CLI

Pour afficher des instantanés avec la fonction de restauration rapide des instantanés activée à l'aide du AWS CLI

Utilisez la describe-fast-snapshot-restorescommande pour décrire les instantanés qui sont activés pour une restauration rapide des instantanés.

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

Voici un exemple de sortie.

```
{
    "FastSnapshotRestores": [
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2a",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        },
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2b",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
```

```
        }
    ]
}
```

Afficher les volumes Amazon EBS restaurés à l'aide de la restauration rapide par capture instantanée

Lorsque vous créez un volume à partir d'un instantané qui est activé pour la restauration d'instantané rapide dans la zone de disponibilité du volume, il est restauré à l'aide de la restauration d'instantané rapide.

Utilisez la commande describe-volumes pour afficher les volumes qui ont été créés à partir d'un instantané activé pour la restauration d'instantané rapide.

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

Voici un exemple de sortie.

```
{
    "Volumes": [
        {
            "Attachments": [],
            "AvailabilityZone": "us-east-2a",
            "CreateTime": "2020-01-26T00:34:11.093Z",
            "Encrypted": true,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513e232e843",
            "Size": 20,
            "SnapshotId": "snap-0e946653493cb0447",
            "State": "available",
            "VolumeId": "vol-0d371921d4ca797b0",
            "Iops": 100,
            "VolumeType": "gp2",
            "FastRestored": true
        }
    ]
}
```

Verrouillage d'instantanés Amazon EBS

Vous pouvez verrouiller vos instantanés Amazon EBS pour les protéger contre les suppressions accidentelles ou malveillantes, ou pour les stocker au format WORM (write-once-read-many) pendant une durée déterminée. Lorsqu'un instantané est verrouillé, aucun utilisateur ne peut le supprimer, quelles que soient ses autorisations IAM. Une fois qu'il est restauré, vous pouvez utiliser un instantané de la même manière que n'importe quel autre instantané.

> **Note**
>
> Le verrouillage d'instantané a été évalué par Cohasset Associates en vue de son utilisation dans les environnements soumis aux réglementations SEC 17a-4, CFTC et FINRA. Pour de plus amples informations sur la conformité de la fonctionnalité de verrouillage d'instantané vis-à-vis de ces réglementations, consultez le document Cohasset Associates Compliance Assessment.

Vous pouvez verrouiller les instantanés selon le mode de conformité ou le mode de gouvernance, et ils peuvent être verrouillés pendant une durée spécifique ou jusqu'à une date précise. Pour plus d'informations, consultez Mode de verrouillage et Durée du verrouillage.

Tarification

Vous pouvez verrouiller et déverrouiller les instantanés sans frais supplémentaires. Vous payez les frais de stockage standard des instantanés Amazon EBS pour les instantanés verrouillés.

Rubriques

- Concepts de verrouillage instantané Amazon EBS
- Considérations relatives au verrouillage instantané Amazon EBS
- Contrôlez l'accès à Amazon EBS Snapshot Lock
- Verrouiller un instantané Amazon EBS
- Déverrouillez un instantané Amazon EBS
- Mettre à jour les paramètres de verrouillage des instantanés Amazon EBS
- Surveiller le verrouillage des instantanés Amazon EBS

Concepts de verrouillage instantané Amazon EBS

Les concepts suivants sont importants à comprendre lorsque vous commencez à utiliser le verrouillage par capture instantanée.

Table des matières

Mode de verrouillage

Vous pouvez verrouiller un instantané dans l'un des deux modes suivants :

Mode gouvernance

Une fois qu'un instantané est verrouillé, les utilisateurs disposant des autorisations IAM appropriées peuvent le déverrouiller et modifier le mode de verrouillage ainsi que la durée ou la date d'expiration du verrouillage à tout moment. Lorsque vous verrouillez un instantané en mode de gouvernance, celui-ci est immédiatement verrouillé ; il n'y a pas de période de réflexion. Pour supprimer un instantané une fois qu'il a été verrouillé en mode de gouvernance, vous devez d'abord le déverrouiller ou attendre que le verrouillage expire.

Vous pouvez utiliser le mode de gouvernance pour répondre aux exigences de gouvernance des données de votre entreprise en vous assurant que seuls certains utilisateurs sont autorisés à déverrouiller des instantanés et à modifier les configurations de verrouillage d'instantané. Vous pouvez également utiliser le mode de gouvernance pour tester la configuration de votre verrouillage avant de verrouiller un instantané en mode de conformité.

Mode conformité

Lorsque vous verrouillez un instantané en mode de conformité, vous pouvez spécifier une période de réflexion qui démarre immédiatement après avoir verrouillé l'instantané. Pendant la période de réflexion, les utilisateurs disposant des autorisations appropriées peuvent déverrouiller l'instantané, modifier le mode de verrouillage, augmenter ou diminuer la période de réflexion et augmenter ou diminuer la durée ou la date d'expiration du verrouillage. Une fois la période de réflexion expirée, vous ne pouvez pas déverrouiller l'instantané, modifier le mode de verrouillage ou réduire la durée

ou la date d'expiration du verrouillage ; vous pouvez uniquement augmenter la durée ou la date d'expiration du verrouillage. Pour supprimer un instantané une fois qu'il a été verrouillé conformément à la réglementation et que la période de réflexion a expiré, vous devez attendre que le verrouillage expire.

> **Note**
>
> Vous pouvez verrouiller un instantané en mode de conformité sans période de réflexion en omettant ce délai dans la requête. Dans ce cas, le verrouillage devient effectif immédiatement, et vous ne pouvez pas déverrouiller l'instantané, modifier le mode de verrouillage ou réduire la durée ou la date d'expiration du verrouillage ; vous pouvez uniquement augmenter la durée ou la date d'expiration du verrouillage.

Vous pouvez utiliser le mode de conformité pour protéger les instantanés qui ne doivent pas être supprimés pendant une période spécifique pour des raisons de conformité. Le mode de conformité offre les avantages suivants :

- il permet la configuration WORM (write-once, read-many) pour vos instantanés ;
- il fournit une couche de défense supplémentaire qui protège les instantanés contre les suppressions accidentelles ou malveillantes ;
- il applique des périodes de conservation, qui empêchent les suppressions anticipées par des utilisateurs privilégiés, afin de respecter les politiques et procédures de protection des données de votre entreprise.

> **Note**
>
> La seule façon de supprimer un instantané verrouillé en mode de conformité avant l'expiration de son verrouillage est de fermer le AWS compte associé.

Durée du verrouillage

La durée du verrouillage est la période pendant laquelle l'instantané doit rester verrouillé. Vous pouvez spécifier la durée du verrouillage d'une des deux façons suivantes, mais des deux en même temps :

Nombre de jours

La durée du verrouillage est spécifiée sous la forme d'un nombre de jours pendant lesquels l'instantané doit rester verrouillé. Une fois le nombre de jours spécifié écoulé, l'instantané est automatiquement déverrouillé. La durée peut aller de 1 jour à 36 500 jours (100 ans).

Date d'expiration du verrouillage

La durée du verrouillage est déterminée par une date d'expiration future. L'instantané reste verrouillé jusqu'à ce que la date d'expiration du verrouillage soit atteinte. Lorsque la date d'expiration du verrouillage est atteinte, l'instantané est automatiquement déverrouillé.

Période de réflexion

La période de réflexion est une période facultative que vous pouvez spécifier lorsque vous verrouillez un instantané en mode de conformité. Pendant la période de réflexion, les utilisateurs disposant des autorisations appropriées peuvent déverrouiller l'instantané, modifier le mode de verrouillage, augmenter ou diminuer la période de réflexion et augmenter ou diminuer la durée du verrouillage. Une fois la période de réflexion expirée, les utilisateurs ne peuvent pas déverrouiller l'instantané, modifier le mode de verrouillage, rétablir la période de réflexion ou réduire la durée du verrouillage, quelles que soient leurs autorisations.

Il n'est pas possible de supprimer un instantané pendant la période de réflexion.

Si cela est spécifié, la période de réflexion commence immédiatement après le verrouillage de l'instantané. Si cela est omis, l'instantané est immédiatement verrouillé en mode de conformité sans période de réflexion.

La période de réflexion peut aller de 1 à 72 heures. Pour verrouiller un instantané en mode de conformité immédiatement sans période de réflexion, ne spécifiez pas ce délai dans la requête.

État du verrouillage

Un verrouillage d'instantané peut avoir l'un des états suivants :

- `compliance-cooloff` : l'instantané a été verrouillé en mode de conformité, mais sa période de réflexion est toujours en cours. L'instantané ne peut pas être supprimé, mais il peut être déverrouillé et les paramètres de verrouillage peuvent être modifiés par les utilisateurs disposant des autorisations appropriées.
- `governance` : l'instantané est verrouillé en mode de gouvernance. L'instantané ne peut pas être supprimé, mais il peut être déverrouillé et les paramètres de verrouillage peuvent être modifiés par les utilisateurs disposant des autorisations appropriées.

- `compliance` : l'instantané est verrouillé en mode de conformité sans période de réflexion ou la période de réflexion a expiré. L'instantané ne peut pas être déverrouillé ou supprimé. La durée du verrouillage ne peut être augmentée que par les utilisateurs disposant des autorisations appropriées.
- `expired` : l'instantané a été verrouillé en mode de conformité ou de gouvernance, mais le verrouillage a expiré. L'instantané n'est pas verrouillé et peut être supprimé.

Considérations relatives au verrouillage instantané Amazon EBS

Tenez compte des points suivants lorsque vous verrouillez les instantanés Amazon EBS.

- Vous ne pouvez verrouiller un instantané que s'il est à l'état `pending` ou `completed`.
  - Si vous verrouillez un instantané alors qu'il est à l'état `pending`, et que vous le verrouillez pendant une durée spécifique, la durée de verrouillage ne commence que lorsque l'instantané atteint l'état `completed`. L'instantané ne peut pas être supprimé tant qu'il est à l'état `pending`.
  - Si vous verrouillez un instantané alors qu'il est à l'état `pending` et que la création de l'instantané échoue pour une raison quelconque, le verrouillage est annulé.
- Si vous prolongez la durée de verrouillage d'un instantané verrouillé en mode de conformité après l'expiration de la période de réflexion, vous ne pouvez pas spécifier une autre période de réflexion. Si vous spécifiez une période de réflexion, la requête échoue.
- Vous pouvez verrouiller les instantanés archivés. Et vous pouvez archiver les instantanés verrouillés.
- Vous pouvez verrouiller les instantanés associés à une AMI.
- Vous pouvez annuler l'inscription d'une AMI qui a des instantanés verrouillés associés.
- Vous pouvez supprimer la clé KMS utilisée pour chiffrer un instantané verrouillé.
- Nous vous recommandons de ne pas verrouiller les instantanés créés par AWS Backup. AWS Backup garantit déjà que ses instantanés ne sont pas supprimés avant l'expiration de leur période de conservation. Pour ajouter un niveau de sécurité supplémentaire aux instantanés gérés par AWS Backup, nous vous recommandons d'utiliser AWS Backup Vault Lock. Pour plus d'informations, consultez la page AWS Backup Vault Lock.
- Vous ne pouvez pas verrouiller les instantanés lors de leur création ou de l'inscription de l'AMI.
- Vous ne pouvez pas verrouiller les instantanés Amazon EBS locaux sur AWS Outposts.
- La seule façon de supprimer un instantané verrouillé en mode de conformité avant l'expiration de son verrouillage est de fermer le AWS compte associé.

Si vous fermez votre AWS compte alors que vous avez verrouillé les instantanés, votre compte est AWS suspendu pendant 90 jours en conservant vos instantanés intacts. Si vous ne rouvrez pas votre compte dans les 90 jours, AWS supprime vos instantanés, même s'ils sont verrouillés.

Contrôlez l'accès à Amazon EBS Snapshot Lock

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les verrouillages d'instantanés. Pour permettre aux utilisateurs d'utiliser les verrouillages d'instantanés, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Pour plus d'informations, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Rubriques

- Autorisations requises
- Limitation de l'accès avec des clés de condition

Autorisations requises

Pour utiliser les verrouillages d'instantanés, les utilisateurs ont besoin des autorisations suivantes.

- `ec2:LockSnapshot` : pour verrouiller les instantanés.
- `ec2:UnlockSnapshot` : pour déverrouiller les instantanés.
- `ec2:DescribeLockedSnapshots` : pour afficher les paramètres de verrouillage d'instantané.

Voici un exemple de politique IAM qui autorise les utilisateurs à verrouiller et déverrouiller des instantanés et à afficher les paramètres de verrouillage d'instantané. Elle inclut l'autorisation `ec2:DescribeSnapshots` pour les utilisateurs de la console. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:LockSnapshot",
            "ec2:UnlockSnapshot",
            "ec2:DescribeLockedSnapshots",
            "ec2:DescribeSnapshots"
```

```
        ]
    }]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Limitation de l'accès avec des clés de condition

Vous pouvez utiliser des clés de condition pour limiter la manière dont les utilisateurs sont autorisés à verrouiller les instantanés.

Rubriques

- EC2 : SnapshotLockDuration
- EC2 : CoolOffPeriod

EC2 : SnapshotLockDuration

Vous pouvez utiliser la clé de condition `ec2:SnapshotLockDuration` pour limiter les utilisateurs à des durées de verrouillage spécifiques lors du verrouillage d'instantanés.

L'exemple de politique suivant limite les utilisateurs à spécifier une durée de verrouillage comprise entre `10` et `50` jours.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan" : {
          "ec2:SnapshotLockDuration" : 10
        }
        "NumericLessThan":{
          "ec2:SnapshotLockDuration": 50
        }
      }
    }
  ]
}
```

EC2 : CoolOffPeriod

Vous pouvez utiliser la clé de condition `ec2:CoolOffPeriod` pour empêcher les utilisateurs de verrouiller les instantanés en mode de conformité sans période de réflexion.

L'exemple de politique suivant limite les utilisateurs à spécifier une période de réflexion supérieure à 48 heures lorsqu'ils verrouillent des instantanés en mode de conformité.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan": {
          "ec2:CoolOffPeriod": 48
        }
      }
    }
  ]
}
```

Verrouiller un instantané Amazon EBS

Vous pouvez verrouiller un instantané qui est à l'état `pending` ou `completed`. Pour de plus amples informations, veuillez consulter Considérations relatives au verrouillage instantané Amazon EBS.

Console

Pour verrouiller un instantané

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané à verrouiller, puis choisissez Actions, Paramètres d'instantané, Gérer le verrouillage d'instantané.
4. Sélectionnez Verrouiller l'instantané.
5. Pour Mode de verrouillage, choisissez Mode de gouvernance ou Mode de conformité. Pour de plus amples informations, veuillez consulter Mode de verrouillage.
6. Pour Durée du verrouillage, effectuez l'une des opérations suivantes :

   - Pour verrouiller l'instantané pendant une période spécifique, choisissez Verrouiller l'instantané pour, puis saisissez la période en jours ou en années.
   - Pour verrouiller l'instantané jusqu'à une date et une heure spécifiques, choisissez Verrouiller l'instantané jusqu'à, puis sélectionnez la date et l'heure d'expiration.

   Pour de plus amples informations, veuillez consulter Durée du verrouillage.
7. (Mode de conformité uniquement) Pour Période de réflexion, spécifiez une période de réflexion pendant laquelle vous pouvez déverrouiller l'instantané et modifier la configuration du verrouillage. Pour de plus amples informations, veuillez consulter Période de réflexion.
8. (Mode de conformité uniquement) Pour confirmer que vous souhaitez verrouiller l'instantané en mode de conformité et que vous ne pourrez pas le déverrouiller après l'expiration de la période de réflexion, choisissez Reconnaître.
9. Choisissez Enregistrer les paramètres de verrouillage.

AWS CLI

Pour verrouiller un instantané en mode de gouvernance

Utilisez la commande lock-snapshot de l' AWS CLI . Pour `--snapshot-id`, spécifiez l'ID de l'instantané à verrouiller. Pour `--lock-mode`, spécifiez `governance`. Pour verrouiller l'instantané pendant une période spécifique, pour`--lock-duration`, spécifiez la période pendant laquelle vous souhaitez verrouiller l'instantané. Sinon, pour verrouiller l'instantané jusqu'à une date précise, pour `--expiration-date`, spécifiez la date et l'heure auxquelles le verrouillage doit expirer, dans le fuseau horaire UTC (`YYYY-MM-DDThh:mm:ss.sssZ`).

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \
 --lock-mode governance \
 --lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Pour verrouiller un instantané en mode de conformité

Utilisez la commande lock-snapshot de l' AWS CLI . Pour `--snapshot-id`, spécifiez l'ID de l'instantané à verrouiller. Pour `--lock-mode`, spécifiez `compliance`. Pour `--cool-off-period`, vous pouvez spécifier une période de réflexion en heures. Pour verrouiller l'instantané pendant une période spécifique, pour`--lock-duration`, spécifiez la période pendant laquelle vous souhaitez verrouiller l'instantané. Sinon, pour verrouiller l'instantané jusqu'à une date précise, pour `--expiration-date`, spécifiez la date et l'heure auxquelles le verrouillage doit expirer, dans le fuseau horaire UTC (`YYYY-MM-DDThh:mm:ss.sssZ`).

```
$ aws ec2 lock-snapshot --snapshot-id snapshot_id \
 --lock-mode compliance \
 --cool-off-period 1-72_hours \
 --lock-duration 1-36500_days | --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

Déverrouillez un instantané Amazon EBS

Vous ne pouvez déverrouiller un instantané que s'il est verrouillé en mode de gouvernance ou s'il est verrouillé en mode de conformité et qu'il est toujours dans la période de réflexion.

Console

Pour déverrouiller un instantané

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.

3. Sélectionnez l'instantané à déverrouiller, puis choisissez Actions, Paramètres d'instantané, Gérer le verrouillage d'instantané.
4. Choisissez Déverrouiller un instantané, puis choisissez à nouveau Déverrouiller un instantané pour confirmer.

AWS CLI

Pour déverrouiller un instantané

Utilisez la commande unlock-snapshot de l' AWS CLI . Pour `--snapshot-id`, spécifiez l'ID de l'instantané à déverrouiller.

```
$ aws ec2 unlock-snapshot --snapshot-id snapshot_id
```

Mettre à jour les paramètres de verrouillage des instantanés Amazon EBS

Les mises à jour autorisées dépendent de l'état du verrouillage :

- `governance` : vous pouvez modifier le mode de verrouillage et augmenter ou diminuer la durée ou la date d'expiration du verrouillage.
- `compliance-cooloff` : vous pouvez modifier le mode de verrouillage, augmenter ou diminuer la période de réflexion, et augmenter ou diminuer la durée ou la date d'expiration du verrouillage.
- `compliance` : vous pouvez uniquement augmenter la durée ou la date d'expiration du verrouillage.

Console

Pour mettre à jour les paramètres de verrouillage d'instantané

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Snapshots.
3. Sélectionnez l'instantané pour lequel vous souhaitez modifier les paramètres de verrouillage, puis choisissez Actions, Paramètres d'instantané, Gérer le verrouillage d'instantané.
4. Mettez à jour les paramètres selon vos besoins, puis choisissez Enregistrer les paramètres de verrouillage.

AWS CLI

Pour mettre à jour les paramètres de verrouillage d'instantané

Utilisez la commande lock-snapshot de l' AWS CLI . Pour `--snapshot-id`, spécifiez l'ID de l'instantané pour lequel vous souhaitez mettre à jour les paramètres de verrouillage. Ensuite, spécifiez uniquement les options à modifier.

Surveiller le verrouillage des instantanés Amazon EBS

Vous pouvez surveiller les actions liées au verrouillage des instantanés Amazon EBS à l'aide des outils suivants :

Rubriques

- Surveillez les blocages de snapshots Amazon EBS à l'aide de AWS CloudTrail
- Surveillez les blocages de snapshots Amazon EBS à l'aide d'Amazon EventBridge

Surveillez les blocages de snapshots Amazon EBS à l'aide de AWS CloudTrail

Vous pouvez surveiller les appels d'API pour les verrouillages instantanés sous forme d'événements, y compris les appels depuis la console et depuis des appels de code vers le APIs. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour plus d'informations, consultez la section Enregistrer les appels d'API à l'aide de AWS CloudTrail.

Surveillez les blocages de snapshots Amazon EBS à l'aide d'Amazon EventBridge

Amazon EBS émet des événements liés aux actions de verrouillage d'instantané. Vous pouvez utiliser AWS Lambda Amazon EventBridge pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Les événements suivants sont émis :

- Instantané verrouillé avec succès en mode de gouvernance ou de conformité.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "source": 012345678901,
    "lockState": "compliance-cooloff",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Échec du verrouillage lorsqu'un instantané est verrouillé alors qu'il est à l'état `pending` et qu'il ne parvient pas à atteindre l'état `completed`.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
```

```
    "result": "failed",
    "cause": "snapshot failed",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "pending-compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- Verrouillage expiré

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockDurationExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "expired",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123
  }
}
```

- La période de réflexion a expiré après avoir le verrouillage en mode de conformité.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
```

```
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "cooloffperiodExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Bloquer l'accès public aux instantanés Amazon EBS

Pour empêcher le partage public de vos instantanés, vous pouvez activer le blocage de l'accès public pour les instantanés. Une fois que vous avez activé le blocage de l'accès public pour les instantanés dans une région, toute tentative de partage public d'instantanés dans cette région est automatiquement bloquée. Cela peut vous aider à améliorer la sécurité de vos instantanés et à protéger les données de vos instantanés contre tout accès non autorisé ou involontaire.

Le blocage de l'accès public pour les instantanés peut être activé dans l'un des deux modes suivants :

- Bloquer tous les partages : bloque tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- Bloquer les nouveaux partages : bloque tout nouveau partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

Considérations

Tenez compte des points suivants lorsque vous utilisez le blocage de l'accès public pour les instantanés.

- Bloquer l'accès public aux instantanés n'empêche pas le partage d'instantanés privés.
- L'activation du blocage de l'accès public pour les instantanés en mode de partage complet ne modifie pas les autorisations pour les instantanés déjà partagés publiquement. À la place, ces instantanés ne sont plus visibles et accessibles au public. Les attributs de ces instantanés indiquent donc toujours qu'ils sont partagés publiquement, même s'ils ne sont pas accessibles au public.

  Si vous désactivez ultérieurement le blocage de l'accès public ou si vous modifiez le mode pour bloquer tout nouveau partage, ces instantanés seront de nouveau accessibles au public.
- Le blocage de l'accès public pour les instantanés est un paramètre régional. Il s'applique à tous les instantanés de la région dans laquelle il est activé. Vous devez activer le blocage de l'accès public pour les instantanés dans chaque région dans laquelle vous souhaitez empêcher le partage public de vos instantanés.
- Le bloquer de l'accès public est un paramètre défini au niveau du compte. Il s'applique à tous les utilisateurs du compte, y compris aux utilisateurs administrateurs. Vous ne pouvez pas activer le blocage de l'accès public pour les instantanés au niveau de l'entreprise.
- Le paramètre de blocage de l'accès public est configuré soit directement dans le compte, soit à l'aide d'une politique déclarative. L'utilisation d'une politique déclarative vous permet d'appliquer le paramètre à plusieurs régions simultanément, ainsi qu'à plusieurs comptes simultanément. Lorsqu'une politique déclarative est utilisée, vous ne pouvez pas modifier le paramètre directement dans un compte. Cette rubrique décrit comment configurer le paramètre directement dans un compte. Pour plus d'informations sur l'utilisation des politiques déclaratives, consultez la section Politiques déclaratives dans le Guide de l'utilisateur AWS Organizations .
- Bloquer l'accès public aux instantanés n'empêche pas le partage public des instantanés sauvegardés par AMIs EBS. Si vous activez le blocage de l'accès public aux instantanés, les utilisateurs peuvent toujours partager publiquement des données soutenues par AMIs EBS. Si une AMI basée sur EBS est partagée publiquement, les utilisateurs ayant accès à cette AMI peuvent créer des volumes à partir des instantanés associés. Pour empêcher le partage public de votre contenu AMIs, activez le blocage de l'accès public pour AMIs.
- Le blocage de l'accès public aux instantanés n'est pas pris en charge lorsque les instantanés locaux sont activés. AWS Outposts

Tarification

Le blocage de l'accès public pour les instantanés peut être activé sans frais supplémentaires.

Table des matières

Autorisations IAM pour bloquer l'accès public aux instantanés Amazon EBS

Par défaut, les utilisateurs ne sont pas autorisés à utiliser le blocage de l'accès public pour les instantanés. Pour permettre aux utilisateurs d'utiliser le blocage de l'accès public pour les instantanés, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter les autorisations à vos utilisateurs, groupes ou rôles.

Pour utiliser le blocage de l'accès public pour les instantanés, les utilisateurs ont besoin des autorisations suivantes.

- `ec2:EnableSnapshotBlockPublicAccess` : activer le blocage de l'accès public pour les instantanés et modifier le mode.
- `ec2:DisableSnapshotBlockPublicAccess` : désactiver le blocage de l'accès public pour les instantanés
- `ec2:GetSnapshotBlockPublicAccessState` : afficher le paramètre de blocage de l'accès public pour instantanés pour une région.

Voici un exemple de politique IAM. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

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

```
            "ec2:EnableSnapshotBlockPublicAccess",
            "ec2:DisableSnapshotBlockPublicAccess",
            "ec2:GetSnapshotBlockPublicAccessState"
        ],
        "Resource": "*"
    }]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Configurer le blocage de l'accès public pour les instantanés Amazon EBS

Activez le blocage de l'accès public pour les instantanés pour empêcher le partage public des instantanés dans la région. Une fois cette fonctionnalité activée, les demandes de partage public d'instantanés dans la région sont bloquées.

> **Important**
>
> L'activation du blocage de l'accès public pour les instantanés en mode de partage complet ne modifie pas les autorisations pour les instantanés déjà partagés publiquement. À la place, ces instantanés ne sont plus visibles et accessibles au public. Les attributs de ces instantanés indiquent donc toujours qu'ils sont partagés publiquement, même s'ils ne sont pas accessibles au public.

Si vous désactivez ultérieurement le blocage de l'accès public ou si vous modifiez le mode pour bloquer tout nouveau partage, ces instantanés seront de nouveau accessibles au public.

> **Note**
>
> Ce paramètre est configuré au niveau du compte, soit directement dans le compte, soit à l'aide d'une politique déclarative. Il doit être configuré dans chaque Région AWS endroit où vous souhaitez empêcher le partage public de clichés. L'utilisation d'une politique déclarative vous permet d'appliquer le paramètre à plusieurs régions simultanément, ainsi qu'à plusieurs comptes simultanément. Lorsqu'une politique déclarative est utilisée, vous ne pouvez pas modifier le paramètre directement dans un compte. Cette rubrique décrit comment configurer le paramètre directement dans un compte. Pour plus d'informations sur l'utilisation des politiques déclaratives, consultez la section Politiques déclaratives dans le Guide de l'utilisateur AWS Organizations .

Console

Pour configurer le blocage de l'accès public pour les instantanés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez EC2 Tableau de bord, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. Dans la section Bloquer l'accès public pour les instantanés EBS, choisissez Gérer.
4. Sélectionnez Bloquer l'accès public, puis choisissez l'une des options suivantes :
   - Bloquer tous les accès publics : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
   - Bloquer les nouveaux partages publics : pour bloquer tout nouveau partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.
5. Choisissez Mettre à jour.

AWS CLI

Pour activer ou modifier le blocage de l'accès public pour les instantanés

Utilisez la commande enable-snapshot-block-public-access. Pour `--state`, spécifiez l'une des valeurs suivantes :

- `block-all-sharing` : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- `block-new-sharing` : pour bloquer uniquement les nouveaux partages publics de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

Pour activer ou modifier le blocage de l'accès public aux instantanés d'une région spécifique

```
aws ec2 enable-snapshot-block-public-access \
--state block-all-sharing|block-new-sharing \
--region us-east-1
```

Exemple de sortie

```
{
    "State": "block-new-sharing"
}
```

Pour activer ou modifier le blocage de l'accès public aux instantanés pour toutes les régions

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-snapshot-block-public-access \
            --region $region \
```

```
            --state block-all-sharing|block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Exemple de sortie

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
…
```

Tools for PowerShell

Pour activer ou modifier le blocage de l'accès public pour les instantanés

Utilisez la commande Enable-EC2SnapshotBlockPublicAccess. Pour `-State`, spécifiez l'une des valeurs suivantes :

- `block-all-sharing` : pour bloquer tout partage public de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont plus accessibles au public.
- `block-new-sharing` : pour bloquer uniquement les nouveaux partages publics de vos instantanés. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.

Pour activer ou modifier le blocage de l'accès public aux instantanés d'une région spécifique

```
Enable-EC2SnapshotBlockPublicAccess `
-Region us-east-1 `
-State block-new-sharing | block-all-sharing
```

Exemple de sortie

```
Value
-----
```

```
block-new-sharing
```

Pour activer ou modifier le blocage de l'accès public aux instantanés pour toutes les régions

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
            Enable-EC2SnapshotBlockPublicAccess `
                -Region $_ `
                -State block-new-sharing | block-all-sharing)
    }
} | `
Format-Table -AutoSize
```

Exemple de sortie

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

Afficher le paramètre de blocage de l'accès public pour les instantanés Amazon EBS

Vous pouvez bloquer l'accès public dans l'un des états suivants pour chaque région de votre compte.

- Bloquer tous les partages : tous les partages publics de vos instantanés sont bloqués. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. En outre, les instantanés déjà partagés publiquement sont considérés comme privés et ne sont pas accessibles au public.
- Bloquer les nouveaux partages : seuls les nouveaux partages de vos instantanés sont bloqués. Les utilisateurs du compte ne peuvent pas demander un nouveau partage public. Cependant, les instantanés déjà partagés publiquement restent accessibles au public.
- Débloqué : le partage public n'est pas bloqué. Les utilisateurs peuvent partager des instantanés publiquement.

Console

Pour afficher le paramètre de blocage de l'accès public pour les instantanés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez EC2 Tableau de bord, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. La section Bloquer l'accès public pour les instantanés EBS montre le paramètre actuel.

AWS CLI

Pour afficher le paramètre de blocage de l'accès public pour les instantanés

Utilisez la commande get-snapshot-block-public-access-state.

- Pour une région spécifique

```
aws ec2 get-snapshot-block-public-access-state --region us-east-1
```

Exemple de sortie

Le champ indique `ManagedBy` l'entité qui a configuré le paramètre. Dans cet exemple, `account` indique que le paramètre a été configuré directement dans le compte. Une valeur de `declarative-policy` signifierait que le paramètre a été configuré par une politique déclarative. Pour plus d'informations, consultez la section Politiques déclaratives dans le Guide de l'utilisateur AWS Organizations .

```
{
    "State": "unblocked",
    "ManagedBy": "account"
}
```

- Pour toutes les régions

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
```

```
        --output text
    );
    do (output=$(
        aws ec2 get-snapshot-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Exemple de sortie

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
```

Tools for Windows PowerShell

Pour afficher le paramètre de blocage de l'accès public pour les instantanés

Utilisez la commande Get-EC2SnapshotBlockPublicAccessState.

- Pour une région spécifique

```
Get-EC2SnapshotBlockPublicAccessState -Region us-east-1
```

Exemple de sortie

```
Value
-----
block-new-sharing
```

- Pour toutes les régions

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Get-EC2SnapshotBlockPublicAccessState -Region $_)
```

```
    }
} | `
Format-Table -AutoSize
```

Exemple de sortie

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

Désactiver le blocage de l'accès public pour les instantanés Amazon EBS

Désactivez le blocage de l'accès public pour les instantanés pour autoriser le partage public des instantanés dans la région. Une fois cette fonctionnalité désactivée, les utilisateurs peuvent partager publiquement des instantanés dans la région.

Important

L'activation du blocage de l'accès public pour les instantanés en mode de partage complet ne modifie pas les autorisations pour les instantanés déjà partagés publiquement. À la place, ces instantanés ne sont plus visibles et accessibles au public. Les attributs de ces instantanés indiquent donc toujours qu'ils sont partagés publiquement, même s'ils ne sont pas accessibles au public.
Si vous désactivez le blocage de l'accès public, ces instantanés seront à nouveau accessibles au public.

Note

Ce paramètre est configuré au niveau du compte, soit directement dans le compte, soit à l'aide d'une politique déclarative. Il doit être configuré dans chaque Région AWS endroit où vous souhaitez autoriser le partage public des instantanés. L'utilisation d'une politique déclarative vous permet d'appliquer le paramètre à plusieurs régions simultanément, ainsi qu'à plusieurs comptes simultanément. Lorsqu'une politique déclarative est utilisée, vous ne pouvez pas modifier le paramètre directement dans un compte. Cette rubrique décrit

comment configurer le paramètre directement dans un compte. Pour plus d'informations sur l'utilisation des politiques déclaratives, consultez la section Politiques déclaratives dans le Guide de l'utilisateur AWS Organizations .

Console

Pour désactiver le blocage de l'accès public pour les instantanés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez EC2 Tableau de bord, puis dans Attributs du compte (sur le côté droit), choisissez Protection et sécurité des données.
3. Dans la section Bloquer l'accès public pour les instantanés EBS, choisissez Gérer.
4. Effacez Bloquer l'accès public et choisissez Enregistrer.

AWS CLI

Pour désactiver le blocage de l'accès public pour les instantanés

Utilisez la commande disable-snapshot-block-public-access.

- Pour une région spécifique

```
aws ec2 disable-snapshot-block-public-access --region us-east-1
```

Exemple de sortie

```
{
    "State": "unblocked"
}
```

- Pour toutes les régions

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
```

```
    );
    do (output=$(
        aws ec2 disable-snapshot-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

Exemple de sortie

```
Region           Public Access State
--------------   ---------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
```

Tools for Windows PowerShell

Pour désactiver le blocage de l'accès public pour les instantanés

Utilisez la commande Disable-EC2SnapshotBlockPublicAccess.

- Pour une région spécifique

```
Disable-EC2SnapshotBlockPublicAccess -Region us-east-1
```

Exemple de sortie

```
Value
-----
unblocked
```

- Pour toutes les régions

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2SnapshotBlockPublicAccess -Region $_)
    }
```

```
} | `
Format-Table -AutoSize
```

Exemple de sortie

```
Region         PublicAccessState
------         -----------------
ap-south-1     unblocked
eu-north-1     unblocked
eu-west-3      unblocked
...
```

Surveillez le blocage de l'accès public aux instantanés Amazon EBS à l'aide de EventBridge

Amazon EBS émet des événements liés au blocage de l'accès public pour les instantanés. Vous pouvez utiliser AWS Lambda Amazon EventBridge pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Les événements suivants sont émis :

- Activation du blocage de l'accès public pour les instantanés en mode bloquer tous les partages

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-all-sharing",
    "message": "Block Public Access was successfully enabled in 'block-all-sharing'
 mode"
  }
}
```

- Activation du blocage de l'accès public pour les instantanés en mode bloquer les nouveaux partages

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-new-sharing",
    "message": "Block Public Access was successfully enabled in 'block-new-sharing'
 mode"
  }
}
```

- Désactivation du blocage de l'accès public pour les instantanés

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Disabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "unblocked",
    "message": "Block Public Access was successfully disabled"
  }
}
```

Amazon EBS local snapshots on Outposts

Les instantanés Amazon EBS sont une point-in-time copie de vos volumes EBS.

Par défaut, les instantanés des volumes EBS sur un Outpost sont stockés dans Amazon S3 dans la région de l'Outpost. Vous pouvez également utiliser des Instantanés locaux Amazon EBS sur Outposts pour stocker des instantanés de volumes sur un Outpost localement dans Amazon S3 sur

l'Outpost lui-même. Cela garantit que les données d'instantané résident sur l'Outpost et dans vos locaux. En outre, vous pouvez utiliser les politiques et les autorisations AWS Identity and Access Management (IAM) pour définir des politiques d'application de la résidence des données afin de garantir que les données instantanées ne quittent pas l'avant-poste. Cela est particulièrement utile si vous résidez dans un pays ou une région qui n'est pas encore desservi par une AWS région et qui impose des exigences en matière de résidence des données.

Cette rubrique fournit des informations sur l'utilisation d'Instantanés locaux Amazon EBS sur Outposts. Pour plus d'informations sur les instantanés Amazon EBS et sur l'utilisation des instantanés dans une AWS région, consultez. Instantanés Amazon EBS

Pour plus d'informations, consultez AWS Outposts la documentation sur la AWS Outposts famille et la famille.

Rubriques

Questions fréquentes (FAQ)

1. Présentation d'instantanés locaux

   Par défaut, les instantanés Amazon EBS des volumes sur un Outpost sont stockés dans Amazon S3 dans la Région de l'Outpost. Si l'Outpost est configuré avec Amazon S3 sur Outposts, vous pouvez choisir de stocker les instantanés localement sur l'Outpost lui-même. Les instantanés sont des sauvegardes incrémentielles, ce qui signifie que seuls les blocs du volume qui ont changé depuis votre instantané le plus récent sont enregistrés. Vous pouvez utiliser ces instantanés pour restaurer un volume sur le même Outpost que l'instantané à tout moment. Pour plus d'informations sur les instantanés Amazon EBS, consultez Instantanés Amazon EBS.

2. Pourquoi utiliser des instantanés locaux ?

   Les instantanés constituent un moyen pratique de sauvegarder vos données. Avec les instantanés locaux, toutes vos données instantanées sont stockées localement sur l'Outpost. Cela signifie qu'il ne quitte pas vos locaux. Cela est particulièrement utile si vous résidez dans un pays

ou une région qui n'est pas encore desservi par une AWS région et qui impose des conditions de résidence.

En outre, l'utilisation d'instantanés locaux peut aider à réduire la bande passante utilisée pour la communication entre la Région et l'Outpost dans les environnements à bande passante limitée.

3. Comment appliquer la résidence des données d'instantané sur Outposts ?

Vous pouvez utiliser des politiques AWS Identity and Access Management (IAM) pour contrôler les autorisations accordées aux principaux (AWS comptes, utilisateurs IAM et rôles IAM) lorsqu'ils travaillent avec des instantanés locaux et pour appliquer la résidence des données. Vous pouvez créer une politique qui empêche les principaux de créer des instantanés à partir de volumes et d'instances Outpost et de stocker les instantanés dans une région. AWS Actuellement, la copie d'instantanés et d'images d'un Outpost vers une Région n'est pas prise en charge. Pour plus d'informations, consultez Contrôle de l'accès avec IAM.

4. Les instantanés locaux à volumes multiples et cohérents en cas d'incidents sont-ils pris en charge ?

Oui, vous pouvez créer des instantanés locaux à volumes multiples et cohérents en cas d'incidents à partir d'instances sur un Outpost.

5. Comment créer des instantanés locaux ?

Vous pouvez créer des instantanés manuellement à l'aide de la AWS Command Line Interface (AWS CLI) ou de la EC2 console Amazon. Pour de plus amples informations, veuillez consulter Utilisation des instantanés locaux. Vous pouvez également automatiser le cycle de vie des instantanés locaux utilisant Amazon Data Lifecycle Manager. Pour plus d'informations, consultez Automatiser des instantanés sur un Outpost.

6. Puis-je créer, utiliser ou supprimer des instantanés locaux si mon Outpost perd la connectivité avec sa Région ?

Non. L'Outpost doit avoir une connectivité avec sa Région car celle-ci fournit les services d'accès, d'autorisation, de journalisation et de surveillance qui sont essentiels pour l'intégrité de vos instantanés. S'il n'y a pas de connectivité, vous ne pouvez pas créer de nouveaux instantanés locaux, créer des volumes ou lancer des instances à partir d'instantanés locaux existants ou supprimer des instantanés locaux.

7. À quelle vitesse la capacité de stockage Amazon S3 est-elle disponible après la suppression des instantanés locaux ?

   La capacité de stockage Amazon S3 est disponible 72 heures après la suppression des instantanés locaux et des volumes qui y font référence.

8. Comment puis-je m'assurer que je ne manque pas de capacité Amazon S3 sur mon Outpost ?

   Nous vous recommandons d'utiliser les CloudWatch alarmes Amazon pour surveiller votre capacité de stockage Amazon S3 et de supprimer les instantanés et les volumes dont vous n'avez plus besoin pour éviter de manquer de capacité de stockage. Si vous utilisez Amazon Data Lifecycle Manager pour automatiser le cycle de vie des instantanés locaux, assurez-vous que vos politiques de rétention d'instantanés ne conservent pas les instantanés plus longtemps que nécessaire.

9. Que se passe-t-il si je manque de capacité Amazon S3 locale sur mes Outposts ?

   Si vous n'avez plus de capacité Amazon S3 locale sur vos Outposts, Amazon Data Lifecycle Manager ne sera pas en mesure de créer des instantanés locaux sur les Outposts. Amazon Data Lifecycle Manager tentera de créer les instantanés locaux sur les Outposts, mais les instantanés passent immédiatement à l'état `error` avant d'être supprimés par Amazon Data Lifecycle Manager. Nous vous recommandons d'utiliser la CloudWatch métrique `SnapshotsCreateFailed` Amazon pour surveiller vos politiques de cycle de vie des instantanés en cas d'échec de création d'instantanés. Pour de plus amples informations, veuillez consulter Surveillez les politiques de Data Lifecycle Manager à l'aide CloudWatch.

10. Puis-je utiliser des instantanés locaux AMIs appuyés par des instantanés locaux avec des instances Spot et un parc Spot ?

    Non, vous ne pouvez pas utiliser de snapshots locaux ou s'appuyer AMIs sur des snapshots locaux pour lancer des instances Spot ou un parc Spot.

11. Puis-je utiliser des instantanés locaux et AMIs sauvegardés par des instantanés locaux avec Amazon EC2 Auto Scaling ?

    Oui, vous pouvez utiliser des instantanés locaux, AMIs appuyés par des instantanés locaux, pour lancer des groupes Auto Scaling dans un sous-réseau situé sur le même Outpost que les instantanés. Le rôle lié au service du groupe Amazon EC2 Auto Scaling doit être autorisé à utiliser la clé KMS utilisée pour chiffrer les instantanés.

    Vous ne pouvez pas utiliser des instantanés locaux ou AMIs sauvegardés par des instantanés locaux pour lancer des groupes Auto Scaling dans une AWS région.

Prérequis

Pour stocker des instantanés sur un Outpost, vous devez disposer d'un Outpost qui est provisionné avec Amazon S3 sur Outposts. Pour plus d'informations sur Amazon S3 on Outposts, consultez Amazon S3 on Outposts dans le guide de l'utilisateur d'Amazon S3 on Outposts.

Considérations

Gardez ce qui suit à l'esprit lorsque vous travaillez avec des instantanés locaux.

- Les Outposts doivent être connectés à leur AWS région pour utiliser les instantanés locaux.
- Les métadonnées des instantanés sont stockées dans la AWS région associée à l'avant-poste. Cela n'inclut pas les données d'instantanés.
- Les instantanés stockés sur Outposts sont chiffrés par défaut. Les instantanés non chiffrés ne sont pas pris en charge. Les instantanés créés sur un Outpost et les instantanés copiés dans un Outpost sont chiffrés à l'aide de la clé KMS par défaut pour la Région ou d'une autre clé KMS que vous spécifiez au moment de la demande.
- Lorsque vous créez un volume sur un Outpost à partir d'un instantané local, vous ne pouvez pas le rechiffrer à l'aide d'une autre clé KMS. Les volumes créés à partir d'instantanés locaux doivent être chiffrés à l'aide de la même clé KMS que l'instantané source.
- Après la suppression d'instantanés locaux d'un Outpost, la capacité de stockage Amazon S3 utilisée par les instantanés supprimés devient disponible dans les 72 heures. Pour plus d'informations, consultez Supprimer les instantanés locaux.
- Vous ne pouvez pas exporter des instantanés locaux depuis un Outpost.
- Vous ne pouvez pas activer la restauration rapide des instantanés pour les instantanés locaux.
- Les instantanés locaux ne APIs sont pas compatibles avec les instantanés EBS.
- Vous ne pouvez pas copier des instantanés locaux ou AMIs d'un avant-poste vers une AWS région, d'un avant-poste à un autre ou au sein d'un avant-poste. Toutefois, vous pouvez copier des instantanés d'une Région AWS vers un Outpost. Pour de plus amples informations, veuillez consulter Copier des instantanés d'une AWS région vers un avant-poste.
- Lorsque vous copiez un instantané d'une AWS région vers un avant-poste, les données sont transférées via le lien de service. La copie simultanée de plusieurs instantanés peut avoir un impact sur d'autres services exécutés sur l'Outpost.
- Tu ne peux pas partager les instantanés locaux.

- Vous devez utiliser des politiques IAM pour vous assurer que vos exigences en matière de résidence des données sont respectées. Pour plus d'informations, consultez Contrôle de l'accès avec IAM.
- Les Instantanés locaux sont des sauvegardes incrémentielles. Seuls les blocs du volume qui ont changé depuis votre instantané le plus récent sont enregistrés. Chaque instantané local contient toutes les informations nécessaires à la restauration de vos données (à partir du moment où l'instantané a été pris) sur un nouveau volume EBS. Pour de plus amples informations, veuillez consulter Comment fonctionnent les instantanés Amazon EBS.
- Vous ne pouvez pas utiliser les politiques IAM pour imposer la résidence des données CopySnapshotet les CopyImageactions.

Contrôle de l'accès avec IAM

Vous pouvez utiliser des politiques AWS Identity and Access Management (IAM) pour contrôler les autorisations accordées aux principaux (AWS comptes, utilisateurs IAM et rôles IAM) lorsqu'ils travaillent avec des instantanés locaux. Voici des exemples de politiques que vous pouvez utiliser pour accorder ou refuser l'autorisation d'effectuer des actions spécifiques avec les instantanés locaux.

> **Important**
>
> La copie d'instantanés et d'images d'un Outpost vers une Région n'est actuellement pas prise en charge. Par conséquent, vous ne pouvez actuellement pas utiliser les politiques IAM pour appliquer la résidence des données CopySnapshotet les CopyImageactions.

Rubriques

- Appliquer la résidence des données pour les instantanés
- Empêcher les principaux de supprimer les instantanés locaux

Appliquer la résidence des données pour les instantanés

L'exemple de politique suivant empêche tous les principaux de créer des instantanés à partir de volumes et d'instances sur Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef` et de stocker les données des instantanés dans une région. AWS Les

principaux peuvent toujours créer des instantanés locaux. Cette politique garantit que tous les instantanés restent sur l'Outpost.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
                },
                "Null": {
                    "ec2:OutpostArn": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Empêcher les principaux de supprimer les instantanés locaux

L'exemple de stratégie suivant empêche tous les principaux de supprimer des instantanés locaux stockés sur Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

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

```
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilisation des instantanés locaux

Les sections suivantes expliquent comment utiliser les instantanés locaux.

Rubriques

- Règles de stockage des instantanés
- Créer des instantanés locaux à partir de volumes sur un Outpost
- Création AMIs à partir d'instantanés locaux
- Copier des instantanés d'une AWS région vers un avant-poste
- Copier AMIs depuis une AWS région vers un avant-poste
- Créer des volumes à partir d'instantanés locaux
- Lancer des instances à AMIs partir de snapshots locaux
- Supprimer les instantanés locaux
- Automatiser des instantanés sur un Outpost

Règles de stockage des instantanés

Les règles suivantes s'appliquent au stockage des instantanés :

- Si l'instantané le plus récent d'un volume est stocké sur un Outpost, tous les instantanés successifs doivent être stockés sur le même Outpost.
- Si l'instantané le plus récent d'un volume est stocké dans une AWS région, tous les instantanés successifs doivent être stockés dans la même région. Pour commencer à créer des instantanés locaux à partir de ce volume, procédez comme suit :

  1. Créez un instantané du volume dans la AWS région.
  2. Copiez l'instantané vers l'avant-poste depuis la AWS région.
  3. Créez un volume à partir de l'instantané local.
  4. Attachez le volume à une instance sur l'Outpost.

  Pour le nouveau volume sur l'Outpost, l'instantané suivant peut être stocké sur l'Outpost ou dans la Région AWS . Tous les instantanés successifs doivent alors être stockés dans le même emplacement.
- Les instantanés locaux, y compris les instantanés créés sur un avant-poste et les instantanés copiés vers un avant-poste depuis une AWS région, ne peuvent être utilisés que pour créer des volumes sur le même avant-poste.
- Si vous créez un volume sur un Outpost à partir d'un instantané dans une Région, tous les instantanés successifs de ce nouveau volume doivent être dans la même Région.
- Si vous créez un volume sur un Outpost à partir d'un instantané local, tous les instantanés successifs de ce nouveau volume doivent être sur le même Outpost.

Créer des instantanés locaux à partir de volumes sur un Outpost

Vous pouvez créer des instantanés locaux à partir de volumes sur votre Outpost. Vous pouvez choisir de stocker les instantanés sur le même Outpost que le volume source ou dans la Région de l'Outpost.

Instantanés locaux peut être utilisé pour créer des volumes sur le même Outpost uniquement.

Pour plus d'informations, consultez Créer des instantanés Amazon EBS.

Création AMIs à partir d'instantanés locaux

Vous pouvez créer des Amazon Machine Images (AMIs) en combinant des instantanés locaux et des instantanés stockés dans la région de l'avant-poste. Par exemple, si vous avez un Outpost en `us-east-1`, vous pouvez créer une AMI avec des volumes de données qui sont sauvegardés par des instantanés locaux sur cet Outpost, et un volume racine qui est sauvegardé par un instantané dans la Région `us-east-1`.

> **Note**
>
> - Vous ne pouvez pas créer AMIs cela en incluant des instantanés de sauvegarde stockés sur plusieurs Outposts.
> - Vous ne pouvez actuellement pas créer AMIs directement à partir d'instances sur un Outposts à l'aide de l'CreateImageAPI ou de EC2 la console Amazon pour les Outposts activées avec Amazon S3 on Outposts.
> - AMIs qui sont soutenus par des instantanés locaux ne peuvent être utilisés que pour lancer des instances sur le même Outpost.

Pour créer une AMI sur un Outpost à partir d'instantanés dans une Région

1. Copiez les instantanés de la Région vers l'Outpost. Pour de plus amples informations, veuillez consulter Copier des instantanés d'une AWS région vers un avant-poste.
2. Utilisez la EC2 console Amazon ou la commande register-image pour créer l'AMI à l'aide des copies instantanées de l'Outpost. Pour plus d'informations, consultez Création d'une AMI à partir d'un instantané.

Pour créer une AMI sur un Outpost à partir d'une instance d'un Outpost

1. Créez des instantanés à partir de l'instance sur l'Outpost et stockez les instantanés sur l'Outpost. Pour de plus amples informations, veuillez consulter Créer des instantanés Amazon EBS.
2. Utilisez la EC2 console Amazon ou la commande register-image pour créer l'AMI à l'aide des instantanés locaux. Pour plus d'informations, consultez Création d'une AMI à partir d'un instantané.

Pour créer une AMI dans une Région à partir d'une instance d'un Outpost

1. Créez des instantanés à partir de l'instance sur l'Outpost et stockez les instantanés dans la Région. Pour plus d'informations, consultez Créer des instantanés locaux à partir de volumes sur un Outpost ou Créer des instantanés Amazon EBS.
2. Utilisez la EC2 console Amazon ou la commande register-image pour créer l'AMI à l'aide des copies instantanées de la région. Pour plus d'informations, consultez Création d'une AMI à partir d'un instantané.

Copier des instantanés d'une AWS région vers un avant-poste

Vous pouvez copier des instantanés d'une AWS région vers un avant-poste. Vous ne pouvez le faire que si les instantanés se trouvent dans la Région de l'Outpost. Si les instantanés se trouvent dans une autre Région, vous devez d'abord copier l'instantané dans la Région de l'Outpost, puis le copier de cette Région vers l'Outpost.

> **Note**
>
> Vous ne pouvez pas copier les instantanés locaux d'un Outpost vers une Région, d'un Outpost vers un autre ou au sein du même Outpost.

Pour de plus amples informations, veuillez consulter Copier un instantané Amazon EBS.

Copier AMIs depuis une AWS région vers un avant-poste

Vous pouvez effectuer une copie AMIs depuis une AWS région vers un avant-poste. Lorsque vous copiez une AMI d'une Région vers un Outpost, tous les instantanés associés à l'AMI sont copiés de la Région vers l'Outpost.

Vous pouvez copier une AMI d'une Région vers un Outpost uniquement si les instantanés associés à l'AMI se trouvent dans la Région de l'Outpost. Si les instantanés se trouvent dans une autre Région, vous devez d'abord copier l'AMI dans la Région de l'Outpost, puis la copier de cette Région vers l'Outpost.

> **Note**
>
> Vous ne pouvez pas copier une AMI d'un Outpost vers une Région, d'un Outpost vers un autre ou au sein d'un Outpost.

Vous pouvez effectuer une copie AMIs d'une région vers un avant-poste à l'aide de la commande copy-image uniquement AWS CLI .

Créer des volumes à partir d'instantanés locaux

Vous pouvez créer des volumes sur des Outposts à partir d'instantanés locaux. Les volumes doivent être créés sur le même Outpost que les instantanés source. Vous ne pouvez pas utiliser des instantanés locaux pour créer des volumes dans la Région de l'Outpost.

Lorsque vous créez un volume à partir d'un instantané local, vous ne pouvez pas rechiffrer le volume à l'aide d'une autre clé KMS. Les volumes créés à partir d'instantanés locaux doivent être chiffrés à l'aide de la même clé KMS que l'instantané source.

Pour de plus amples informations, veuillez consulter Créez un volume Amazon EBS..

Lancer des instances à AMIs partir de snapshots locaux

Vous pouvez lancer des instances à partir AMIs desquelles des instantanés locaux sont sauvegardés. Vous devez lancer des instances sur le même Outpost que l'AMI source. Pour plus d'informations, consultez la section Lancer une instance sur votre Outpost du Guide de l'utilisateur AWS Outposts .

Supprimer les instantanés locaux

Vous pouvez supprimer les instantanés locaux d'un Outpost. Après avoir supprimé un instantané d'un Outpost, la capacité de stockage Amazon S3 utilisée par l'instantané supprimé devient disponible dans les 72 heures suivant la suppression de l'instantané et des volumes qui font référence à cet instantané.

La capacité de stockage Amazon S3 n'étant pas disponible immédiatement, nous vous recommandons d'utiliser les CloudWatch alarmes Amazon pour surveiller votre capacité de stockage Amazon S3. Supprimez les instantanés et les volumes dont vous n'avez plus besoin pour éviter de manquer de capacité de stockage.

Pour plus d'informations sur la suppression des instantanés, consultez Suppression d'un instantané.

Automatiser des instantanés sur un Outpost

Vous pouvez créer des politiques de cycle de vie d'instantanés Amazon Data Lifecycle Manager qui créent, copient, conservent et suppriment automatiquement des instantanés de vos volumes et instances sur un Outpost. Vous pouvez choisir de stocker les instantanés dans une Région ou de les stocker localement sur un Outpost. En outre, vous pouvez automatiquement copier les instantanés créés et stockés dans une AWS région vers un avant-poste.

Le tableau suivant donne un aperçu des fonctionnalités prises en charge.

Emplacement des ressources	Destination des instantanés	Copie entre régions		Restauration d'instantané rapide	Partage entre comptes
		Vers la région	Vers l'Outpost		
Région	Région	✓	✓	✓	✓
Outpost	Région	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

Considérations

- Seules les politiques de cycle de vie Amazon EBS sont actuellement prises en charge. Les politiques AMI basées sur EBS et les politiques d'événement de partage inter-comptes ne sont pas prises en charge.
- Si une politique gère les instantanés pour les volumes ou les instances d'une Région, les instantanés sont créés dans la même Région que la ressource source.
- Si une politique gère les instantanés pour les volumes ou les instances d'un Outpost, il est possible de créer des instantanés sur l'Outpost source ou dans la Région correspondant à cet Outpost.
- Une seule politique ne peut pas gérer les instantanés d'une Région et les instantanés d'un Outpost. Si vous devez automatiser les instantanés dans une Région et sur un Outpost, vous devez créer des politiques distinctes.
- La restauration d'instantané rapide n'est pas prise en charge pour les instantanés créés sur un Outpost ou pour les instantanés copiés dans un Outpost.
- Le partage entre comptes n'est pas pris en charge pour les instantanés créés sur un Outpost.

Pour plus d'informations sur la création d'un cycle de vie des instantanés qui gère les instantanés locaux, consultez Automatisation des cycles de vie des instantanés.

Instantanés locaux dans des zones locales dédiées

Les instantanés Amazon EBS sont une point-in-time copie de vos volumes EBS.

Les instantanés de volumes EBS dans une zone locale dédiée peuvent être stockés dans Amazon S3 dans la même zone locale dédiée ou dans la région parent de cette zone locale dédiée. Le stockage des instantanés dans une zone locale dédiée peut vous aider à répondre aux besoins de résidence des données en garantissant que les données instantanées sont traitées et stockées dans un pays, un État ou une municipalité spécifique. Vous pouvez également configurer des politiques d'application de la résidence des données à l'aide d'IAM afin de garantir que les données instantanées ne quittent pas la zone locale dédiée.

AWS Les Zones Locales dédiées sont un type d' AWS infrastructure entièrement géré par vous ou votre communauté AWS, conçu pour un usage exclusif par vous ou votre communauté, et placé dans un emplacement ou un centre de données que vous avez spécifié pour vous aider à vous conformer aux exigences réglementaires. Les zones locales dédiées sont un type d'offre de zones AWS locales. Pour plus d'informations, consultez Zones locales dédiées AWS.

Les instantanés locaux ne sont actuellement pas pris en charge dans les autres zones AWS locales.

Rubriques

- Questions fréquentes (FAQ)
- Considérations
- Contrôle de l'accès avec IAM

Questions fréquentes (FAQ)

1. Que sont les instantanés locaux dans des zones locales dédiées ?

   Les instantanés locaux dans les zones locales dédiées sont des instantanés stockés dans Amazon S3 dans une zone locale dédiée. Comme les instantanés dans AWS les régions, les instantanés locaux dans les zones locales dédiées sont incrémentiels, ce qui signifie que seuls les blocs du volume qui ont changé après votre dernier instantané sont enregistrés. Vous pouvez utiliser ces instantanés pour restaurer un volume Amazon EBS dans la même zone locale dédiée à tout moment.

2. Pourquoi utiliser des instantanés locaux ?

Utilisez des instantanés locaux dans des zones locales dédiées pour répondre aux exigences de résidence ou d'isolation des données en vous assurant que vos données instantanées résident dans un emplacement géographique spécifique, tel qu'un pays, un État ou une municipalité.

3. Comment puis-je imposer la résidence des données instantanées dans les Zones Locales Dédiées ?

Vous pouvez utiliser des politiques AWS Identity and Access Management (IAM) pour contrôler les autorisations accordées aux principaux (AWS comptes, utilisateurs IAM et rôles IAM) lorsqu'ils travaillent avec des instantanés locaux dans des zones locales dédiées et pour appliquer la résidence des données. Par exemple, vous pouvez créer une politique qui empêche les utilisateurs de créer des instantanés à partir de volumes situés dans des Zones Locales dédiées et de stocker ces instantanés dans une AWS région. Pour de plus amples informations, veuillez consulter Contrôle de l'accès avec IAM.

4. Les instantanés locaux à volumes multiples et cohérents en cas d'incidents sont-ils pris en charge ?

Oui, vous pouvez créer des instantanés locaux multivolumes résistants aux pannes dans des zones locales dédiées à partir d'instances situées dans une zone locale dédiée.

5. Comment créer des instantanés locaux dans des zones locales dédiées ?

Vous pouvez créer des instantanés locaux dans des zones locales dédiées manuellement à l'aide de la EC2 console Amazon AWS CLI ou de celle-ci. Pour de plus amples informations, veuillez consulter Création d'un instantané Amazon EBS d'un volume EBS. Vous pouvez également automatiser le cycle de vie des instantanés locaux dans des zones locales dédiées à l'aide d'Amazon Data Lifecycle Manager. Pour de plus amples informations, veuillez consulter Création d'une politique personnalisée Amazon Data Lifecycle Manager pour les instantanés EBS.

6. Puis-je copier des instantanés locaux dans des zones locales dédiées ?

Non, il est actuellement impossible de copier des instantanés d'une région vers une zone locale dédiée, d'une zone locale dédiée vers une région ou d'une zone locale dédiée vers une autre.

7. Comment puis-je restaurer des données à partir de snapshots locaux dans des zones locales dédiées ?

Vous pouvez utiliser des instantanés locaux dans des zones locales dédiées pour créer des volumes Amazon EBS uniquement dans la même zone locale dédiée.

8. Comment les instantanés locaux situés dans des zones locales dédiées sont-ils chiffrés ?

   Les instantanés locaux situés dans des zones locales dédiées sont chiffrés par défaut. Les instantanés locaux non chiffrés dans les zones locales dédiées ne sont pas pris en charge. Les instantanés locaux situés dans des zones locales dédiées sont chiffrés à l'aide de la même clé KMS que le volume Amazon EBS source.

9. Puis-je créer des images basées sur EBS à l' AMIs aide d'instantanés locaux dans des zones locales dédiées ?

   Non, vous ne pouvez actuellement pas créer de snapshots locaux basés sur EBS AMIs dans des zones locales dédiées.

10. Puis-je partager des instantanés locaux dans des zones locales dédiées ?

    Oui, vous pouvez partager des instantanés locaux dans des zones locales dédiées avec d'autres AWS comptes qui ont activé l'utilisation de la zone locale dédiée dans leur compte.

Considérations

Tenez compte des points suivants lorsque vous travaillez avec des instantanés locaux dans des zones locales dédiées.

- Les instantanés locaux ne sont pris en charge que dans les zones locales AWS dédiées. Ils ne sont pas pris en charge dans les autres Zones Locales.
- Les fonctionnalités suivantes ne peuvent pas être utilisées avec des instantanés locaux dans des zones locales dédiées :
  - Actions d'importation/exportation de machines virtuelles
  - Restauration d'instantané rapide
  - EBS direct APIs
  - Corbeille
  - Archive d'instantanés
  - Verrou instantané
- Vous devez utiliser les politiques IAM pour faire respecter vos exigences en matière de résidence des données. Pour de plus amples informations, veuillez consulter Contrôle de l'accès avec IAM.

Contrôle de l'accès avec IAM

Vous pouvez utiliser des politiques AWS Identity and Access Management (IAM) pour contrôler les autorisations accordées aux principaux (AWS comptes, utilisateurs IAM et rôles IAM) lorsqu'ils travaillent avec des instantanés locaux dans des zones locales dédiées. Voici des exemples de politiques que vous pouvez utiliser pour accorder ou refuser l'autorisation d'effectuer des actions spécifiques avec des instantanés locaux dans des zones locales dédiées.

Rubriques

Appliquer la résidence des données pour les instantanés locaux dans des zones locales dédiées

L'exemple de politique suivant limite les utilisateurs à créer uniquement des instantanés locaux dans des zones locales dédiées à partir de volumes et d'instances situés dans une zone locale dédiée. Il empêche les utilisateurs de créer des instantanés dans une région à partir de volumes et d'instances situés dans une zone locale dédiée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:region::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceAvailabilityZone": "dedicated_local_zone"
                },
                "StringEquals": {
                    "ec2:Location": "local"
                }
            }
```

```
        }
    ]
}
```

Empêcher le partage d'instantanés locaux dans des zones locales dédiées

L'exemple de politique suivant empêche tous les utilisateurs de partager des instantanés locaux dans des zones locales dédiées.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:region::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:AvailabilityZone": "dedicated_local_zone"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "*"
        }
    ]
}
```

Empêcher les principaux de supprimer des instantanés locaux dans des zones locales dédiées

L'exemple de politique suivant empêche tous les utilisateurs de supprimer des instantanés locaux dans des zones locales dédiées.

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

```
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:region::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:AvailabilityZone": "dedicated_local_zone"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

EBSChiffrement Amazon

Utilisez EBS le chiffrement Amazon comme solution de chiffrement simple pour vos EBS ressources Amazon associées à vos instances AmazonEC2. Avec Amazon EBS Encryption, vous n'êtes pas obligé de créer, de maintenir et de sécuriser votre propre infrastructure de gestion des clés. EBSLe chiffrement Amazon est utilisé AWS KMS keys lors de la création de volumes chiffrés et de snapshots.

Les opérations de chiffrement ont lieu sur les serveurs EC2 hébergeant les instances, garantissant ainsi la sécurité data-in-transit entre une instance data-at-rest et le EBS stockage qui lui est rattaché.

Vous pouvez attacher simultanément des volumes chiffrés et des volumes non chiffrés à une instance. Tous les types d'EC2instances Amazon prennent en charge EBS le chiffrement Amazon.

Table des matières

Comment fonctionne EBS le chiffrement Amazon

Vous pouvez chiffrer à la fois le volume de démarrage et le volume de données d'une EC2 instance.

Lorsque vous créez un EBS volume chiffré et que vous l'attachez à un type d'instance pris en charge, les types de données suivants sont chiffrés :

- Données au repos à l'intérieur du volume
- Toutes les données circulant entre le volume et l'instance
- Tous les instantanés créés à partir du volume
- Tous les volumes créés à partir de ces instantanés

Amazon EBS chiffre votre volume à l'aide d'une clé de données en utilisant le chiffrement de données standard AES -256. La clé de données est générée AWS KMS puis cryptée AWS KMS avec une AWS KMS clé avant d'être stockée avec les informations de votre volume. Amazon crée EBS automatiquement un identifiant unique Clé gérée par AWS dans chaque région dans laquelle vous créez des EBS ressources Amazon. L'alias de la KMS clé est `aws/ebs`. Par défaut, Amazon EBS utilise cette KMS clé pour le chiffrement. Vous pouvez également utiliser une clé de chiffrement symétrique gérée par le client que vous créez. L'utilisation de votre propre KMS clé vous donne plus de flexibilité, notamment la possibilité de créer, de faire pivoter et de désactiver KMS des touches.

Amazon EC2 utilise AWS KMS pour chiffrer et déchiffrer vos EBS volumes de manière légèrement différente selon que l'instantané à partir duquel vous créez un volume chiffré est chiffré ou non chiffré.

Comment fonctionne EBS le chiffrement lorsque le cliché est chiffré

Lorsque vous créez un volume chiffré à partir d'un instantané chiffré que vous possédez, Amazon EC2 travaille avec lui AWS KMS pour chiffrer et déchiffrer vos EBS volumes comme suit :

1. Amazon EC2 envoie une GenerateDataKeyWithoutPlaintextdemande à AWS KMS, en spécifiant la KMS clé que vous avez choisie pour le chiffrement du volume.
2. Si le volume est chiffré à l'aide de la même KMS clé que le cliché, AWS KMS utilise la même clé de données que le cliché et le chiffre sous cette même KMS clé. Si le volume est chiffré à l'aide d'une autre KMS clé, AWS KMS génère une nouvelle clé de données et le chiffre sous la KMS clé que vous avez spécifiée. La clé de données cryptée est envoyée à Amazon EBS pour être stockée avec les métadonnées du volume.
3. Lorsque vous attachez le volume chiffré à une instance, Amazon EC2 envoie une CreateGrantdemande AWS KMS afin de déchiffrer la clé de données.
4. AWS KMS déchiffre la clé de données chiffrée et envoie la clé de données déchiffrée à Amazon. EC2
5. Amazon EC2 utilise la clé de données en texte brut du matériel Nitro pour chiffrer les E/S du disque vers le volume. La clé de données en texte brut est conservée en mémoire tant que le volume est attaché à l'instance.

Comment fonctionne EBS le chiffrement lorsque l'instantané n'est pas chiffré

Lorsque vous créez un volume chiffré à partir d'un instantané non chiffré, Amazon EC2 travaille avec AWS KMS lui pour chiffrer et déchiffrer vos EBS volumes comme suit :

1. Amazon EC2 envoie une CreateGrantdemande à AWS KMS, afin de chiffrer le volume créé à partir de l'instantané.
2. Amazon EC2 envoie une GenerateDataKeyWithoutPlaintextdemande à AWS KMS, en spécifiant la KMS clé que vous avez choisie pour le chiffrement du volume.
3. AWS KMS génère une nouvelle clé de données, la chiffre sous la KMS clé que vous avez choisie pour le chiffrement du volume et envoie la clé de données chiffrée EBS à Amazon pour qu'elle soit stockée avec les métadonnées du volume.
4. Amazon EC2 envoie une demande de déchiffrement AWS KMS pour déchiffrer la clé de données chiffrée, qu'elle utilise ensuite pour chiffrer les données du volume.
5. Lorsque vous attachez le volume chiffré à une instance, Amazon EC2 envoie une CreateGrantdemande à AWS KMS, afin qu'il puisse déchiffrer la clé de données.
6. Lorsque vous attachez le volume chiffré à une instance, Amazon EC2 envoie une demande de déchiffrement à AWS KMS, en spécifiant la clé de données chiffrée.
7. AWS KMS déchiffre la clé de données chiffrée et envoie la clé de données déchiffrée à Amazon. EC2
8. Amazon EC2 utilise la clé de données en texte brut du matériel Nitro pour chiffrer les E/S du disque vers le volume. La clé de données en texte brut est conservée en mémoire tant que le volume est attaché à l'instance.

Pour plus d'informations, consultez Comment Amazon Elastic Block Store (AmazonEBS) utilise AWS KMS et le deuxième EC2 exemple d'Amazon dans le guide du AWS Key Management Service développeur.

Comment les clés inutilisables affectent KMS les clés de données

Lorsqu'une KMS clé devient inutilisable, l'effet est quasi immédiat (sous réserve d'une éventuelle cohérence). L'état de la KMS clé change pour refléter sa nouvelle condition, et toutes les demandes d'utilisation de la KMS clé dans des opérations cryptographiques échouent.

Lorsque vous effectuez une action qui rend la KMS clé inutilisable, il n'y a aucun effet immédiat sur l'EC2instance ou les EBS volumes attachés. Amazon EC2 utilise la clé de données, et non la KMS clé, pour chiffrer toutes les E/S du disque lorsque le volume est attaché à l'instance.

Toutefois, lorsque le EBS volume chiffré est détaché de l'EC2instance, Amazon EBS supprime la clé de données du matériel Nitro. La prochaine fois que le EBS volume chiffré est attaché à une EC2 instance, la pièce jointe échoue, car Amazon EBS ne peut pas utiliser la KMS clé pour déchiffrer la

clé de données chiffrée du volume. Pour réutiliser le EBS volume, vous devez rendre la KMS clé réutilisable.

> **Tip**
>
> Si vous ne souhaitez plus accéder aux données stockées dans un EBS volume chiffré à l'aide d'une clé de données générée à partir d'une KMS clé que vous souhaitez rendre inutilisable, nous vous recommandons de détacher le EBS volume de l'EC2instance avant de rendre la KMS clé inutilisable.

Pour plus d'informations, consultez la section Comment les clés inutilisables affectent KMS les clés de données dans le Guide du AWS Key Management Service développeur.

Exigences relatives au EBS chiffrement Amazon

Avant de commencer, vérifiez que les conditions requises suivantes sont respectées :

Prérequis

- Types de volume pris en charge
- Types d'instance pris en charge
- Autorisations pour les utilisateurs
- Autorisations pour les instances

Types de volume pris en charge

Le chiffrement est pris en charge par tous les types de EBS volumes. Vous pouvez vous attendre aux mêmes IOPS performances sur les volumes chiffrés que sur les volumes non chiffrés, avec un effet minimal sur la latence. Vous pouvez accéder à des volumes chiffrés de la même façon qu'à des volumes non chiffrés. Le chiffrement et le déchiffrement sont gérés de façon transparente et ne nécessitent aucune action supplémentaire de votre part ou de vos applications.

Types d'instance pris en charge

EBSLe chiffrement Amazon est disponible sur tous les types d'instances de génération actuelle et précédente.

Autorisations pour les utilisateurs

Lorsque vous utilisez une KMS clé pour le EBS chiffrement, la politique des KMS clés permet à tout utilisateur ayant accès aux AWS KMS actions requises d'utiliser cette KMS clé pour chiffrer ou déchiffrer EBS des ressources. Vous devez autoriser les utilisateurs à effectuer les actions suivantes afin d'utiliser EBS le chiffrement :

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:ReEncrypt`

> **Tip**
>
> Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour permettre à l'utilisateur de créer des autorisations sur la KMS clé uniquement lorsque l'autorisation est créée en son nom par un AWS service, comme indiqué dans l'exemple suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
```

```
    ]
}
```

Pour plus d'informations, consultez Autoriser l'accès au AWS compte et activer IAM les politiques dans la section Politique de clé par défaut du Guide du AWS Key Management Service développeur.

Autorisations pour les instances

Lorsqu'une instance tente d'interagir avec un volume chiffréAMI, un instantané ou un volume, une KMS clé est octroyée au rôle d'identité uniquement de l'instance. Le rôle d'identité uniquement est un IAM rôle utilisé par l'instance pour interagir avec des volumes chiffrés AMIs ou des instantanés en votre nom.

Les rôles réservés à l'identité n'ont pas besoin d'être créés ou supprimés manuellement, et aucune stratégie ne leur est associée. De plus, vous ne pouvez pas accéder aux informations d'identification du rôle réservé à l'identité.

> **Note**
>
> Les rôles d'identité uniquement ne sont pas utilisés par les applications de votre instance pour accéder à d'autres ressources AWS KMS chiffrées, telles que les objets Amazon S3 ou les tables Dynamo DB. Ces opérations sont effectuées à l'aide des informations d'identification d'un rôle d'EC2instance Amazon ou d'autres AWS informations d'identification que vous avez configurées sur votre instance.

Les rôles dotés uniquement d'une identité sont soumis aux politiques de contrôle des services (SCPs) et aux politiques KMSclés. Si une KMS clé SCP ou refuse au rôle d'identité uniquement l'accès à une KMS clé, vous risquez de ne pas lancer d'EC2instances avec des volumes chiffrés, d'utiliser des données chiffrées ou des AMIs instantanés.

Si vous créez une politique clé SCP ou qui refuse l'accès en fonction de l'emplacement du réseau à l'aide des clés de condition `aws:SourceIp` `aws:VpcSourceIpaws:SourceVpc`,, ou `aws:SourceVpce` AWS globales, vous devez vous assurer que ces déclarations de politique ne s'appliquent pas aux rôles réservés aux instances. Pour obtenir des exemples de stratégies, consultez la section Exemples de stratégies relatives aux périmètres de données (français non garanti).

Le rôle à identité uniquement ARNs utilise le format suivant :

```
arn:aws-partition:iam::account_id:role/aws:ec2-infrastructure/instance_id
```

Lorsqu'une attribution de clé est attribuée à une instance, elle est attribuée à la session à rôle assumé spécifique à cette instance. Le directeur du bénéficiaire ARN utilise le format suivant :

```
arn:aws-partition:sts::account_id:assumed-role/aws:ec2-infrastructure/instance_id
```

Activer le EBS chiffrement Amazon par défaut

Vous pouvez configurer votre AWS compte pour appliquer le chiffrement des nouveaux EBS volumes et des copies instantanées que vous créez. Par exemple, Amazon EBS chiffre les EBS volumes créés lorsque vous lancez une instance et les instantanés que vous copiez à partir d'un instantané non chiffré. Pour des exemples de transition de ressources non chiffrées à des EBS ressources chiffrées, consultez. Chiffrer les ressources non chiffrées

Le chiffrement par défaut n'a aucun effet sur les EBS volumes ou les instantanés existants.

Considérations

- Le chiffrement par défaut est un paramètre spécifique à une région. Si vous l'activez pour une région, vous ne pouvez pas le désactiver pour certains volumes ou instantanés spécifiques dans cette région.
- EBSLe chiffrement Amazon est pris en charge par défaut sur tous les types d'instances de génération actuelle et précédente.
- Si vous copiez un instantané et que vous le chiffrez sur une nouvelle KMS clé, une copie complète (non incrémentielle) est créée. Cela entraîne des coûts de stockage supplémentaires.
- Lorsque vous migrez des serveurs à l'aide de AWS Server Migration Service (SMS), n'activez pas le chiffrement par défaut. Si le chiffrement par défaut est déjà activé et que vous rencontrez des échecs de réplication delta, désactivez cette fonction. Activez plutôt AMI le chiffrement lorsque vous créez la tâche de réplication.

Amazon EC2 console

Pour activer le chiffrement par défaut pour une région

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans la barre de navigation, sélectionnez la région.

3. Dans le volet de navigation, sélectionnez EC2Tableau de bord.
4. En haut à droite de la page, choisissez Attributs du compte, Protection des données et sécurité.
5. Dans la section EBSde chiffrement, choisissez Gérer.
6. Sélectionnez Activer. Vous conservez l' Clé gérée par AWS alias `aws/ebs` créé en votre nom comme clé de chiffrement par défaut, ou vous choisissez une clé de chiffrement symétrique gérée par le client.
7. Choisissez Mettre à jour EBS le chiffrement.

AWS CLI

Pour afficher le paramètre de chiffrement par défaut

- Pour une région spécifique

```
$ aws ec2 get-ebs-encryption-by-default --region region
```

- Pour toutes les régions de votre compte

```
$ echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 get-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

Pour activer le chiffrement par défaut

- Pour une région spécifique

```
$ aws ec2 enable-ebs-encryption-by-default --region region
```

- Pour toutes les régions de votre compte

```
$ echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 enable-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

Pour désactiver le chiffrement par défaut

- Pour une région spécifique

```
$ aws ec2 disable-ebs-encryption-by-default --region region
```

- Pour toutes les régions de votre compte

```
$ echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 disable-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

PowerShell

Pour afficher le paramètre de chiffrement par défaut

- Pour une région spécifique

```
PS C:\> Get-EC2EbsEncryptionByDefault -Region region
```

- Pour toutes les régions de votre compte

```
PS C:\> (Get-EC2Region).RegionName |`
    ForEach-Object {
    [PSCustomObject]@{
        Region                     = $_;
        EC2EbsEncryptionByDefault = Get-EC2EbsEncryptionByDefault -Region $_;
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } |`
    Format-Table -AutoSize
```

Pour activer le chiffrement par défaut

- Pour une région spécifique

```
PS C:\> Enable-EC2EbsEncryptionByDefault -Region region
```

- Pour toutes les régions de votre compte

```
PS C:\> (Get-EC2Region).RegionName |`
    ForEach-Object {
    [PSCustomObject]@{
        Region                     = $_;
        EC2EbsEncryptionByDefault = Enable-EC2EbsEncryptionByDefault -Region $_;
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } | `
    Format-Table -AutoSize
```

Pour désactiver le chiffrement par défaut

- Pour une région spécifique

```
PS C:\> Disable-EC2EbsEncryptionByDefault -Region region
```

- Pour toutes les régions de votre compte

```
PS C:\> (Get-EC2Region).RegionName |`
    ForEach-Object {
    [PSCustomObject]@{
        Region                     = $_;
```

```
        EC2EbsEncryptionByDefault = Disable-EC2EbsEncryptionByDefault -Region $_;
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } | `
    Format-Table -AutoSize
```

Vous ne pouvez pas modifier la KMS clé associée à un instantané ou à un volume chiffré existant. Toutefois, vous pouvez associer une KMS clé différente lors d'une opération de copie instantanée afin que l'instantané copié obtenu soit chiffré par la nouvelle KMS clé.

Chiffrer les ressources EBS

Vous cryptez les EBS volumes en activant le chiffrement, soit en utilisant le chiffrement par défaut, soit en activant le chiffrement lorsque vous créez un volume que vous souhaitez chiffrer.

Lorsque vous chiffrez un volume, vous pouvez spécifier la KMS clé de chiffrement symétrique à utiliser pour chiffrer le volume. Si vous ne spécifiez pas de KMS clé, la KMS clé utilisée pour le chiffrement dépend de l'état de chiffrement de l'instantané source et de son propriétaire. Pour plus d'informations, consultez le tableau des résultats de chiffrement.

> **Note**
>
> Si vous utilisez le API ou AWS CLI pour spécifier une KMS clé, sachez que la clé est AWS authentifiée de KMS manière asynchrone. Si vous spécifiez un identifiant de KMS clé, un alias ou un ARN identifiant non valide, l'action peut sembler terminée, mais elle finit par échouer.

Vous ne pouvez pas modifier la KMS clé associée à un instantané ou à un volume existant. Toutefois, vous pouvez associer une KMS clé différente lors d'une opération de copie instantanée afin que l'instantané copié obtenu soit chiffré par la nouvelle KMS clé.

Chiffrer un volume vide lors de sa création

Lorsque vous créez un nouveau EBS volume vide, vous pouvez le chiffrer en activant le chiffrement pour l'opération de création de volume spécifique. Si vous avez activé EBS le chiffrement par défaut, le volume est automatiquement chiffré à l'aide de votre KMS clé de EBS chiffrement par défaut. Vous pouvez également spécifier une KMS clé de chiffrement symétrique différente pour l'opération de création de volume spécifique. Le volume est chiffré dès sa mise à disposition afin que vos données

soient toujours sécurisées. Pour connaître les procédures détaillées, consultez Créez un volume Amazon EBS..

Par défaut, la KMS clé que vous avez sélectionnée lors de la création d'un volume chiffre les instantanés que vous créez à partir du volume et les volumes que vous restaurez à partir de ces instantanés chiffrés. Vous ne pouvez pas supprimer le chiffrement d'un volume ou d'un instantané chiffré, ce qui signifie qu'un volume restauré à partir d'un instantané chiffré, ou une copie d'un instantané chiffré, reste toujours chiffré(e).

Les instantanés publics de volumes chiffrés ne sont pas pris en charge. Vous pouvez cependant partager un instantané chiffré avec certains comptes. Pour obtenir des instructions complètes, consultez Partager un instantané Amazon EBS avec d'autres comptes AWS.

Chiffrer les ressources non chiffrées

Vous ne pouvez pas directement chiffrer les volumes ou les instantanés non chiffrés existants. Toutefois, vous pouvez créer des volumes ou des instantanés chiffrés à partir de volumes ou d'instantanés non chiffrés. Si vous activez le chiffrement par défaut, Amazon chiffre EBS automatiquement les nouveaux volumes et les nouveaux instantanés à l'aide de votre KMS clé de chiffrement par défaut. EBS Sinon, vous pouvez activer le chiffrement lorsque vous créez un volume ou un instantané individuel, en utilisant soit la KMS clé par défaut pour le EBS chiffrement Amazon, soit une clé de chiffrement symétrique gérée par le client. Pour plus d'informations, consultez Créez un volume Amazon EBS. et Copier un instantané Amazon EBS.

Pour chiffrer la copie instantanée sur une clé gérée par le client, vous devez à la fois activer le chiffrement et spécifier la KMS clé, comme indiqué dansCopie d'un instantané non chiffré (chiffrement par défaut non activé).

> **Important**
>
> Amazon EBS ne prend pas en charge les KMS clés de chiffrement asymétriques. Pour plus d'informations, consultez la section Utilisation de KMS clés de chiffrement symétriques et asymétriques dans le manuel du AWS Key Management Service développeur.

Vous pouvez également appliquer de nouveaux états de chiffrement lors du lancement d'une instance à partir d'un système basé sur EBS -backedAMI. Cela est dû au fait que EBS -backed AMIs inclut des instantanés de EBS volumes qui peuvent être chiffrés comme décrit. Pour plus d'informations, voir Utiliser le chiffrement avec EBS -backed AMIs.

Rotation AWS KMS des clés utilisées pour le EBS chiffrement Amazon

Les bonnes pratiques de chiffrement décourage la réutilisation étendue des clés de chiffrement.

Pour créer un nouveau matériel cryptographique à utiliser avec le EBS chiffrement Amazon, vous pouvez créer une nouvelle clé gérée par le client, puis modifier vos applications pour qu'elles utilisent cette nouvelle KMS clé. Vous pouvez également activer la rotation automatique des clés pour une clé gérée par le client existante.

Lorsque vous activez la rotation automatique des clés pour une clé gérée par le client, de nouveaux éléments cryptographiques sont AWS KMS générés chaque année pour la KMS clé. AWS KMS enregistre toutes les versions précédentes du matériel cryptographique afin que vous puissiez continuer à déchiffrer et à utiliser les volumes et les instantanés précédemment chiffrés avec ce KMS matériel clé. AWS KMS ne supprime aucun élément clé pivoté tant que vous n'avez pas supprimé la KMS clé.

Lorsque vous utilisez une clé gérée par le client pivotée pour chiffrer un nouveau volume ou un nouvel instantané, elle AWS KMS utilise le (nouveau) contenu clé actuel. Lorsque vous utilisez une clé gérée par le client pivotée pour déchiffrer un volume ou un instantané, AWS KMS utilisez la version du matériel cryptographique utilisé pour le chiffrer. Si un volume ou un instantané est chiffré avec une version précédente du matériel cryptographique, continuez AWS KMS à utiliser cette version précédente pour le déchiffrer. AWS KMS ne rechiffre pas les volumes ou les instantanés précédemment chiffrés pour utiliser le nouveau matériel cryptographique après une rotation de clé. Ils restent chiffrés avec le matériel cryptographique avec lequel ils ont été initialement chiffrés. Vous pouvez utiliser en toute sécurité une clé gérée par le client avec rotation dans les applications et les AWS services sans modifier le code.

> **Note**
>
> - La rotation automatique des clés n'est prise en charge que pour les clés symétriques gérées par le client dont le contenu clé est AWS KMS créé.
> - AWS KMS change automatiquement Clés gérées par AWS chaque année. Vous ne pouvez pas activer ou désactiver la rotation des clés pour Clés gérées par AWS.

Pour plus d'informations, voir Rotating KMS key dans le guide du AWS Key Management Service développeur.

Exemples EBS de chiffrement Amazon

Lorsque vous créez une EBS ressource chiffrée, elle est chiffrée par la KMS clé de EBS chiffrement par défaut de votre compte, sauf si vous spécifiez une autre clé gérée par le client dans les paramètres de création du volume ou dans le mappage des périphériques par blocs pour l'instance AMI ou.

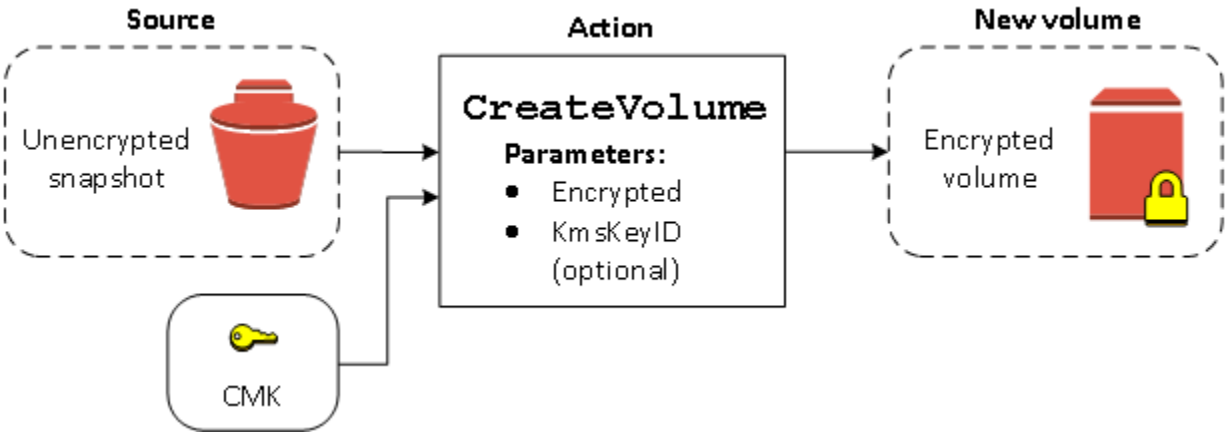
Les exemples suivants montrent comment vous pouvez gérer l'état de chiffrement de vos volumes et instantanés. Pour obtenir une liste complète des cas de chiffrement, consultez le tableau des résultats de chiffrement.

Exemples

- Restauration d'un volume non chiffré (chiffrement par défaut non activé)
- Restauration d'un volume non chiffré (chiffrement par défaut activé)
- Copie d'un instantané non chiffré (chiffrement par défaut non activé)
- Copie d'un instantané non chiffré (chiffrement par défaut activé)
- Rechiffrement d'un volume chiffré
- Rechiffrement d'un instantané chiffré
- Migration des données entre les volumes chiffrés et non chiffrés
- Résultats du chiffrement

Restauration d'un volume non chiffré (chiffrement par défaut non activé)

Sans le chiffrement par défaut activé, un volume restauré à partir d'un instantané non chiffré est non chiffré par défaut. Cependant, vous pouvez chiffrer le volume créé en définissant le paramètre `Encrypted` et, éventuellement, le paramètre `KmsKeyId`. Le schéma suivant illustre le processus.

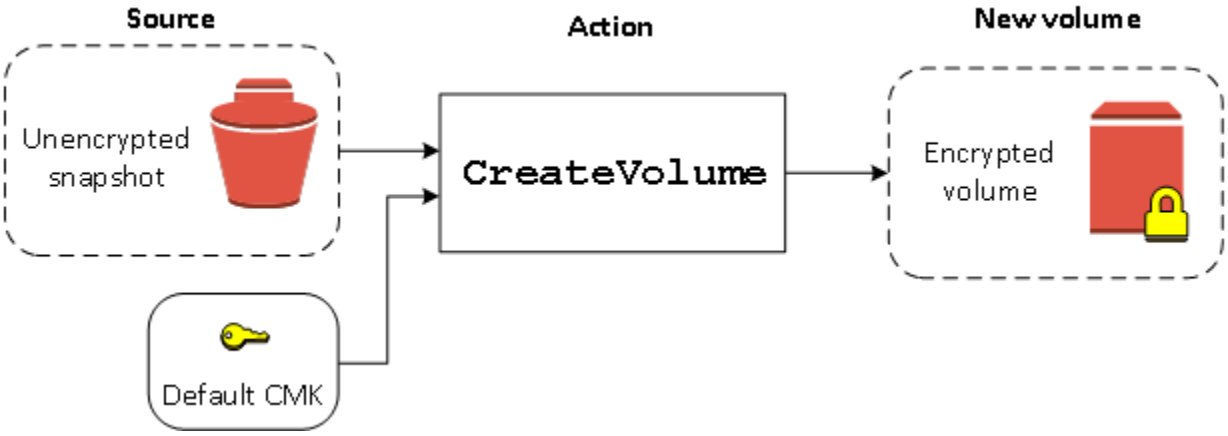


Si vous omettez ce `KmsKeyId` paramètre, le volume obtenu est chiffré à l'aide de votre KMS clé de EBS chiffrement par défaut. Vous devez spécifier un ID de KMS clé pour chiffrer le volume avec une autre KMS clé.

Pour de plus amples informations, veuillez consulter Créez un volume Amazon EBS..

Restauration d'un volume non chiffré (chiffrement par défaut activé)

Lorsque vous avez activé le chiffrement par défaut, le chiffrement est obligatoire pour les volumes restaurés à partir d'instantanés non chiffrés, et aucun paramètre de chiffrement n'est requis pour que votre KMS clé par défaut soit utilisée. Le schéma suivant illustre ce cas simple par défaut :

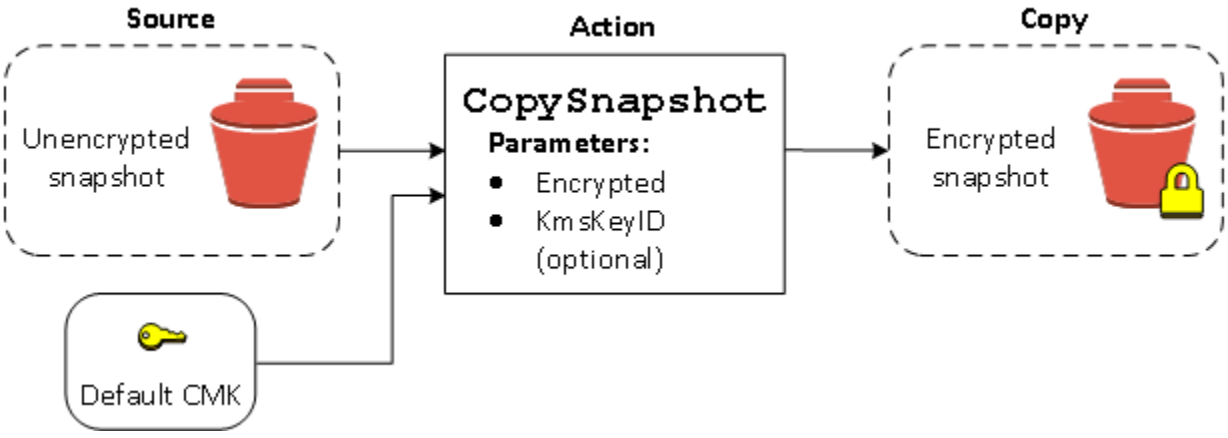


Si vous souhaitez chiffrer le volume restauré avec une clé de chiffrement gérée par le client symétrique, vous devez fournir les paramètres `Encrypted` et `KmsKeyId`, comme illustré dans Restauration d'un volume non chiffré (chiffrement par défaut non activé).

Copie d'un instantané non chiffré (chiffrement par défaut non activé)

Sans le chiffrement par défaut activé, une copie d'un instantané non chiffré est non chiffrée par défaut. Cependant, vous pouvez chiffrer l'instantané créé en définissant le paramètre `Encrypted` et, éventuellement, le paramètre `KmsKeyId`. Si vous omettez`KmsKeyId`, l'instantané obtenu est chiffré à l'aide de votre KMS clé par défaut. Vous devez spécifier un ID de KMS clé pour chiffrer le volume avec une autre clé de chiffrement KMS symétrique.

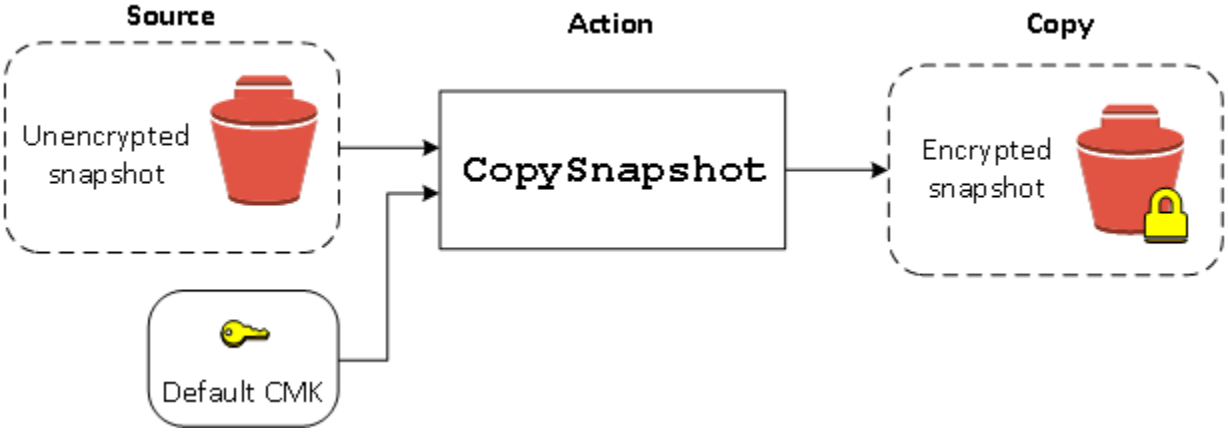
Le schéma suivant illustre le processus.



Vous pouvez chiffrer un EBS volume en copiant un instantané non chiffré sur un instantané chiffré, puis en créant un volume à partir de l'instantané chiffré. Pour de plus amples informations, veuillez consulter Copier un instantané Amazon EBS.

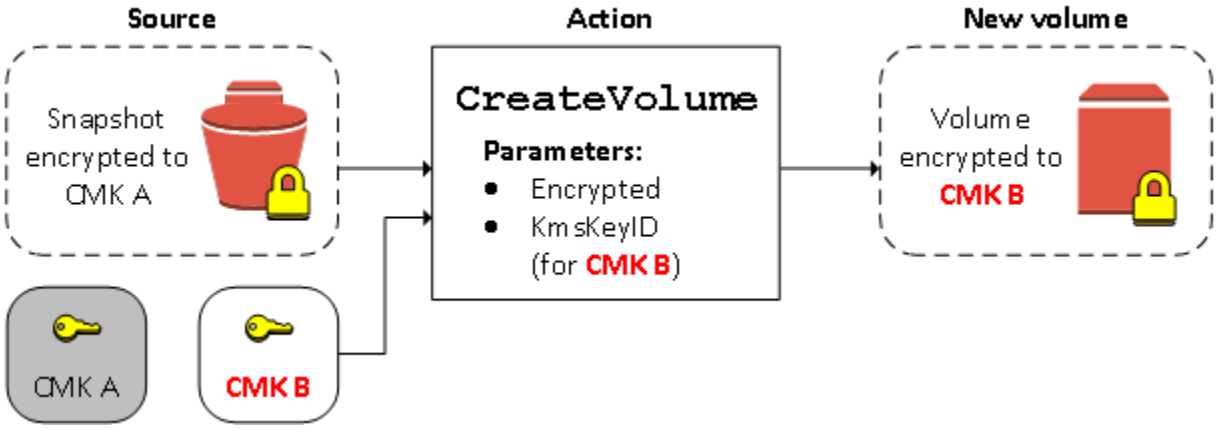
Copie d'un instantané non chiffré (chiffrement par défaut activé)

Lorsque vous avez activé le chiffrement par défaut, le chiffrement est obligatoire pour les copies d'instantanés non chiffrés, et aucun paramètre de chiffrement n'est requis si votre KMS clé par défaut est utilisée. Le schéma suivant illustre ce scénario par défaut :



Rechiffrement d'un volume chiffré

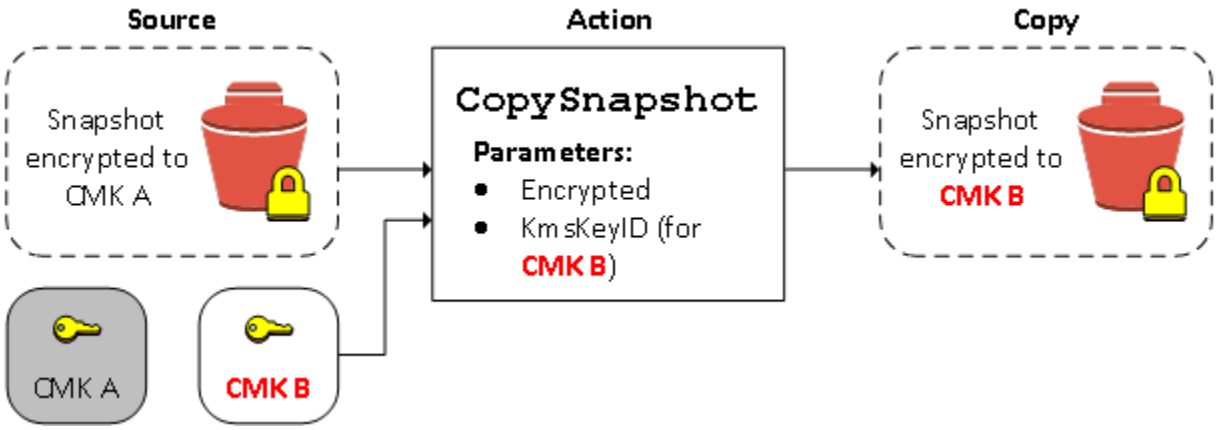
Lorsque l'`CreateVolume`action est exécutée sur un instantané chiffré, vous avez la possibilité de le rechiffrer avec une autre KMS clé. Le schéma suivant illustre le processus. Dans cet exemple, vous possédez deux KMS clés, la KMS clé A et la KMS clé B. L'instantané source est chiffré par la KMS clé A. Lors de la création du volume, avec l'KMSID de KMS clé B spécifié en paramètre, les données source sont automatiquement déchiffrées, puis rechiffrées par la clé B. KMS



Pour de plus amples informations, veuillez consulter Créez un volume Amazon EBS..

Rechiffrement d'un instantané chiffré

La possibilité de chiffrer un instantané pendant la copie vous permet d'appliquer une nouvelle KMS clé de chiffrement symétrique à un instantané déjà chiffré dont vous êtes propriétaire. Les volumes restaurés à partir de la copie résultante ne sont accessibles qu'à l'aide de la nouvelle KMS clé. Le schéma suivant illustre le processus. Dans cet exemple, vous possédez deux KMS clés, la KMS clé A et la KMS clé B. L'instantané source est chiffré par la KMS clé A. Pendant la copie, avec l'KMSID de KMS clé B spécifié en paramètre, les données source sont automatiquement rechiffrées par la KMS clé B.



Dans un scénario similaire, vous pouvez choisir d'appliquer de nouveaux paramètres de chiffrement à une copie d'instantané partagée avec vous. Par défaut, la copie est chiffrée à l'aide d'une KMS clé partagée par le propriétaire de l'instantané. Toutefois, nous vous recommandons de créer une copie de l'instantané partagé à l'aide d'une autre KMS clé que vous contrôlez. Cela protège votre accès au volume si la KMS clé d'origine est compromise ou si le propriétaire révoque la KMS clé pour une quelconque raison. Pour de plus amples informations, veuillez consulter Chiffrement et copie d'instantanés.

Migration des données entre les volumes chiffrés et non chiffrés

Lorsque vous avez accès à un volume chiffré et à un volume non chiffré, vous pouvez librement transférer des données entre eux. EC2effectue les opérations de chiffrement et de déchiffrement de manière transparente.

Instances Linux

Par exemple, utilisez la commande rsync pour copier les données. Dans l'exemple suivant, les données source se trouvent à l'emplacement `/mnt/source` et le volume de destination est monté à l'emplacement `/mnt/destination`.

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

instances Windows

Par exemple, utilisez la commande robocopy pour copier les données. Dans l'exemple suivant, les données source se trouvent à l'emplacement `D:\` et le volume de destination est monté à l'emplacement `E:\`.

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

Nous vous conseillons d'utiliser des dossiers plutôt que de copier tout un volume, afin d'éviter d'éventuels problèmes de dossiers masqués.

Résultats du chiffrement

Le tableau suivant décrit le résultat du chiffrement pour chaque combinaison possible de paramètres.

Le chiffrement EBS est-il activé ?	Le chiffrement par défaut est-il activé ?	Source du volume	Par défaut (aucune clé gérée par le client n'est spécifiée)	Personnalisé (clé gérée par le client spécifiée)
Non	Non	Nouveau volume (vide)	Non chiffré	N/A
Non	Non	Instantané non chiffré que vous possédez	Non chiffré	
Non	Non	Instantané chiffré que vous possédez	Chiffré par la même clé	
Non	Non	Instantané non chiffré qui est partagé avec vous	Non chiffré	
Non	Non	Instantané chiffré qui est partagé avec vous	Chiffré par clé gérée par le client par défaut*	
Oui	Non	Nouveau volume	Chiffré par défaut par clé gérée par le client	Chiffré par une clé gérée par le client spécifiée**
Oui	Non	Instantané non chiffré que vous possédez	Chiffré par défaut par clé gérée par le client	

Le chiffrement EBS est-il activé ?	Le chiffrement par défaut est-il activé ?	Source du volume	Par défaut (aucune clé gérée par le client n'est spécifiée)	Personnalisé (clé gérée par le client spécifiée)
Oui	Non	Instantané chiffré que vous possédez	Chiffré par la même clé	
Oui	Non	Instantané non chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Oui	Non	Instantané chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Non	Oui	Nouveau volume (vide)	Chiffré par défaut par clé gérée par le client	N/A
Non	Oui	Instantané non chiffré que vous possédez	Chiffré par défaut par clé gérée par le client	
Non	Oui	Instantané chiffré que vous possédez	Chiffré par la même clé	
Non	Oui	Instantané non chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Non	Oui	Instantané chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Oui	Oui	Nouveau volume	Chiffré par défaut par clé gérée par le client	Chiffré par une clé gérée par le client spécifiée

Le chiffrement EBS est-il activé ?	Le chiffrement par défaut est-il activé ?	Source du volume	Par défaut (aucune clé gérée par le client n'est spécifiée)	Personnalisé (clé gérée par le client spécifiée)
Oui	Oui	Instantané non chiffré que vous possédez	Chiffré par défaut par clé gérée par le client	
Oui	Oui	Instantané chiffré que vous possédez	Chiffré par la même clé	
Oui	Oui	Instantané non chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	
Oui	Oui	Instantané chiffré qui est partagé avec vous	Chiffré par défaut par clé gérée par le client	

* Il s'agit de la clé gérée par le client par défaut utilisée pour le EBS chiffrement du AWS compte et de la région. Par défaut, il s'agit d'une Clé gérée par AWS forme uniqueEBS, ou vous pouvez spécifier une clé gérée par le client.

** Il s'agit d'une clé gérée par le client spécifiée pour le volume au moment du lancement. Cette clé gérée par le client est utilisée à la place de la clé gérée par le client par défaut pour le AWS compte et la région.

Performances des volumes Amazon EBS

Plusieurs facteurs, dont les caractéristiques d'I/O et la configuration de vos instances et volumes, peuvent avoir des répercussions sur les performances d'Amazon EBS. Si vous suivez les instructions figurant sur nos pages détaillées sur les EC2 produits Amazon EBS et Amazon, vous obtiendrez généralement de bonnes performances. Cependant, dans certains cas, vous devrez peut-être effectuer des réglages pour obtenir des performances optimales. Nous vous recommandons d'optimiser les performances à l'aide des informations provenant de votre charge de travail réelle, en plus des comparaisons, afin de déterminer votre configuration optimale. Maintenant que vous maîtrisez les bases de l'utilisation des volumes EBS, nous allons examiner les performances d'I/O dont vous avez besoin et les options qui vous permettront d'améliorer les performances d'Amazon EBS afin de répondre à ces besoins.

AWS les mises à jour des performances des types de volumes EBS peuvent ne pas prendre effet immédiatement sur vos volumes existants. Pour bénéficier de performances optimales sur un ancien volume, vous devrez peut-être d'abord effectuer une action `ModifyVolume` sur celui-ci. Pour de plus amples informations, veuillez consulter Modifier un volume Amazon EBS à l'aide des opérations Elastic Volumes.

Table des matières

Conseils sur les performances Amazon EBS

Ces conseils constituent des bonnes pratiques à appliquer pour obtenir des performances optimales à partir de vos volumes EBS, dans différents scénarios d'utilisation.

Utiliser les instances optimisées pour EBS

Sur les instances sans prise en charge d'un débit optimisé pour EBS, le trafic réseau peut se heurter au trafic entre votre instance et vos volumes EBS. Sur les instances optimisées pour EBS, les deux types de trafic sont séparés. Certaines configurations d'instance optimisées pour EBS entraînent des frais supplémentaires (par exemple, C3, R3 et M3), tandis que d'autres sont optimisées pour EBS sans frais supplémentaires (par exemple, M4, C4, C5 et D2). Pour de plus amples informations, veuillez consulter Optimisation Amazon EBS.

Configurer la bande passante de l'instance

Pour les types d'instances pris en charge, vous pouvez configurer la pondération de la bande passante de l'instance pour augmenter la bande passante Amazon EBS de 25 % à l'aide de la pondération de `ebs-1` bande passante. Cette fonctionnalité vous permet d'optimiser l'allocation des ressources réseau de votre instance entre le réseau EBS et le réseau VPC, ce qui peut améliorer les performances d'EBS pour les charges de travail intensives en E/S. Pour de plus amples informations, veuillez consulter Pondération de bande passante d'instance configurable.

Comprendre comment les performances sont calculées

Lorsque vous mesurez les performances de vos volumes EBS, il est important de comprendre les unités de mesure impliquées et la méthode de calcul des performances. Pour plus d'informations, consultez Caractéristiques et surveillance des E/S Amazon EBS.

Comprendre votre charge de travail

Il existe un lien entre les performances maximales de vos volumes EBS, la taille et le nombre d'opérations d'I/O, et le temps nécessaire pour effectuer chaque action. Chacun de ces critères (performances, I/O et latence) a un impact sur les autres, et chaque application est plus ou moins sensible à un critère ou à un autre. Pour de plus amples informations, veuillez consulter Évaluez les volumes Amazon EBS.

Être conscient des pertes de performances lors de l'initialisation des volumes à partir d'instantanés

La latence augmente considérablement la première fois que vous accédez à chaque bloc de données sur un nouveau volume EBS créé à partir d'un instantané. Vous pouvez éviter cette baisse de performances à l'aide de l'une des solutions suivantes :

- Accédez à chaque bloc avant de placer le volume en production. Ce processus est appelé initialisation (anciennement « préchauffage »). Pour plus d'informations, consultez Initialiser les volumes Amazon EBS.
- Activez la restauration d'instantané rapide sur un instantané pour vous assurer que les volumes EBS créés à partir de l'instantané sont entièrement initialisés à la création et fournissent instantanément la totalité des performances allouées. Pour plus d'informations, consultez Restauration d'instantané rapide Amazon EBS.

Facteurs qui peuvent dégrader les performances des volumes HDD

Lorsque vous créez un instantané d'un volume HDD à débit optimisé (`st1`) ou HDD à froid (`sc1`), les performances peuvent diminuer jusqu'à la valeur de référence du volume pendant que l'instantané est en cours de création. Ce comportement est propre à ces types de volume. Voici d'autres facteurs qui peuvent limiter les performances : débit généré supérieur à celui que l'instance peut accepter, pertes de performance lors de l'initialisation des volumes créés à partir d'un instantané, et quantité excessive d'I/O aléatoires de petite taille sur le volume. Pour plus d'informations sur le calcul du débit des volumes HDD, consultez Types de volume Amazon EBS.

Vos performances peuvent également être affectées si votre application n'envoie pas suffisamment de demandes d'I/O. Il est possible de contrôler ce phénomène en examinant la longueur de file d'attente et la taille d'I/O de votre volume. La longueur de la file d'attente est le nombre de demandes d'I/O en attente, en provenance de votre application et à destination de votre volume. Pour une cohérence optimale, les volumes basés sur HDD doivent conserver une longueur de file d'attente de 4 ou plus (arrondie au nombre entier le plus proche) lors de l'exécution d'I/O séquentielles d'1 Mio. Pour plus d'information sur la manière de garantir des performances constantes sur vos volumes, consultez Caractéristiques et surveillance des E/S Amazon EBS

Augmentez la lecture anticipée pour les charges de travail à haut débit et en lecture intense sur et (instances Linux uniquement) ***st1 sc1***

Certaines charges de travail impliquent une forte densité de lecture et accèdent au périphérique de stockage en mode bloc via le cache d'une page du système d'exploitation (par exemple, à partir d'un système de fichiers). Dans ce cas, afin d'obtenir un débit optimal, nous vous recommandons de configurer le paramètre de lecture anticipée sur 1 Mio. Il s'agit d'un per-block-device paramètre qui ne doit être appliqué qu'aux volumes de votre disque dur.

Afin d'examiner la valeur actuelle de lecture anticipée pour vos périphériques de stockage en mode bloc, utilisez la commande suivante :

```
$ sudo blockdev --report /dev/<device>
```

Les informations sur les périphériques de stockage en mode bloc s'affichent au format suivant :

```
RO    RA   SSZ   BSZ   StartSec            Size   Device
rw   256   512  4096       4096      8587820544   /dev/<device>
```

Le périphérique affiché indique une valeur de lecture anticipée de 256 (la valeur par défaut). Multipliez ce nombre par la taille du secteur (512 octets) afin d'obtenir la taille de la mémoire tampon de lecture anticipée (128 Kio ici). Pour définir la valeur de la mémoire tampon sur 1 Mio, utilisez la commande suivante :

```
$ sudo blockdev --setra 2048 /dev/<device>
```

Pour vérifier que le paramètre de lecture anticipée affiche maintenant 2 048, exécutez de nouveau la première commande.

N'utilisez ce paramètre que lorsque votre charge de travail se compose d'I/O séquentielles de grande taille. Si elle se compose essentiellement d'I/O aléatoires de petite taille, ce paramètre va dégrader vos performances. En général, si votre charge de travail se compose principalement d'I/O aléatoires ou de petite taille, vous devez envisager d'utiliser un volume SSD à usage général (gp2 et gp3) plutôt qu'un volume `st1` ou `sc1`.

Utiliser un noyau Linux moderne (instances Linux uniquement)

Utilisez un noyau Linux récent avec une prise en charge des descripteurs indirects. Tout noyau Linux 3.8 ou supérieur prend en charge ce support, ainsi que toute instance de la génération actuelle EC2 . Si votre taille moyenne d'I/O atteint 44 Kio ou s'en rapproche, il est possible que vous utilisiez une instance ou un noyau qui ne prend pas en charge les descripteurs indirects. Pour plus d'informations sur le calcul de la taille moyenne des E/S à partir CloudWatch des métriques Amazon, consultez. Caractéristiques et surveillance des E/S Amazon EBS

Pour obtenir un débit optimal sur les volumes `st1` ou `sc1`, nous vous recommandons d'appliquer la valeur 256 au paramètre `xen_blkfront.max` (pour les versions de noyau Linux antérieures à la 4.6) ou au paramètre `xen_blkfront.max_indirect_segments` (pour un noyau Linux version 4.6

et supérieures). Le paramètre approprié peut être défini dans la ligne de commande de démarrage de votre système d'exploitation.

Par exemple, dans une AMI Amazon Linux avec un noyau antérieur, vous pouvez l'ajouter à la fin de la ligne du noyau, dans la configuration GRUB disponible dans `/boot/grub/menu.lst`:

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
 xen_blkfront.max=256
```

Pour un noyau plus récent, la commande serait semblable à ce qui suit :

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
 xen_blkfront.max_indirect_segments=256
```

Redémarrez votre instance pour que ce paramètre prenne effet.

Pour plus d'informations, voir Configurer GRUB pour le AMIs paravirtual. D'autres distributions Linux, en particulier celles qui n'utilisent pas le programme d'amorçage GRUB, peuvent nécessiter une approche différente pour le réglage des paramètres du noyau.

Pour plus d'informations sur les caractéristiques d'I/O EBS, consultez la présentation re:Invent à ce sujet, intitulée Amazon EBS: Designing for Performance.

Utiliser RAID 0 pour optimiser l'utilisation des ressources d'instance

Certains types d'instance peuvent générer un débit d'I/O supérieur à celui que vous pouvez provisionner pour un seul volume EBS. Vous pouvez associer plusieurs volumes dans une configuration RAID 0 afin d'utiliser la bande passante disponible pour ces instances. Pour de plus amples informations, veuillez consulter Configuration d'Amazon EBS et du RAID.

Surveillez les performances des volumes Amazon EBS

Vous pouvez surveiller et analyser les performances de vos volumes Amazon EBS à l'aide d'Amazon CloudWatch, des contrôles de statut et des statistiques de performance détaillées d'EBS. Pour plus d'informations, consultez CloudWatch Métriques Amazon pour Amazon EBS et Statistiques de performance EBS détaillées d'Amazon.

Optimisation Amazon EBS

Une instance optimisée pour Amazon EBS utilise une pile de configuration optimisée et fournit une capacité supplémentaire dédiée aux I/O Amazon EBS. Cette optimisation offre les meilleures performances pour vos volumes EBS en réduisant les conflits entre les I/O Amazon EBS et le trafic restant de votre instance.

Les instances optimisées par EBS fournissent une bande passante dédiée vers Amazon EBS. Lorsqu'ils sont attachés à une instance optimisée pour EBS, les volumes SSD polyvalents (`gp2` et `gp3`) sont conçus pour garantir au moins 90 % de leurs performances d'IOPS provisionnés, et ce 99 % du temps au cours d'une année donnée, et les volumes SSD à IOPS provisionnées (`io1` et `io2`) sont conçus pour garantir au moins 90 % de leurs performances provisionnées, et ce 99,9 % du temps au cours d'une année donnée. Les volumes HDD à débit optimisé (`st1`) et les volumes HDD à froid (`sc1`) garantissent tous deux au moins 90 % de leurs performances de débit prévues, et ce 99 % du temps au cours d'une année donnée. Les périodes non conformes sont assez uniformément réparties, en ciblant 99 % du débit total attendu chaque heure. Pour de plus amples informations, veuillez consulter Types de volume Amazon EBS.

Pour plus d'informations, consultez la section Instances optimisées pour Amazon EBS dans le guide de EC2 l'utilisateur Amazon.

Pondération de bande passante d'instance configurable

La configuration de la bande passante d'instance (IBC) est une fonctionnalité qui vous permet d'ajuster l'allocation de bande passante réseau entre Amazon EBS et le réseau VPC pour une instance Amazon. EC2 Cette fonctionnalité peut vous aider à optimiser les performances pour les charges de travail nécessitant une bande passante spécifique. La configuration de la bande passante des instances n'est prise en charge que sur certaines instances. Pour plus d'informations, consultez la section Configuration de la pondération de la bande passante de l'instance.

Pour les performances EBS, l'utilisation de la pondération de `ebs-1` bande passante augmente la bande passante EBS de base de 25 % tout en réduisant la bande passante du réseau VPC du même montant absolu. Cela peut être bénéfique pour les charges de travail intensives en E/S qui nécessitent un débit EBS plus élevé.

Lorsque vous planifiez votre charge de travail, prenez bien en compte la taille et les modèles de vos E/S. Les petites tailles d'E/S sont généralement moins affectées par les limitations de bande passante, tandis que les tailles d'E/S plus importantes ou les charges de travail séquentielles peuvent

avoir des impacts plus importants en cas de modifications de bande passante. Il est essentiel de tester minutieusement votre charge de travail spécifique pour garantir des performances optimales avec la pondération de bande passante que vous avez choisie.

Considérations

- La bande passante d'instance configurable est prise en charge sur certains types d'instances. Pour plus d'informations, consultez la section Types d'instances pris en charge.
- L'utilisation de la pondération de `ebs-1` bande passante augmente la bande passante EBS jusqu'à 25 %, ce qui peut améliorer les performances des applications gourmandes en E/S. Cependant, gardez à l'esprit que la bande passante du réseau VPC sera réduite du même montant absolu (la spécification de bande passante combinée entre EBS et réseau ne change pas).
- Les modifications de la pondération de la bande passante peuvent affecter de manière significative les performances d'E/S. Avec la pondération de la `vpc-1` bande passante, la bande passante du réseau est augmentée, mais il est possible que vous constatiez des IOPS inférieures aux attentes pour les volumes EBS. Cela est dû au fait que vous pouvez atteindre la limite de bande passante EBS avant la limite d'IOPS, en particulier avec des tailles d'E/S plus importantes. Par exemple, un type d'instance qui prend généralement en charge 240 000 IOPS avec une taille d'E/S de 16 KiB peut atteindre moins d'IOPS en utilisant le poids de bande passante en raison de la diminution de la `vpc-1` bande passante EBS.
- Testez toujours votre charge de travail spécifique pour vous assurer que la pondération de bande passante que vous avez choisie répond à vos besoins de performance.
- Vous pouvez configurer la pondération de la bande passante lors du lancement de l'instance ou la modifier pour les instances arrêtées. Pour plus d'informations, consultez Configurer la pondération de bande passante pour votre instance.
- Vous pouvez configurer la pondération de la bande passante de l'instance sans frais supplémentaires.

Caractéristiques et surveillance des E/S Amazon EBS

Sur une configuration de volume donnée, certaines caractéristiques d'I/O déterminent les performances pour vos volumes EBS.

- Les volumes sauvegardés sur SSD, les SSD à usage général (`gp2etgp3`) et les SSD à IOPS provisionnés (`io1etio2`) offrent des performances constantes, qu'une opération d'E/S soit aléatoire ou séquentielle.

- Les volumes sauvegardés sur disque dur, le disque dur à débit optimisé (`st1`) et le disque dur froid (`sc1`), offrent des performances optimales uniquement lorsque les opérations d'E/S sont volumineuses et séquentielles.

Afin de comprendre comment les volumes SSD et HDD se comporteront dans votre application, il est important de comprendre la connexion entre la demande sur le volume, le nombre d'IOPS disponibles pour ce dernier, le temps nécessaire pour effectuer une opération d'I/O et les limites de débit du volume.

Rubriques

IOPS

Les IOPS sont une unité de mesure qui représente une efficacité input/output operations per second. The operations are measured in KiB, and the underlying drive technology determines the maximum amount of data that a volume type counts as a single I/O. I/O size is capped at 256 KiB for SSD volumes and 1,024 KiB for HDD volumes because SSD volumes handle small or random I/O bien plus élevée que les volumes de disque dur.

Lorsque des opérations d'I/O de petite taille sont physiquement séquentielles, Amazon EBS tente de les fusionner dans une seule opération d'I/O, sans dépasser la taille maximale. De même, lorsque les opérations d'I/O sont supérieures à la taille maximale d'I/O, Amazon EBS tente de les diviser en opérations d'I/O de petite taille. Le tableau suivant montre quelques exemples.

Type de volume	Taille d'I/O maximum	Opérations d'I/O de votre application	Nombre d'IOPS	Remarques
SSD	256 Kio	1 opération d'I/O de 1 024 KiB	4 (1 024÷256=4)	Amazon EBS divise les 1 024

Type de volume	Taille d'I/O maximum	Opérations d'I/O de votre application	Nombre d'IOPS	Remarques
				opérations d'I/O en quatre opérations plus petites de 256 KiB.
		8 x opérations d'I/O séquentielles de 32 Kio	1 (8x32=256)	Amazon EBS fusionne les huit opérations d'I/O séquentielles de 32 KiB en une seule opération de 256 KiB.
		8 opérations d'I/O aléatoires de 32 KiB	8	Amazon EBS compte séparément les opérations d'I/O aléatoires.
HDD	1 024 KiB	1 opération d'I/O de 1 024 KiB	1	L'opération d'I/O est déjà égale à la taille d'I/O maximale. Elle n'est ni fusionnée ni divisée.
		8 x opérations d'I/O séquentielles de 128 Kio	1 (8x128=1 024)	Amazon EBS fusionne les huit opérations d'I/O séquentielles de 128 Kio dans une seule opération d'I/O de 1 024 Kio.

Type de volume	Taille d'I/O maximum	Opérations d'I/O de votre application	Nombre d'IOPS	Remarques
		8 opérations d'I/O aléatoires de 32 KiB	8	Amazon EBS compte séparément les opérations d'I/O aléatoires.

Par conséquent, lorsque vous créez un volume soutenu par SSD prenant en charge 3 000 IOPS (soit en provisionnant un `io1` `io2` volume avec 3 000 IOPS, en dimensionnant un volume `gp2` à 1 000 GiB, soit en utilisant un `gp3` volume), et que vous l'attachez à une instance optimisée pour EBS capable de fournir une bande passante suffisante, vous pouvez transférer jusqu'à 3 000 E/S de données par seconde, avec un débit déterminé par la taille des E/S.

Latence et longueur de file d'attente d'un volume

La longueur de file d'attente d'un volume correspond au nombre de demandes d'I/O pour un appareil. La latence est le temps réel passé par le end-to-end client lors d'une opération d'E/S, en d'autres termes, le temps écoulé entre l'envoi d'une E/S à EBS et la réception d'un accusé de réception d'EBS indiquant que la lecture ou l'écriture des E/S est terminée. La longueur de la file d'attente doit être correctement calibrée avec la taille et la latence d'I/O, pour éviter de créer des goulots d'étranglement sur le système d'exploitation « invité » ou sur le lien réseau vers EBS.

La longueur de la file d'attente optimale varie en fonction des charges de travail, selon la sensibilité de votre application à la latence et à l'IOPS. Si votre charge de travail ne fournit pas suffisamment de demandes d'I/O pour tirer pleinement parti des performances disponibles dans votre volume EBS, il est possible que le volume ne donne pas les IOPS ou le débit que vous avez provisionnés.

Les applications qui génèrent de nombreuses transactions sont sensibles à une latence d'I/O accrue et sont adaptées à des volumes basés sur SSD. Vous pouvez conserver des IOPS élevées et une latence faible grâce à une longueur de file d'attente moyenne réduite et à un nombre élevé d'IOPS disponibles pour le volume. Si vous envoyez vers un volume un nombre d'IOPS supérieur à la quantité qu'il peut contenir, vous risquez d'accroître la latence d'I/O.

Les applications qui génèrent des débits élevés sont moins sensibles à une latence d'I/O accrue et sont adaptées à des volumes basés sur HDD. Vous pouvez conserver un débit élevé vers les volumes basés sur HDD grâce à une longueur de file d'attente élevée lors de l'exécution d'I/O séquentielles volumineuses.

Taille des I/O et limites de débit par volume

Pour les volumes basés sur SSD, si votre taille d'I/O est très volumineuse, vous aurez peut-être un nombre inférieur d'IOPS par rapport aux IOPS provisionnées, dans la mesure où vous aurez atteint le débit limite pour le volume. Par exemple, un gp2 volume inférieur à 1 000 GiB avec des crédits de rafale disponibles a une limite d'IOPS de 3 000 et une limite de débit de 250 MiB/s. If you are using a 256 KiB I/O size, your volume reaches its throughput limit at 1000 IOPS (1000 x 256 KiB = 250 MiB). For smaller I/O sizes (such as 16 KiB), this same volume can sustain 3,000 IOPS because the throughput is well below 250 MiB/s. (These examples assume that your volume's I/O n'atteint pas les limites de débit de l'instance.) Pour plus d'informations sur les limites de débit pour chaque type de volume EBS, consultez Types de volume Amazon EBS.

Pour les opérations d'E/S de moindre envergure, vous pouvez voir une valeur d' higher-than-provisionedIOPS mesurée depuis l'intérieur de votre instance. Cela se produit lorsque le système d'exploitation de l'instance fusionne les petites opérations d'I/O dans une opération de plus grande taille avant de les transmettre à Amazon EBS.

Si votre charge de travail utilise des I/O séquentielles sur des volumes `st1` et `sc1` basés sur HDD, vous risquez d'obtenir un nombre d'IOPS plus élevé que prévu (mesuré depuis votre instance). Cela se produit lorsque le système d'exploitation de l'instance fusionne des I/O séquentielles et les comptabilise dans des unités de 1 024 Kio. Si votre charge de travail utilise des I/O de petite taille ou aléatoires, vous risquez d'obtenir un débit moins élevé que prévu. En effet, nous comptabilisons chaque I/O aléatoire et non séquentielle par rapport au nombre total d'IOPS, ce qui peut vous conduire à atteindre la limite d'IOPS du volume plus tôt que prévu.

Quel que soit le type de volume EBS, si vous ne bénéficiez pas des IOPS ou du débit attendus dans votre configuration, assurez-vous que la bande passante de votre EC2 instance n'est pas le facteur limitant. Vous devez toujours utiliser une instance optimisée pour EBS de génération actuelle (ou une instance qui inclut 10 Gb/s network connectivity) for optimal performance. Another possible cause for not experiencing the expected IOPS is that you are not driving enough I/O volumes EBS).

Surveillez les caractéristiques des E/S à l'aide de CloudWatch

Vous pouvez surveiller ces caractéristiques d'E/S à l'aide des métriques de volume de chaque CloudWatch volume.

Moniteur pour les E/S bloquées

`VolumeStalledIOCheck` surveille le statut de vos volumes EBS afin de déterminer à quel moment ils sont dégradés. La métrique est une valeur binaire qui renvoie un statut `0` (réussite) ou un statut 1 (échec) selon que le volume EBS peut ou non effectuer des opérations d'E/S.

Si la `VolumeStalledIOCheck` métrique échoue, vous pouvez soit attendre AWS que le problème soit résolu, soit prendre des mesures, telles que le remplacement du volume concerné ou l'arrêt et le redémarrage de l'instance à laquelle le volume est attaché. Dans la plupart des cas, lorsque cette métrique échoue, EBS diagnostique et restaure automatiquement votre volume en quelques minutes. Vous pouvez utiliser l'action Pause I/O AWS Fault Injection Service pour exécuter des expériences contrôlées afin de tester votre architecture et votre surveillance sur la base de cette métrique afin d'améliorer votre résilience face aux défaillances de stockage.

Surveiller la latence des E/S pour un volume

Vous pouvez surveiller la latence moyenne pour les opérations de lecture et d'écriture d'un volume Amazon EBS à l'aide des `VolumeAvgWriteLatency` métriques `VolumeAvgReadLatency` et respectivement.

Si la latence de vos E/S est supérieure à ce dont vous avez besoin, assurez-vous que votre application n'essaie pas de générer plus d'IOPS ou de débit que ce que vous avez prévu pour votre volume. Utilisez les formules suivantes pour calculer les IOPS et le débit moyens acheminés vers votre volume sur une période donnée, puis comparez-les aux IOPS et au débit provisionnés du volume.

```
                                  Sum(VolumeReadOps) + Sum(VolumeWriteOps)
Estimated average IOPS in ops/s = ----------------------------------------
                                        Period - Sum(VolumeIdleTime)
```

```
                                        (Sum(VolumeReadBytes) +
 Sum(VolumeWriteBytes)) / 1024
Estimated average throughput in KiB/s =
 ------------------------------------------------------
                                                  Period - Sum(VolumeIdleTime)
```

Vous pouvez également surveiller les `VolumeThroughputExceededCheck` indicateurs `VolumeIOPSExceededCheck` et pour déterminer si votre charge de travail a constamment tenté de générer des IOPS ou un débit supérieur aux performances provisionnées de votre volume au cours d'une minute donnée. Si les IOPS pilotées dépassent régulièrement les performances d'IOPS provisionnées de votre volume, la `VolumeIOPSExceededCheck` métrique est renvoyée. 1 Si

le débit piloté dépasse régulièrement les performances de débit provisionné de votre volume, la `VolumeThroughputExceededCheck` métrique est renvoyée. 1 Si les IOPS et le débit pilotés sont conformes aux performances allouées à votre volume, les indicateurs sont renvoyés. `0`

Si votre application a besoin d'un nombre d'IOPS supérieur à ce que votre volume peut fournir, envisagez d'utiliser l'une des options suivantes :

- Un volume `gp3`, `io2`, ou `io1` approvisionné avec suffisamment d'IOPS pour atteindre la latence requise
- Un volume `gp2` plus important qui fournit des performances IOPS de base suffisantes

Les volumes `st1` et `sc1` basés sur HDD sont conçus pour générer de meilleures performances avec des charges de travail qui tirent parti de la taille d'I/O maximale de 1 024 Kio. Pour déterminer la taille moyenne des E/S de votre volume, divisez `VolumeWriteBytes` par`VolumeWriteOps`. Le même calcul s'applique pour les opérations de lecture. Si la taille d'I/O moyenne est inférieure à 64 Kio, vous devriez pouvoir améliorer les performances en augmentant la taille des opérations d'I/O envoyées à un volume `st1` ou `sc1`.

Surveillez l'équilibre des compartiments en rafale pour**`gp2`**,**`st1`**, et les **`sc1`** volumes

`BurstBalance` affiche l'équilibre du compartiment en rafales des volumes `gp2`, `st1` et `sc1` sous forme de pourcentage du solde restant. Lorsque votre compartiment en rafales est épuisé, le I/O du volume (pour volumes `gp2`) ou le débit de volume (pour les volumes `st1` et `sc1`) est limité au niveau de référence. Vérifiez la valeur `BurstBalance` pour déterminer si votre volume est limité pour cette raison. Pour obtenir la liste complète des métriques Amazon EBS disponibles, consultez CloudWatch Métriques Amazon pour Amazon EBS et les métriques Amazon EBS pour les instances basées sur Nitro.

Surveillez les statistiques de performance des E/S en temps réel

Vous pouvez accéder à des statistiques de performance détaillées en temps réel pour les volumes Amazon EBS attachés à des instances Amazon EC2 basées sur Nitro.

Vous pouvez combiner ces statistiques pour obtenir la latence moyenne et les IOPS, ou pour vérifier si les opérations d'E/S sont terminées. Vous pouvez également consulter la durée totale pendant laquelle votre application a dépassé les IOPS ou les limites de débit allouées à votre volume EBS ou à l'instance attachée. En suivant l'augmentation de ces statistiques au fil du temps, vous pouvez déterminer si vous devez augmenter vos IOPS provisionnées ou vos limites de débit pour optimiser

les performances de votre application. Les statistiques de performances détaillées incluent également des histogrammes pour les opérations d'E/S en lecture et en écriture, qui fournissent une distribution de votre latence d'E/S en suivant le nombre total d'opérations d'E/S effectuées dans une bande de latence.

Pour de plus amples informations, veuillez consulter Statistiques de performance EBS détaillées d'Amazon.

Ressources connexes

Pour en savoir plus sur les caractéristiques d'I/O Amazon EBS, consultez la présentation re:Invent suivante : Amazon EBS: Designing for Performance.

Initialiser les volumes Amazon EBS

Les volumes EBS vides reçoivent leurs performances maximum au moment où ils sont créés et ne nécessitent pas d'initialisation (anciennement préchauffage).

Pour les volumes, quel que soit leur type, qui ont été créés à partir d'instantanés, les blocs de stockage doivent être extraits d'Amazon S3 et écrits sur le volume avant que vous puissiez y accéder. Cette action préalable prend du temps et peut causer une hausse significative de la latence des opérations d'I/O lors du premier accès à chaque bloc. Les performances du volume sont obtenues une fois que tous les blocs ont été téléchargés et écrits sur le volume.

> **Important**
>
> Lors de l'initialisation des volumes Provisioned IOPS SSD créés à partir d'instantanés, les performances du volume peuvent chuter jusqu'à plus de 50 % en dessous du niveau attendu, ce qui entraîne l'affichage par le volume d'un état `warning` dans le contrôle de statut Performances des I/O. Cette situation est attendue et vous pouvez ignorer l'état `warning` des volumes Provisioned IOPS SSD lorsque vous les initialisez. Pour plus d'informations, consultez Contrôles de l'état des volumes Amazon EBS.

Pour la plupart des applications, l'amortissement du coût d'initialisation sur la durée de vie du volume est acceptable. Pour éviter cette baisse de performances initiale dans un environnement de production, vous pouvez utiliser l'une des solutions suivantes :

- Forcez l'initialisation immédiate de la totalité du volume. Pour plus d'informations, consultez Instances Linux (instances Linux) ou instances Windows (instances Windows).
- Activez la restauration d'instantané rapide sur un instantané pour vous assurer que les volumes EBS créés à partir de l'instantané sont entièrement initialisés à la création et fournissent instantanément la totalité des performances allouées. Pour de plus amples informations, veuillez consulter Restauration d'instantané rapide Amazon EBS.

Instances Linux

Pour initialiser un volume créé à partir d'un instantané sur Linux

1. Attachez le volume qui vient d'être restauré à votre instance Linux.
2. Utilisez la commande lsblk pour afficher les périphériques de stockage en mode bloc attachés à votre instance.

```
$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0  30G  0 disk
xvda1 202:1    0   8G  0 disk /
```

   Ici, vous pouvez voir que le nouveau volume, `/dev/xvdf`, est attaché, mais pas monté (car aucun chemin n'est répertorié sous la colonne `MOUNTPOINT`).
3. Utilisez les utilitaires dd ou fio pour lire tous les blocs de l'appareil. La commande dd est installée par défaut sur les systèmes Linux, mais la commande fio est nettement plus rapide dans la mesure où elle permet les lectures multithreads.

   > **Note**
   >
   > Cette étape peut prendre de quelques minutes à plusieurs heures, en fonction de la bande passante de votre EC2 instance, des IOPS provisionnées pour le volume et de la taille du volume.

   [dd] Le paramètre `if` (fichier en entrée) doit être défini sur le lecteur que vous souhaitez initialiser. Le paramètre `of` (fichier de sortie) doit être défini sur l'appareil virtuel null Linux, `/dev/null`. Le paramètre `bs` définit la taille de bloc de l'opération de lecture. Pour des performances optimales, il doit être défini sur 1 Mo.

> **Important**
>
> L'utilisation incorrecte de la commande dd peut facilement entraîner la destruction des données d'un volume. Veillez à suivre précisément l'exemple de commande ci-dessous. Seul le paramètre `if=/dev/xvdf` varie en fonction du nom de l'appareil que vous lisez.

```
$ sudo dd if=/dev/xvdf of=/dev/null bs=1M status=progress
```

[fio] Si la commande fio est installée sur votre système, utilisez la commande suivante pour initialiser votre volume. Le paramètre `--filename` (fichier en entrée) doit être défini sur le lecteur que vous souhaitez initialiser.

```
$ sudo fio --filename=/dev/xvdf --rw=read --bs=1M --iodepth=32 --ioengine=libaio --
direct=1 --name=volume-initialize
```

Pour installer la commande fio sur Amazon Linux, utilisez la commande suivante :

```
sudo yum install -y fio
```

Pour installer la commande fio sur Ubuntu, utilisez la commande suivante :

```
sudo apt-get install -y fio
```

Une fois l'opération terminée, un rapport s'affiche au sujet de l'opération de lecture. Votre volume est maintenant prêt à être utilisé. Pour de plus amples informations, veuillez consulter Rendre un volume Amazon EBS disponible pour utilisation.

instances Windows

Avant d'utiliser un outil, rassemblez des informations au sujet des disques sur votre système comme suit :

Pour collecter des informations sur les disques système

1. Utilisez la commande wmic afin d'afficher une liste des disques disponibles sur votre système :

```
wmic diskdrive get size,deviceid
```

Voici un exemple de sortie :

```
DeviceID            Size
\\.\PHYSICALDRIVE2  80517265920
\\.\PHYSICALDRIVE1  80517265920
\\.\PHYSICALDRIVE0  128849011200
\\.\PHYSICALDRIVE3  107372805120
```

2. Identifiez le disque à initialiser à l'aide de dd ou de fio. Le lecteur `C:` se trouve sur `\\.\PHYSICALDRIVE0`. Vous pouvez utiliser l'utilitaire `diskmgmt.msc` afin de comparer les lettres de lecteur aux numéros de lecteur de disque si vous avez des doutes sur le numéro de lecteur à utiliser.

Use the dd utility

Suivez les procédures suivantes pour installer et utiliser dd pour initialiser un volume.

Considérations Importantes

- L'initialisation d'un volume prend de quelques minutes à plusieurs heures, en fonction de la bande passante de votre EC2 instance, des IOPS allouées au volume et de sa taille.
- L'utilisation incorrecte de la commande dd peut facilement entraîner la destruction des données d'un volume. Assurez-vous de suivre précisément cette procédure.

Pour installer dd pour Windows

La commande dd pour le programme Windows fonctionne de la même manière que pour le programme dd généralement disponible pour Linux et les systèmes Unix. Elle vous permet en outre d'initialiser les volumes Amazon EBS qui ont été créés à partir d'instantanés. Les versions bêta les plus récentes prennent en charge le périphérique `/dev/null` virtuel. Si vous installez une version antérieure, vous pouvez utiliser le périphérique `nul` virtuel à la place. Une documentation détaillée est disponible sur http://www.chrysocome.net/dd.

1. Téléchargez la version binaire la plus récente de dd pour Windows sur http://www.chrysocome.net/dd.

2. (Facultatif) Créez un dossier pour les utilitaires de ligne de commande en veillant à ce qu'il soit facile à trouver et à mémoriser, par exemple `C:\bin`. Si vous avez déjà un dossier désigné pour les utilitaires de ligne de commande, vous pouvez l'utiliser au cours de l'étape suivante.
3. Décompressez le package binaire et copiez le fichier `dd.exe` dans votre dossier des utilitaires de ligne de commande (par exemple, `C:\bin`).
4. Ajoutez le dossier des utilitaires de ligne de commande à la variable d'environnement Path afin de pouvoir exécuter les programmes de ce dossier où que vous vous trouviez.
    a. Choisissez Démarrer, ouvrez le menu contextuel (clic droit) pour Ordinateur, puis sélectionnez Propriétés.
    b. Choisissez Paramètres système avancés, Variables d'environnement.
    c. Pour Variables système, sélectionnez la variable Chemin et choisissez Modifier.
    d. Pour Valeur de la variable, ajoutez un point-virgule et l'emplacement de votre dossier des utilitaires de ligne de commande (**`;C:\bin\`**) à la fin de la valeur existante.
    e. Choisissez OK pour fermer la fenêtre Modifier la variable système.
5. Ouvrez une nouvelle fenêtre d'invite de commandes. L'étape précédente ne met pas à jour les variables d'environnement dans votre fenêtre active d'invite de commandes. Les fenêtres d'invite de commandes que vous ouvrez maintenant que vous avez terminé l'étape précédente sont mises à jour.

Pour initialiser un volume à l'aide de la commande dd pour Windows

Exécutez la commande suivante pour lire tous les blocs sur l'appareil spécifié (et envoyer la sortie vers l'appareil virtuel `/dev/null`). Cette commande initialise en toute sécurité les données existantes.

```
dd if=\\.\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```

Une erreur peut s'afficher si dd tente de lire au-delà de la fin du volume. Vous pouvez l'ignorer sans risque.

Si vous avez utilisé une version antérieure de la commande dd, celle-ci ne prend pas en charge l'appareil `/dev/null`. Au lieu de cela, vous pouvez utiliser l'appareil `nul` comme suit.

```
dd if=\\.\PHYSICALDRIVEn of=nul bs=1M --progress --size
```

Use the fio utility

Suivez les procédures suivantes pour installer et utiliser fio pour initialiser un volume.

Pour installer fio pour Windows

La commande fio pour le programme Windows fonctionne de la même manière que pour le programme fio généralement disponible pour Linux et les systèmes Unix. Elle vous permet en outre d'initialiser les volumes Amazon EBS qui ont été créés à partir d'instantanés. Pour plus d'informations, voir https://github.com/axboe/fio.

1. Téléchargez le programme d'installation fio MSI en développant Ressources pour la dernière version et en sélectionnant le programme d'installation MSI.
2. Installer fio.

Pour Initialiser un volume à l'aide de la commande fio pour Windows

1. Exécutez une commande similaire à ce qui suit afin d'initialiser un volume :

```
fio --filename=\\.\PHYSICALDRIVEn  --rw=read --bs=128k --iodepth=32 --direct=1
 --name=volume-initialize
```

2. Une fois l'opération terminée, vous êtes prêt à utiliser votre nouveau volume. Pour de plus amples informations, veuillez consulter Rendre un volume Amazon EBS disponible pour utilisation.

Configuration d'Amazon EBS et du RAID

Avec Amazon EBS, vous pouvez utiliser toute configuration RAID standard que vous pourriez utiliser avec un serveur bare metal traditionnel, dans la mesure où cette configuration RAID est prise en charge par le système d'exploitation de votre instance. Cela est dû au fait que l'ensemble de la configuration RAID est mise en œuvre au niveau logiciel.

Les données de volume Amazon EBS sont répliquées sur plusieurs serveurs dans une zone de disponibilité pour éviter la perte de données résultant de la défaillance d'un seul composant. Cette réplication rend les volumes Amazon EBS dix fois plus fiables que les disques durs classiques. Pour plus d'informations, consultez la section Fonctionnalités d'Amazon EBS.

Table des matières

Options de configuration RAID

La création d'une grappe RAID 0 vous permet d'obtenir un niveau de performance plus élevé pour un système de fichiers que vous pouvez mettre en service sur un volume Amazon EBS unique. Utilisez RAID 0 quand les performances d'I/O sont de la plus haute importance. Avec un RAID 0, les I/O sont réparties entre les volumes dans un agrégat par bandes. Si vous ajoutez un volume, du débit et des IOPS sont ajoutés directement. Cependant, gardez à l'esprit que les performances de l'agrégat par bandes sont limitées à celles du volume le moins performant, et que la perte d'un seul volume entraîne la perte complète des données pour la grappe.

La taille résultante d'une grappe RAID 0 est la somme des tailles des volumes contenues par celle-ci, et la bande passante correspond au total de bande passante disponible des volumes de la grappe. Par exemple, deux volumes `io1` de 500 Gio avec 4 000 IOPS approvisionnés pour chacun créent une grappe RAID 0 de 1 000 Gio avec une bande passante disponible de 8 000 IOPS et 1 000 Mo/s de débit.

> **Important**
>
> RAID 5 et RAID 6 ne sont pas recommandés pour Amazon EBS, car les opérations d'écritures de parité de ces modes RAID consomment certaines des IOPS (IOPS) disponibles pour vos volumes. En fonction de la configuration de votre grappe RAID, ces modes RAID fournissent de 20 à 30 % d'IOPS utilisables en moins qu'une configuration RAID 0. Le coût accru est également un facteur à prendre en compte avec ces modes RAID ; avec l'utilisation de tailles et de vitesses de volume identiques, une grappe RAID 0 à 2 volumes peut offrir de meilleures performances qu'une grappe RAID 6 à 4 volumes dont le coût est deux fois plus élevé.
>
> L'utilisation d'un RAID 1 n'est pas non plus recommandée avec Amazon EBS. Le RAID 1 nécessite plus de bande passante Amazon EC2 vers Amazon EBS que les configurations non RAID, car les données sont écrites simultanément sur plusieurs volumes. En outre, un RAID 1 ne fournit aucune amélioration des performances d'écriture.

Création d'une matrice RAID 0

Pour créer la grappe RAID 0, suivez la procédure suivante.

Considérations

- Avant d'exécuter cette procédure, vous devez déterminer la taille de votre matrice RAID 0 et le nombre d'IOPS à allouer.
- Créez des volumes avec des tailles et des valeurs de performances d'IOPS (IOPS) identiques pour votre grappe. Assurez-vous de ne pas créer une baie qui dépasse la bande passante disponible de votre EC2 instance.
- Vous devez éviter de démarrer à partir d'un volume RAID. Si l'un des appareils tombe en panne, il se peut que vous ne puissiez pas démarrer le système d'exploitation.

Instances Linux

Pour créer une grappe RAID 0 sous Linux

1. Créez les volumes Amazon EBS pour votre grappe. Pour de plus amples informations, veuillez consulter Créez un volume Amazon EBS..
2. Attachez les volumes Amazon EBS à l'instance devant héberger la grappe. Pour plus d'informations, consultez Associer un volume Amazon EBS à une instance Amazon EC2 .
3. Utilisez la commande mdadm pour créer une unité RAID logique à partir des volumes Amazon EBS nouvellement attachés. Remplacez le nombre de volumes de votre matrice par *`number_of_volumes`* et les noms des périphériques de chaque volume de la matrice (par exemple`/dev/xvdf`) par*`device_name`*. Vous pouvez également le *`MY_RAID`* remplacer par votre propre nom unique pour le tableau.

   > **Note**
   >
   > Vous pouvez afficher la liste des unités de votre instance avec la commande lsblk pour trouver les noms d'unité.

   Pour créer une grappe RAID 0, exécutez la commande suivante (notez l'option `--level=0` pour agréger la grappe) :

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --
raid-devices=number_of_volumes device_name1 device_name2
```

> **Tip**
>
> Si l'erreur `mdadm: command not found` s'affiche, utilisez la commande suivante pour installer mdadm : `sudo yum install mdadm`.

4. Laissez à la grappe RAID le temps de s'initialiser et se synchroniser. Vous pouvez suivre la progression de ces opérations avec la commande suivante :

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

Voici un exemple de sortie :

```
Personalities : [raid0]
md0 : active raid0 xvdc[1] xvdb[0]
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

En général, vous pouvez afficher des informations détaillées sur votre grappe RAID avec la commande suivante :

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

Voici un exemple de sortie :

```
/dev/md0:
           Version : 1.2
     Creation Time : Wed May 19 11:12:56 2021
        Raid Level : raid0
        Array Size : 41910272 (39.97 GiB 42.92 GB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Wed May 19 11:12:56 2021
```

```
              State : clean
     Active Devices : 2
    Working Devices : 2
     Failed Devices : 0
      Spare Devices : 0

         Chunk Size : 512K

Consistency Policy : none

               Name : MY_RAID
               UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
             Events : 0

    Number   Major   Minor   RaidDevice State
       0     202       16        0      active sync   /dev/sdb
       1     202       32        1      active sync   /dev/sdc
```

5. Créez un système de fichiers sur votre grappe RAID et attribuez-lui une étiquette à utiliser quand vous le monterez ultérieurement. Par exemple, pour créer un système de fichiers ext4 avec l'étiquette*MY_RAID*, exécutez la commande suivante :

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

   Selon les exigences de votre application ou les restrictions de votre système d'exploitation, vous pouvez utiliser un autre système de fichiers, comme ext3 ou XFS (consultez la documentation relative à votre système de fichiers pour trouver la commande de création de système de fichiers correspondante).

6. Pour vous assurer que la grappe RAID est réassemblée automatiquement au démarrage, créez un fichier de configuration qui contient les informations RAID :

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

   > **Note**
   >
   > Si vous utilisez une distribution Linux autre qu'Amazon Linux, il se peut que vous deviez modifier cette commande. Par exemple, il se peut que vous deviez placer le fichier dans un autre emplacement, ou ajouter le Paramètre `--examine`. Pour plus d'informations, exécutez man mdadm.conf sur votre instance Linux.

7. Créez une nouvelle une image ramdisk pour précharger correctement les modules de périphérique de stockage en mode bloc pour votre nouvelle configuration RAID :

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. Créez un point de montage (mount) pour votre grappe RAID.

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. Enfin, montez l'unité RAID sur le point de montage que vous avez créé :

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

   Votre unité RAID est maintenant prête à être utilisée.

10. (Facultatif) Pour monter ce volume Amazon EBS à chaque redémarrage du système, ajoutez une entrée pour l'appareil dans le fichier `/etc/fstab`.

    a. Créez une sauvegarde de votre fichier `/etc/fstab` que vous pouvez utiliser si vous détruisez ou supprimez accidentellement ce fichier en l'éditant.

    ```
    [ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
    ```

    b. Ouvrez le fichier `/etc/fstab` avec votre éditeur de texte préféré (comme nano ou vim).

    c. Placez en commentaires les lignes commençant par « `UUID=` » et, à la fin du fichier, ajoutez une nouvelle ligne pour votre volume RAID à l'aide du format suivant :

    ```
    device_label mount_point file_system_type fs_mntops fs_freq fs_passno
    ```

    Les trois derniers champs de cette ligne correspondent aux options de montage du système de fichiers, à la fréquence de vidage du système de fichiers et à l'ordre des contrôles de système de fichiers au démarrage. Si vous ne savez pas quelles valeurs utiliser, utilisez les valeurs de l'exemple ci-dessous (`defaults,nofail 0 2`). Pour plus d'informations sur les entrées `/etc/fstab`, consultez la page du manuel fstab (en entrant man fstab sur la ligne de commande). Par exemple, pour monter le système de fichiers ext4 sur l'unité avec l'étiquette MY_RAID au point de montage `/mnt/raid`, ajoutez l'entrée suivante à `/etc/fstab`.

> **Note**
>
> Si jamais vous prévoyez de démarrer votre instance sans ce volume attaché (par exemple, pour que ce volume puisse basculer entre différentes instances), vous devez ajouter l'option de montage `nofail` qui permet à l'instance de démarrer même si des erreurs se produisent lors du montage du volume. Les dérivés Debian, comme Ubuntu, doivent également ajouter l'option de montage `nobootwait`.

```
LABEL=MY_RAID       /mnt/raid   ext4    defaults,nofail        0       2
```

d. Après avoir ajouté la nouvelle entrée à `/etc/fstab`, vous devez vérifier que celle-ci fonctionne. Exécutez la commande sudo mount -a pour monter tous les systèmes de fichiers dans `/etc/fstab`.

```
[ec2-user ~]$ sudo mount -a
```

Si la commande précédente ne génère pas d'erreur, votre fichier `/etc/fstab` est correct et votre système de fichiers sera monté automatiquement au prochain démarrage. Si la commande génère des erreurs, examinez celles-ci et essayez de corriger votre fichier `/etc/fstab`.

> **Warning**
>
> Des erreurs dans le fichier `/etc/fstab` peuvent rendre un système impossible à démarrer. N'arrêtez pas un système dont le fichier `/etc/fstab` contient des erreurs.

e. (Facultatif) Si vous n'êtes pas sûr de savoir comment corriger des erreurs dans `/etc/fstab`, vous avez toujours la possibilité de restaurer votre fichier `/etc/fstab` de sauvegarde avec la commande suivante.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

instances Windows

Pour créer une grappe RAID 0 sous Windows

1. Créez les volumes Amazon EBS pour votre grappe. Pour de plus amples informations, veuillez consulter Créez un volume Amazon EBS..
2. Attachez les volumes Amazon EBS à l'instance devant héberger la grappe. Pour plus d'informations, consultez Associer un volume Amazon EBS à une instance Amazon EC2 .
3. Connectez-vous à votre instance Windows. Pour plus d'informations, consultez Connexion à votre instance Windows.
4. Ouvrez une invite de commande et tapez la commande diskpart.

```
diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51CO
```

5. A l'invite DISKPART, affichez la liste des disques disponibles avec la commande suivante.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B
  Disk 2    Online            8 GB      0 B
```

   Identifiez les disques que vous souhaitez utiliser dans votre grappe et notez leurs numéros.

6. Chaque disque à utiliser dans votre grappe doit être un disque dynamique en ligne ne contenant pas de volumes existants. Utilisez les étapes suivantes pour convertir des disques de base en disques dynamiques et supprimer les volumes existants.

   a. Sélectionnez le disque que vous souhaitez utiliser dans votre matrice à l'aide de la commande suivante, en le *n* remplaçant par votre numéro de disque.

```
DISKPART> select disk n

Disk n is now the selected disk.
```

b. Si le disque sélectionné est affiché comme étant `Offline`, mettez-le en ligne en exécutant la commande online disk.

c. Si le disque sélectionné ne comporte pas d'astérisque dans la colonne Dyn dans la sortie de la commande list disk précédente, vous devez le convertir en disque dynamique.

```
DISKPART> convert dynamic
```

> **Note**
>
> Si une erreur indique que le disque est protégé en écriture, vous pouvez effacer l'indicateur de lecture seule avec la commande ATTRIBUTE DISK CLEAR READONLY, puis retenter la conversion en disque dynamique.

d. Utilisez la commande detail disk pour vérifier s'il existe des volumes sur le disque sélectionné.

```
DISKPART> detail disk

XENSRC PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type   : SCSI
Status : Online
Path   : 0
Target : 1
LUN ID : 0
Location Path : PCIROOT(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only  : No
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 2     D   NEW VOLUME   FAT32  Simple      8189 MB  Healthy
```

Notez les numéros des volumes figurant sur le disque. Dans cet exemple, le numéro de volume est 2. Si le disque ne contient pas de volume, vous pouvez ignorer l'étape suivante.

e. (Obligatoire uniquement si des volumes ont été identifiés à l'étape précédente) Sélectionnez et supprimez les volumes existants sur le disque que vous avez identifiés à l'étape précédente.

> **Warning**
>
> Cette opération détruit les données existant sur le volume.

i. Sélectionnez le volume en le *n* remplaçant par votre numéro de volume.

```
DISKPART> select volume n
Volume n is the selected volume.
```

ii. Supprimez le volume.

```
DISKPART> delete volume

DiskPart successfully deleted the volume.
```

iii. Répétez ces sous-étapes pour chaque volume à supprimer sur le disque sélectionné.

f. Répétez l'opération Step 6 pour chaque disque à utiliser dans votre grappe.

7. Vérifiez que les disques que vous voulez utiliser sont maintenant dynamiques. Dans ce cas, nous utilisons les disques 1 et 2 pour le volume RAID.

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B   *
  Disk 2    Online            8 GB      0 B   *
```

8. Créez votre grappe RAID. Sous Windows, un volume RAID 0 est appelé volume agrégé par bandes.

   Pour créer une grappe de volumes agrégés par bandes sur les disques 1 et 2, utilisez la commande suivante (notez l'option `stripe` pour agréger la grappe) :

```
DISKPART> create volume stripe disk=1,2
```

```
DiskPart successfully created the volume.
```

9. Vérifiez votre nouveau volume.

```
DISKPART> list volume

  DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     C                NTFS   Partition     29 GB  Healthy    System
  Volume 1                      RAW    Stripe        15 GB  Healthy
```

Remarquez que la colonne `Type` indique maintenant que le volume 1 est un volume `stripe`.

10. Sélectionnez et formatez votre volume pour pouvoir commencer à l'utiliser.

    a. Sélectionnez le volume que vous souhaitez formater en le *n* remplaçant par votre numéro de volume.

```
DISKPART> select volume n

Volume n is the selected volume.
```

    b. Formatez le volume.

> **Note**
>
> Pour effectuer un formatage complet, omettez l'option `quick`.

```
DISKPART> format quick recommended label="My new volume"

  100 percent completed

DiskPart successfully formatted the volume.
```

    c. Affectez une lettre de lecteur disponible à votre volume.

```
DISKPART> assign letter f
```

```
DiskPart successfully assigned the drive letter or mount point.
```

Votre nouveau volume est maintenant prêt à être utilisé.

Créer des instantanés de volumes dans une grappe RAID

Si vous voulez sauvegarder les données sur les volumes EBS d'une grappe RAID à l'aide d'instantanés, vous devez vous assurer que les instantanés sont cohérents. La raison en est que les instantanés de ces volumes sont créés indépendamment. La restauration de volumes EBS d'une grappe RAID à partir d'instantanés non synchronisés peut dégrader l'intégrité de la grappe.

Pour créer un ensemble cohérent d'instantanés pour votre grappe RAID, utilisez les instantanés multi-volume EBS. Les instantanés multivolumes vous permettent de prendre point-in-time des instantanés coordonnés avec les données et cohérents en cas de crash sur plusieurs volumes EBS attachés à une instance. EC2 Vous n'avez pas à arrêter votre instance pour la coordonner entre les volumes et assurer la régularité, car les instantanés sont automatiquement pris sur plusieurs volumes EBS. Pour plus d'informations, consultez les étapes de création d'instantanés multi-volumes sous Créer des instantanés Amazon EBS.

Évaluez les volumes Amazon EBS

Vous pouvez tester les performances des volumes Amazon EBS en simulant des charges de travail d'I/O. Procédez comme suit :

1. Lancez une instance optimisée EBS.
2. Créez des volumes EBS.
3. Attachez les volumes à votre instance optimisée pour EBS.
4. Configurez et installez le périphérique de stockage en mode bloc.
5. Installez un outil permettant de comparer les performances d'I/O.
6. Comparez les performances d'I/O de vos volumes.
7. Supprimez vos volumes et mettez l'instance hors service pour éviter de générer des frais.

> **Important**
>
> Certaines des procédures entraîneront la destruction des données existantes sur les volumes EBS que vous comparez. Les procédures de comparaison sont conçues pour être utilisées sur des volumes créés spécialement à des fins de tests, et pas sur des volumes de production.

Configurer votre instance

Afin d'obtenir des performances optimales des volumes EBS, nous vous recommandons d'utiliser une instance optimisée pour EBS. Les instances optimisées pour EBS fournissent un débit dédié entre Amazon et EC2 Amazon EBS, avec instance. Les instances optimisées pour EBS fournissent une bande passante dédiée entre EC2 Amazon et Amazon EBS, les spécifications dépendant du type d'instance.

Pour créer une instance optimisée pour EBS, choisissez Launch en tant qu'instance optimisée pour EBS lorsque vous lancez l'instance à l'aide de la EC2 console Amazon, ou spécifiez-le --ebs-optimized lorsque vous utilisez la ligne de commande. Assurez-vous de sélectionner un type d'instance compatible avec cette option.

Configurer des volumes Provisioned IOPS SSD ou SSD à usage général

Pour créer des volumes SSD IOPS provisionnés (**`io1`**et**`io2`**) ou SSD à usage général (**`gp2`**et**`gp3`**) à l'aide de la EC2 console Amazon, pour le type de volume, choisissez SSD IOPS provisionné (io1), SSD IOPS provisionné (io2), SSD à usage général (gp2) ou SSD à usage général (gp3). Sur la ligne de commande, spécifiez `io1`, `io2`, `gp2` ou `gp3` pour le paramètre --volume-type. Pour les volumes `io1`, `io2` et `gp3`, spécifiez le nombre d'opérations d'I/O par seconde (IOPS) pour le paramètre --iops. Pour plus d'informations, consultez Types de volume Amazon EBS et Créez un volume Amazon EBS..

(Instances Linux uniquement) Pour les exemples de tests, nous vous recommandons de créer une matrice RAID 0 de 6 volumes, qui offre un haut niveau de performance. Dans la mesure où vous êtes facturé en fonction des gigaoctets provisionnés (et du nombre d'IOPS provisionnés pour les volumes io1, io2 et gp3), et non du nombre de volumes, aucun coût supplémentaire ne sera appliqué pour la création de plusieurs volumes de plus petite taille, puis pour leur utilisation afin de créer un agrégat par bandes. Si vous utilisez Oracle Orion afin de comparer vos volumes, vous pouvez effectuer une simulation de l'agrégation par bandes comme avec Oracle ASM. C'est pourquoi nous

vous recommandons de laisser Orion se charger de l'agrégation par bandes. Si vous utilisez un outil de comparaison différent, vous devez effectuer vous-même l'agrégation des volumes par bandes.

Pour plus d'informations sur la création d'une matrice RAID 0, consultezCréation d'une matrice RAID 0.

Configuration des volumes HDD à débit optimisé (**st1**) ou HDD à froid (**sc1**)

Pour créer un `st1` volume, choisissez Throughput Optimized HDD lorsque vous créez le volume à l'aide de la EC2 console Amazon, ou spécifiez-le --type **`st1`** lorsque vous utilisez la ligne de commande. Pour créer un `sc1` volume, choisissez Cold HDD lorsque vous créez le volume à l'aide de la EC2 console Amazon, ou spécifiez-le --type **`sc1`** lorsque vous utilisez la ligne de commande. Pour plus d'informations sur la création de volumes EBS, consultez Créez un volume Amazon EBS.. Pour plus d'informations sur la liaison de ces volumes à votre instance, consultez Associer un volume Amazon EBS à une instance Amazon EC2 .

(instances Linux uniquement) AWS fournit un modèle JSON à utiliser AWS CloudFormation qui simplifie cette procédure de configuration. Accédez au modèle et enregistrez-le sous forme de fichier JSON. AWS CloudFormation vous permet de configurer vos propres clés SSH et de configurer plus facilement un environnement de test de performance pour évaluer les `st1` volumes. Le modèle crée une instance de la génération actuelle et un volume `st1` de 2 Tio, et attache ce dernier à l'instance dans `/dev/xvdf`.

(Instances Linux uniquement) Pour créer un volume HDD à l'aide du modèle

1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
2. Choisissez Create Stack.
3. Choisissez Télécharger un modèle sur Amazon S3 et sélectionnez le modèle JSON que vous avez obtenu précédemment.
4. Donnez à votre pile un nom tel que « ebs-perf-testing », puis sélectionnez un type d'instance (la valeur par défaut est r3.8xlarge) et une clé SSH.
5. Choisissez Suivant à deux reprises, puis sélectionnez Créer une pile.
6. Lorsque l'état de votre nouvelle pile passe de CREATE_IN_PROGRESS à COMPLETE, choisissez Outputs (Sorties) afin d'obtenir l'entrée DNS publique de votre nouvelle instance, qui sera attachée à un volume `st1` de 2 Tio.
7. Connectez-vous à votre nouvelle pile via SSH en tant qu'utilisateur **`ec2-user`**, avec le nom d'hôte obtenu à partir de l'entrée DNS lors de l'étape précédente.

8. Passez à Installer les outils d'évaluation.

Installer les outils d'évaluation

Les tableaux suivants répertorient certains des outils que vous pouvez utiliser pour évaluer les performances des volumes EBS.

Instances Linux

Outil	Description

fio	Pour comparer les performances d'I/O. (Notez que la commande fio a une dépendance sur `libaio-devel` .)
	
	Pour installer fio sur Amazon Linux, exécutez la commande suivante :
	
	`$ sudo yum install -y fio`
	
	Pour installer fio sur Ubuntu, exécutez la commande suivante :
	
	`sudo apt-get install -y fio`

Outil de calibrage Oracle Orion	Pour calibrer les performances d'I/O des systèmes de stockage à utiliser avec les bases de données Oracle.

instances Windows

Outil	Description
DiskSpd	DiskSpd est un outil de performance du stockage développé par les équipes d'ingénierie Windows, Windows Server et Cloud Server Infrastructure de Microsoft. Il est disponible en téléchargement sur https://github.com/Microsoft/diskspd/releases. Après avoir téléchargé le fichier exécutable `diskspd.exe` , ouvrez une invite de commande avec des droits d'administration (en choisissant « Exécuter en

Outil	Description
	tant qu'administrateur »), puis accédez au répertoire où vous avez copié le fichier `diskspd.exe` . Copiez le fichier `diskspd.exe` exécutable souhaité à partir du dossier exécutable approprié (`amd64fre`, `armfre` ou `x86fre`) vers un chemin d'accès court et simple tel que `C:\DiskSpd` . Dans la plupart des cas, vous aurez besoin de la version 64 bits de DiskSpd depuis le `amd64fre` dossier. Le code source de DiskSpd est hébergé sur GitHub : https://github.com/Microsoft/diskspd.
CrystalDiskMark	CrystalDiskMark est un simple logiciel de test de disque. Il est disponible en téléchargement à l'adresse https://crystalmark. info/en/software/crystaldiskmark/.

Ces outils de comparaison prennent en charge un large éventail de paramètres de test. Vous devez utiliser des commandes proches des charges de travail que vos volumes devront prendre en charge. Les commandes ci-dessous sont proposées à titre d'exemple pour vous permettre de débuter.

Choisir la longueur de la file d'attente d'un volume

Choisissez la meilleure longueur de file d'attente du volume en fonction de votre charge de travail et du type de volume.

Longueur de la file d'attente sur les volumes basés sur SSD

Afin de déterminer la longueur moyenne optimale de file d'attente pour votre charge de travail sur des volumes basés sur SSD, nous vous recommandons de cibler une longueur de file d'attente de 1 toutes les 1 000 IOPS disponibles (quantité de référence pour les volumes SSD à usage général et quantité provisionnée pour les volumes Provisioned IOPS SSD). Vous pouvez ensuite contrôler les performances de votre application et ajuster cette valeur en fonction des exigences de votre application.

L'augmentation de la longueur de file d'attente offre un avantage jusqu'à ce que vous atteigniez le nombre d'IOPS provisionnés, le débit ou la valeur optimale de la longueur de file d'attente du système, actuellement définie sur 32. Par exemple, un volume avec 3 000 IOPS provisionnés doit

cibler une longueur de file d'attente de 3. Vous devez essayer d'augmenter ou de diminuer ces valeurs afin de déterminer ce qui fonctionne le mieux pour votre application.

Longueur de la file d'attente sur les volumes basés sur HDD

Afin de déterminer la longueur moyenne optimale de file d'attente pour votre charge de travail sur des volumes basés sur HDD, nous vous recommandons de cibler une longueur de file d'attente de 4 tout en exécutant des I/O séquentielles d'1 Mio. Vous pouvez ensuite contrôler les performances de votre application et ajuster cette valeur en fonction des exigences de votre application. Par exemple, un `st1` volume de 2 TiB avec un débit en rafale de 500 respectivement. MiB/s and IOPS of 500 should target a queue length of 4, 8, or 16 while performing 1,024 KiB, 512 KiB, or 256 KiB sequential I/Os Vous devez essayer d'augmenter ou de diminuer ces valeurs afin de déterminer ce qui fonctionne le mieux pour votre application.

Désactivation des états « C-state »

Avant de procéder à des comparaisons, vous devez désactiver les états « C-state » du processeur. Les cœurs temporairement inutilisés dans une UC prise en charge peuvent passer à l'état « C-state » pour économiser de l'énergie. Lorsque le cœur est appelé afin de reprendre le traitement, un certain laps de temps est nécessaire avant que le cœur soit à nouveau entièrement opérationnel. Cette latence peut interférer avec les routines de comparaison du processeur. Pour plus d'informations sur les états C et les types d' EC2 instances qui les prennent en charge, consultez la section Contrôle de l'état du processeur pour votre EC2 instance.

Instances Linux

Vous pouvez désactiver les états « C-state » sur Amazon Linux, RHEL et CentOS de la manière suivante :

1. Identifiez le nombre d'états « C-state ».

```
$ cpupower idle-info | grep "Number of idle states:"
```

2. Désactivez les états « C-state » de c1 à cN. Idéalement, l'état des cœurs doit être c0.

```
$ for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

instances Windows

Vous pouvez désactiver les états « C-state » sur un système Windows de la manière suivante :

1. Dans PowerShell, obtenez le schéma d'alimentation actif actuel.

```
$current_scheme = powercfg /getactivescheme
```

2. Identifiez le GUID du mode de gestion de l'alimentation.

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter
 "ElementName='High performance'").InstanceID
```

3. Identifiez le GUID du paramètre d'alimentation.

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter
 "ElementName='Processor idle disable'").InstanceID
```

4. Identifiez le GUID du sous-groupe du paramètre d'alimentation.

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -
Filter "ElementName='Processor power management'").InstanceID
```

5. Désactivez les états « C-state » en paramétrant la valeur de l'index sur 1. La valeur 0 indique que les états « C-state » sont désactivés.

```
powercfg /
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>
 1
```

6. Définissez le mode actif afin de garantir l'enregistrement des paramètres.

```
powercfg /setactive <power_scheme_guid>
```

Effectuer la comparaison

Les procédures suivantes décrivent les commandes de comparaison pour différents types de volume EBS.

Exécutez les commandes suivantes sur une instance optimisée pour EBS avec les volumes EBS attachés. Si les volumes EBS ont été créés à partir d'instantanés, veillez à les initialiser avant

d'effectuer la comparaison. Pour de plus amples informations, veuillez consulter Initialiser les volumes Amazon EBS.

> **Tip**
>
> Vous pouvez utiliser les histogrammes de latence d'E/S fournis par les statistiques de performances détaillées d'EBS pour comparer la distribution des performances d'E/S dans vos tests d'analyse comparative. Pour de plus amples informations, veuillez consulter Statistiques de performance EBS détaillées d'Amazon.

Lorsque vous avez terminé de tester vos volumes, consultez les rubriques suivantes pour obtenir de l'aide sur le nettoyage : Supprimer un volume Amazon EBS et Mettez fin à votre instance.

Définir des points de référence pour les volumes Provisioned IOPS SSD et SSD à usage général

Instances Linux

Exécutez fio sur la grappe RAID 0 que vous avez créée.

La commande suivante effectue des opérations d'écriture aléatoires 16 Ko.

```
$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --name fio_test_file --
direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --
group_reporting --norandommap
```

La commande suivante effectue des opérations de lecture aléatoires 16 Ko.

```
$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1 --rw=randread
 --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --group_reporting --
norandommap
```

Pour plus d'informations sur l'interprétation des résultats, consultez le didacticiel Inspecting disk IO performance with fio.

instances Windows

Exécutez DiskSpd sur le volume que vous avez créé.

La commande suivante exécute un test d'I/O aléatoire de 30 secondes à l'aide d'un fichier de test de 20 Go situé sur le lecteur `C:`, avec un taux d'écriture de 25 % et de lecture de 75 %, ainsi qu'une taille de bloc de 8 Ko. Elle utilisera huit threads de travail, chacun avec quatre I/O exceptionnelles, et une valeur d'entropie d'écriture de 1 Go. Les résultats du test seront enregistrés dans un fichier texte appelé `DiskSpeedResults.txt`. Ces paramètres simulent une charge de travail OLTP SQL Server.

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

Pour plus d'informations sur l'interprétation des résultats, consultez ce didacticiel : Inspection des performances d'E/S du disque avec Disk SPd.

Benchmark **`st1`** et **`sc1`** volumes (instances Linux)

Exécutez la commande fio sur votre volume `st1` ou `sc1`.

> **Note**
>
> Avant d'exécuter ces tests, définissez les I/O mises en mémoire tampon sur votre instance, comme indiqué dans Augmentez la lecture anticipée pour les charges de travail à haut débit et en lecture intense sur et (instances Linux uniquement) *`st1 sc1`*.

La commande suivante exécute des opérations de lecture séquentielle d'1 Mio sur un périphérique de stockage en mode bloc `st1` attaché (par exemple, `/dev/xvdf`) :

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

La commande suivante exécute des opérations d'écriture séquentielle d'1 Mio sur un périphérique de stockage en mode bloc `st1` attaché :

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

Certaines charges de travail exécutent une combinaison de lectures séquentielles et d'écritures séquentielles dans différentes parties du périphérique de stockage en mode bloc. Pour évaluer une

telle charge de travail, nous vous recommandons d'utiliser des tâches fio distinctes et simultanées pour les lectures et les écritures, et d'utiliser l'option fio `offset_increment` pour cibler différents emplacements du périphérique de stockage en mode bloc pour chaque tâche.

L'exécution de cette charge de travail est un peu plus compliquée qu'une charge de travail d'écriture séquentielle ou de lecture séquentielle. Utilisez un éditeur de texte pour créer un fichier de tâche fio, appelé `fio_rw_mix.cfg` dans cet exemple, contenant les éléments suivants :

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

Ensuite, exécutez la commande suivante :

```
$ sudo fio fio_rw_mix.cfg
```

Pour plus d'informations sur l'interprétation des résultats, consultez le didacticiel Inspecting disk I/O performance with fio.

Plusieurs tâches fio pour l'I/O directe, même en cas d'utilisation d'opérations de lecture ou d'écriture séquentielle, peuvent se traduire par un débit inférieur à celui attendu pour les volumes `st1` et `sc1`. Nous vous recommandons d'utiliser une tâche d'I/O directe et le paramètre `iodepth` pour contrôler le nombre d'opérations d'I/O simultanées.

Automatisez les sauvegardes avec Amazon Data Lifecycle Manager

Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création, la conservation et la suppression des instantanés EBS et des copies sauvegardées par EBS. AMIs Lorsque vous automatisez la gestion des instantanés et des AMI, cela vous aide à :

- protéger les données importantes en appliquant un planning de sauvegarde régulière ;
- Créez une norme AMIs qui peut être actualisée à intervalles réguliers.
- conserver des sauvegardes comme exigé par les auditeurs ou les réglementations internes ;
- réduire les frais de stockage en supprimant les sauvegardes périmées.
- Créez des politiques de sauvegarde de reprise après sinistre qui sauvegardent les données sur des régions ou des comptes isolés.

Associé aux fonctionnalités de surveillance d'Amazon EventBridge et d'Amazon Data Lifecycle Manager AWS CloudTrail, il fournit une solution de sauvegarde complète pour les EC2 instances Amazon et les volumes EBS individuels, sans frais supplémentaires.

> **⚠ Important**
>
> - Amazon Data Lifecycle Manager ne peut pas gérer les instantanés ni les AMIs créer par aucun autre moyen.
> - Amazon Data Lifecycle Manager ne peut pas automatiser la création, la conservation et la suppression d'instances sauvegardées en magasin AMIs.

Table des matières

- Créez une politique personnalisée Amazon Data Lifecycle Manager pour les applications soutenues par EBS AMIs
- Automatisez les copies instantanées entre comptes avec Data Lifecycle Manager
- Modifier les politiques d'Amazon Data Lifecycle Manager
- Supprimer les politiques d'Amazon Data Lifecycle Manager
- Contrôlez l'accès à Amazon Data Lifecycle Manager à l'aide d'IAM
- Surveillez les politiques d'Amazon Data Lifecycle Manager
- Résoudre les problèmes liés à Amazon Data Lifecycle Manager

Quotas

Votre AWS compte possède les quotas suivants liés à Amazon Data Lifecycle Manager :

Description	Quota
Politiques de cycle de vie personnalisées par région	100
Politiques par défaut pour les instantanés EBS par région	1
Politiques par défaut pour les applications soutenues par EBS par région AMIs	1
Étiquettes par ressource	45

Fonctionnement de Amazon Data Lifecycle Manager

Voici les éléments de base de Amazon Data Lifecycle Manager.

Eléments

- Politiques
- Planifications de politiques (politiques personnalisées uniquement)

- Balises de ressources cibles (politiques personnalisées uniquement)
- Instantanés
- Soutenu par EBS AMIs
- Balises Amazon Data Lifecycle Manager

Politiques

Avec Amazon Data Lifecycle Manager, vous créez des politiques pour définir vos exigences en matière de création et de conservation des sauvegardes. Ces politiques spécifient généralement les éléments suivants :

- Type de stratégie : définit le type de ressources de sauvegarde gérées par la politique (instantanés ou sauvegardés par EBS AMIs).
- Ressources cibles : définit le type de ressources ciblées par la politique (instances ou volumes EBS).
- Fréquence de création : définit la fréquence d'exécution de la politique et crée des instantanés ou AMIs.
- Seuil de rétention : définit la durée pendant laquelle la politique conserve les instantanés ou AMIs après leur création.
- Actions supplémentaires : définit les actions supplémentaires que la politique doit effectuer, comme la copie entre régions, l'archivage ou le balisage des ressources.

Amazon Data Lifecycle Manager propose des politiques par défaut et des politiques personnalisées.

Politiques par défaut

Les politiques par défaut sauvegardent tous les volumes et instances d'une région qui ne disposent pas de sauvegardes récentes. Vous pouvez éventuellement exclure des volumes et des instances en spécifiant des paramètres d'exclusion.

Amazon Data Lifecycle Manager prend en charge les politiques par défaut suivantes :

- Politique par défaut pour les instantanés EBS : cible les volumes et automatise la création, la conservation et la suppression des instantanés.
- Politique par défaut pour les instances soutenues par EBS AMIs : cible les instances et automatise la création, la conservation et le désenregistrement des instances soutenues par EBS. AMIs

Chaque compte et chaque Région AWS ne peuvent contenir qu'une seule politique par défaut par type de ressource.

Politiques personnalisées

Les politiques personnalisées ciblent des ressources spécifiques en fonction des balises qui leur sont attribuées et prennent en charge des fonctionnalités avancées, telles que la restauration rapide des instantanés, l'archivage des instantanés, la copie entre comptes et les pré-scripts et post-scripts. Une politique personnalisée peut inclure jusqu'à 4 planifications, chaque planification pouvant avoir sa propre fréquence de création, son propre seuil de conservation et sa propre configuration de fonctionnalités avancées.

Amazon Data Lifecycle Manager prend en charge les politiques personnalisées suivantes :

- Politique pour les instantanés EBS : cible les volumes ou les instances et automatise la création, la conservation et la suppression des instantanés EBS.
- Politique d'AMI basée sur EBS : cible les instances et automatise la création, la conservation et le désenregistrement des instances soutenues par EBS. AMIs
- Politique d'événement de copie entre comptes : automatise les actions de copie entre régions pour les instantanés partagés avec vous.

Pour de plus amples informations, veuillez consulter Politiques par défaut d'Amazon Data Lifecycle Manager et politiques personnalisées.

Planifications de politiques (politiques personnalisées uniquement)

Les calendriers des politiques définissent le moment où les instantanés AMIs sont créés ou sont créés par la politique. Les politiques peuvent comporter jusqu'à quatre planifications : une obligatoire et jusqu'à trois facultatives.

L'ajout de plusieurs programmes à une seule politique vous permet de créer des instantanés ou AMIs à des fréquences différentes en utilisant la même stratégie. Par exemple, vous pouvez créer une politique unique qui crée des instantanés quotidiens, hebdomadaires, mensuels et annuels. Cela vous évite de devoir gérer plusieurs politiques.

Pour chaque planification, vous pouvez définir la fréquence, les paramètres de restauration d'instantané rapide (politiques de cycle de vie des instantanés uniquement), les règles de copie entre régions et les balises. Les balises attribuées à un calendrier sont automatiquement attribuées aux

instantanés ou AMIs sont créées lorsque le calendrier est lancé. En outre, Amazon Data Lifecycle Manager attribue automatiquement une balise générée par le système en fonction de la fréquence de la planification à chaque instantané ou AMI.

Chaque planification est lancée individuellement en fonction de sa fréquence. Si plusieurs planifications sont lancées simultanément, Amazon Data Lifecycle Manager ne crée qu'un seul instantané ou une seule AMI et applique les paramètres de rétention de la planification dont la période de rétention est la plus élevée. Les balises de toutes les planifications lancées sont appliquées à l'instantané ou l'AMI.

- (Stratégies de cycle de vie des instantanés uniquement) Si la restauration d'instantané rapide est activée pour plusieurs planifications lancées, l'instantané est activé pour la restauration d'instantané rapide dans toutes les zones de disponibilité spécifiées parmi toutes les planifications lancées. Les paramètres de rétention les plus élevés des planifications lancées sont utilisés pour chaque zone de disponibilité.
- Si plusieurs des planifications lancées sont activées pour la copie entre régions, l'instantané ou l'AMI est copié dans toutes les régions spécifiées dans toutes les planifications lancées. La période de rétention la plus élevée des planifications lancées est appliquée.

Balises de ressources cibles (politiques personnalisées uniquement)

Les politiques personnalisées Amazon Data Lifecycle Manager utilisent des balises de ressource pour identifier les ressources à sauvegarder. Lorsque vous créez un instantané ou une politique d'AMI basée sur EBS, vous pouvez spécifier plusieurs balises de ressources cibles. Toutes les ressources du type spécifié (instance ou volume) qui ont au moins une des balises spécifiées seront retenues par la politique. Par exemple, si vous créez une politique d'instantané qui cible des volumes et que vous spécifiez `purpose=prod` `cost center=prod` et `environment=live` en tant que balises de ressources cibles, la politique ciblera tous les volumes qui possèdent l'une de ces paires clé-valeur de balise.

Si vous souhaitez exécuter plusieurs politiques sur une ressource, vous pouvez attribuer plusieurs balises à la ressource cible, puis créer des politiques distinctes qui ciblent chacune une balise de ressource spécifique.

Vous ne pouvez pas utiliser les caractères \ ou = dans une clé d'identification. Les balises de ressource cible sont sensibles à la casse. Pour plus d'informations, consultez la section Marquer vos ressources.

Instantanés

Les instantanés représentent le principal moyen de sauvegarde des données de vos volumes EBS. Afin d'économiser les frais de stockage, les instantanés successifs sont incrémentiels ; ils contiennent uniquement les données du volume ayant changé depuis l'instantané précédent. Lorsque vous supprimez un instantané dans une série d'instantanés d'un volume, seules les données figurant uniquement dans cet instantané sont supprimées. Le reste de l'historique de capture du volume est conservé. Pour de plus amples informations, veuillez consulter Instantanés Amazon EBS.

Soutenu par EBS AMIs

Une Amazon Machine Image (AMI) fournit les informations requises pour lancer une instance. Lorsque vous avez besoin de plusieurs instances configurées de manière identique, il est possible de lancer plusieurs instances à partir d'une même AMI. Amazon Data Lifecycle Manager prend uniquement en charge les solutions basées sur EBS. AMIs Les fichiers sauvegardés par EBS AMIs incluent un instantané pour chaque volume EBS attaché à l'instance source. Pour plus d'informations, consultez Amazon Machine Images (AMI).

Balises Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager applique les balises système suivantes à tous les instantanés AMIs créés par une politique, afin de les distinguer des instantanés AMIs créés par tout autre moyen :

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime` — Pour les instantanés créés selon une planification basée sur l'âge. Indique quand l'instantané doit être supprimé du niveau standard.
- `dlm:managed`
- `aws:dlm:archived` — Pour les instantanés archivés selon une planification.
- `aws:dlm:pre-script` : pour les instantanés créés à l'aide de pré-scripts.
- `aws:dlm:post-script` : pour les instantanés créés à l'aide de post-scripts.

Vous pouvez également spécifier des balises personnalisées à appliquer aux instantanés et AMIs lors de leur création. Vous ne pouvez pas utiliser les caractères \ ou = dans une clé d'identification.

Les balises cible utilisées par Amazon Data Lifecycle Manager pour associer des volumes à une politique d'instantanés peuvent éventuellement être appliquées aux instantanés créés par la politique.

De même, les balises cibles utilisées pour associer des instances à une politique AMI peuvent éventuellement être appliquées aux balises AMIs créées par la politique.

Politiques par défaut d'Amazon Data Lifecycle Manager et politiques personnalisées

Cette section compare les politiques par défaut et les politiques personnalisées et met en évidence leurs similitudes et leurs différences.

Rubriques

Comparaison des politiques d'instantanés EBS

Le tableau suivant met en évidence les différences entre la politique d'instantanés EBS par défaut et les politiques d'instantanés EBS personnalisées.

Fonctionnalité	Politique par défaut pour les instantanés EBS	Politique d'instantanés EBS personnalisée
Ressource de sauvegarde gérée	Instantané EBS	Instantané EBS
Types de ressources cibles	Volumes	Volumes ou instances
Ciblage des ressources	Cible tous les volumes de la région qui n'ont pas d'instantanés récents. Vous pouvez définir des paramètres d'exclusion pour exclure des volumes spécifiques.	Cible uniquement les volumes ou les instances dotés de balises spécifiqu es.
Paramètres d'exclusion	Oui, il est possible d'exclure des volumes de démarrage, des types de	Oui, il est possible d'exclure des volumes de démarrage et des

Fonctionnalité	Politique par défaut pour les instantanés EBS	Politique d'instantanés EBS personnalisée
	volumes spécifiques et des volumes dotés de balises spécifiques.	volumes dotés de balises spécifiques lors du ciblage des instances.
AWS Outposts de soutien	Non	Oui
Prise en charge de plusieurs planifications	Non	Oui, jusqu'à 4 planifications par politique
Types de conservation pris en charge	Conservation basée sur l'âge uniquement	Conservation basée sur l'âge et sur le nombre
Fréquence de création d'instantanés	Tous les 1 à 7 jours.	Fréquence quotidienne, hebdomadaire, mensuelle, annuelle ou personnalisée à l'aide d'une expression cron.
Conservation des instantanés	2 à 14 jours.	Jusqu'à 1 000 instantanés (basée sur le nombre) ou 100 ans (basée sur l'âge).
Prise en charge des instantanés cohérents par rapport à l'application	Non	Oui, en utilisant des pré-scripts et des post-scripts
Prise en charge de l'archivage des instantanés	Non	Oui
Prise en charge de la restauration d'instantané rapide	Non	Oui

Fonctionnalité	Politique par défaut pour les instantanés EBS	Politique d'instantanés EBS personnalisée
Prise en charge de la copie entre régions	Oui, avec les paramètres par défaut [1]	Oui, avec des paramètres personnalisés
Prise en charge du partage entre comptes	Non	Oui
Prise en charge de la suppression prolongée [2]	Oui	Non

[1] Pour les politiques par défaut :

- Vous ne pouvez pas copier les balises dans des copies entre régions.
- Les copies utilisent la même période de conservation que l'instantané source.
- Les copies ont le même état de chiffrement que l'instantané source. Si le chiffrement est activé par défaut dans la région de destination, les copies sont toujours chiffrées, même si les instantanés source ne sont pas chiffrés. Les copies sont toujours chiffrées avec la clé KMS par défaut pour la région de destination.

[2] Pour les politiques par défaut et personnalisées :

- Si une instance ou un volume cible est supprimé, Amazon Data Lifecycle Manager continue de supprimer les instantanés jusqu'au dernier, mais sans l'inclure, en se basant sur la période de conservation. Pour les politiques par défaut, vous pouvez étendre la suppression pour inclure le dernier instantané.
- Si une politique est supprimée ou passe à l'état d'erreur ou de désactivation, Amazon Data Lifecycle Manager arrête de supprimer les instantanés. Pour les politiques par défaut, vous pouvez étendre la suppression pour continuer de supprimer les instantanés, y compris le dernier.

Comparaison des politiques d'AMI basées sur EBS

Le tableau suivant met en évidence les différences entre la politique par défaut pour les politiques AMI basées sur EBS AMIs et les politiques AMI personnalisées soutenues par EBS.

Fonctionnalité	Politique par défaut pour EBS Backed AMIs	Politique d'AMI basées sur EBS personnalisée
Ressource de sauvegarde gérée	Soutenu par EBS AMIs	Soutenu par EBS AMIs
Types de ressources cibles	instances	instances
Ciblage des ressources	Cible toutes les instances de la région qui n'ont pas de version récente AMIs. Vous pouvez définir des paramètres d'exclusion pour exclure des instances spécifiques.	Cible uniquement les instances dotées de balises spécifiques.
Redémarrage des instances avant la création de l'AMI	Non	Oui
Paramètres d'exclusion	Oui, il est possible d'exclure des instances dotées de balises spécifiques.	Non
Prise en charge de plusieurs planifications	Non	Oui, jusqu'à 4 planifications par politique.
Fréquence de création des AMI	Tous les 1 à 7 jours.	Fréquence quotidienne, hebdomadaire, mensuelle, annuelle ou personnalisée à l'aide d'une expression cron.

Fonctionnalité	Politique par défaut pour EBS Backed AMIs	Politique d’AMI basées sur EBS personnalisée
Types de conservation pris en charge	Conservation basée sur l’âge uniquement.	Conservation basée sur l’âge et sur le nombre.
AMIs rétention	2 à 14 jours.	Jusqu'à 1 000 AMIs (en fonction du nombre) ou jusqu'à 100 ans (en fonction de l'âge).
Prise en charge de l’obsoles cence des AMI	Non	Oui
Prise en charge de la copie entre régions	Oui, avec les paramètres par défaut [1]	Oui, avec des paramètres personnal isés
Prise en charge de la suppressi on prolongée [2]	Oui	Non

[1] Pour les politiques par défaut :

- Vous ne pouvez pas copier les balises dans des copies entre régions.
- Les copies utilisent la même période de conservation que l’AMI source.
- Les copies ont le même état de chiffrement que l’AMI source. Si le chiffrement est activé par défaut dans la région de destination, les copies sont toujours chiffrées, même si la source AMIs n'est pas chiffrée. Les copies sont toujours chiffrées avec la clé KMS par défaut pour la région de destination.

[2] Pour les politiques par défaut et personnalisées :

- Si une instance ciblée est résiliée, Amazon Data Lifecycle Manager continue de se désinscrire AMIs jusqu'à la dernière instance en fonction de la période de rétention, mais sans inclure cette

dernière instance. Pour les politiques par défaut, vous pouvez étendre l'annulation de l'inscription pour inclure la dernière AMI.

- Si une politique est supprimée ou passe à l'état d'erreur ou de désactivation, Amazon Data Lifecycle Manager arrête le désenregistrement AMIs. Pour les politiques par défaut, vous pouvez étendre la suppression pour poursuivre le désenregistrement AMIs, y compris le dernier.

Création des politiques par défaut d'Amazon Data Lifecycle Manager

Pour créer des instances périodiques basées sur EBS, utilisez AMIs la politique par défaut pour les instances basées sur EBS. AMIs Pour créer des instantanés de tous les volumes, quel que soit leur état d'attachement, ou si vous souhaitez exclure des volumes spécifiques, utilisez la politique par défaut pour les instantanés EBS.

Cette section explique comment créer des politiques par défaut.

Rubriques

Considérations relatives aux politiques par défaut

Gardez ce qui suit à l'esprit lorsque vous utilisez des politiques par défaut :

- Les politiques par défaut ne sauvegardent pas les ressources cibles (instances ou volumes) qui ont fait l'objet de sauvegardes récentes (instantanés ou AMIs). La fréquence de création détermine les ressources sauvegardées. Un volume ou une instance n'est sauvegardé que si son dernier instantané ou sa dernière AMI date d'avant la fréquence de création de la politique. Par exemple, si vous spécifiez une fréquence de création de 3 jours, la politique par défaut pour les instantanés EBS créera un instantané d'un volume uniquement si le dernier instantané date de plus de 3 jours.
- Par défaut, les politiques par défaut ciblent toutes les instances ou tous les volumes de la région, sauf si des paramètres d'exclusion sont spécifiés.

- Les politiques par défaut créeront un ensemble minimal d'instantanés uniques. Par exemple, si vous activez la politique AMI basée sur EBS et la politique d'instantanés EBS, la politique d'instantanés ne dupliquera pas les instantanés de volumes déjà sauvegardés par la politique d'AMI basées sur EBS.
- Les politiques par défaut ne commenceront à cibler que les ressources datant d'au moins 24 heures.
- Si vous supprimez un volume ou mettez fin à une instance ciblée par une politique par défaut, Amazon Data Lifecycle Manager continuera à supprimer les sauvegardes créées précédemment (snapshots ou AMIs) conformément à la période de conservation allant jusqu'à la dernière sauvegarde, mais sans inclure celle-ci. Vous devez supprimer manuellement cette sauvegarde si elle n'est pas nécessaire.

  Si vous souhaitez qu'Amazon Data Lifecycle Manager supprime la dernière sauvegarde, vous pouvez activer la suppression étendue.
- Si une politique par défaut est supprimée ou passe à l'état d'erreur ou de désactivation, Amazon Data Lifecycle Manager arrête de supprimer les sauvegardes créées précédemment (snapshots ou AMIs). Si vous souhaitez qu'Amazon Data Lifecycle Manager continue de supprimer des sauvegardes, y compris la dernière, vous devez activer la suppression étendue avant de supprimer la politique ou avant que la politique ne passe à l'état de désactivation ou de suppression.
- Lorsque vous créez et activez une politique par défaut, Amazon Data Lifecycle Manager affecte de manière aléatoire des ressources ciblées à une fenêtre horaire de quatre heures. Les ressources ciblées sont sauvegardées pendant la fenêtre qui leur est attribuée à la fréquence de création spécifiée. Par exemple, si une politique a une fréquence de création de 3 jours et que la fenêtre 12 h 00 – 16 h 00 est attribuée à une ressource cible, cette ressource sera sauvegardée entre 12 h 00 et 16 h 00 tous les 3 jours.

Création d'une politique par défaut pour les instantanés Amazon EBS

La procédure suivante vous explique comment créer une politique par défaut pour les instantanés EBS.

Console

Pour créer une politique par défaut pour les instantanés EBS

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.

2. Dans le volet de navigation, sélectionnez Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie.
3. Pour Type de stratégie, choisissez Stratégie par défaut, puis Politique d'instantané EBS.
4. Pour Description, saisissez une brève description pour la stratégie.
5. Pour Rôle IAM, sélectionnez le rôle IAM disposant d'autorisations pour gérer les instantanés.

   Nous vous recommandons de choisir Par défaut pour utiliser le rôle IAM par défaut fourni par Amazon Data Lifecycle Manager. Toutefois, vous pouvez également utiliser un rôle IAM personnalisé que vous avez créé précédemment.
6. Pour Fréquence de création, spécifiez la fréquence à laquelle vous souhaitez que la politique s'exécute et crée des instantanés de vos volumes.

   La fréquence que vous spécifiez détermine également les volumes sauvegardés. La politique ne sauvegardera que les volumes qui n'ont pas été sauvegardés par un autre moyen selon la fréquence spécifiée. Par exemple, si vous spécifiez une fréquence de création de 3 jours, la politique créera uniquement des instantanés des volumes qui n'ont pas été sauvegardés au cours des 3 derniers jours.
7. Pour Période de conservation, spécifiez la durée pendant laquelle vous souhaitez que la politique conserve les instantanés qu'elle crée. Lorsqu'un instantané atteint le seuil de conservation, il est automatiquement supprimé. La période de conservation doit être supérieure ou égale à la fréquence de création.
8. (Facultatif) Configurez les Paramètres d'exclusion pour exclure des volumes spécifiques des sauvegardes planifiées. Les volumes exclus ne seront pas sauvegardés lors de l'exécution de la politique.

   a. Pour exclure les volumes de démarrage, sélectionnez Exclure les volumes de démarrage. Si vous excluez les volumes de démarrage, seuls les volumes de données (autres que les volumes de démarrage) seront sauvegardés conformément à la politique. En d'autres termes, la politique ne créera pas d'instantanés des volumes attachés à des instances en tant que volume de démarrage.
   b. Pour exclure des types de volumes spécifiques, choisissez Exclure des types de volumes spécifiques, puis sélectionnez les types de volumes à exclure. Seuls les volumes des types restants seront sauvegardés par la politique.
   c. Pour exclure les volumes dotés de balises spécifiques, choisissez Ajouter une balise, puis spécifiez les clés et les valeurs des balises. La politique ne créera pas d'instantanés des volumes qui ont l'une des balises spécifiées.

9. (Facultatif) Dans les Paramètres avancés, spécifiez les actions supplémentaires que la politique doit effectuer.

   a. Pour copier les balises attribuées des volumes source vers leurs instantanés, sélectionnez Copier les balises depuis les volumes.

   b. Lorsque l'option Étendre la suppression est désactivée :

      - Si un volume source est supprimé, Amazon Data Lifecycle Manager continue de supprimer les instantanés précédemment créés jusqu'au dernier, mais sans l'inclure, en se basant sur la période de conservation. Si vous souhaitez qu'Amazon Data Lifecycle Manager supprime tous les instantanés, y compris le dernier, sélectionnez Étendre la suppression.
      - Si une politique est supprimée ou passe à l'état `error` ou `disabled`, Amazon Data Lifecycle Manager arrête de supprimer les instantanés. Si vous souhaitez qu'Amazon Data Lifecycle Manager continue de supprimer les instantanés, y compris le dernier, sélectionnez Étendre la suppression.

      > **Note**
      >
      > Si vous activez la suppression étendue, vous remplacez simultanément les deux comportements décrits ci-dessus.

   c. Pour copier les instantanés créés par la politique vers d'autres régions, sélectionnez Créer une copie entre régions, puis sélectionnez jusqu'à 3 régions de destination.

      - Si l'instantané source est chiffré ou si le chiffrement par défaut est activé pour la région de destination, les instantanés copiés sont chiffrés à l'aide de la clé KMS par défaut pour le chiffrement EBS dans la région de destination.
      - Si l'instantané source n'est pas chiffré et que le chiffrement par défaut est désactivé pour la région de destination, les instantanés copiés ne sont pas chiffrés.

10. (Facultatif) Pour ajouter une balise à la politique, choisissez Ajouter une balise et saisissez la paire de clé et de valeur de la balise.

11. Choisissez Créer une politique par défaut.

> **Note**
>
> Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consultez Résoudre les problèmes liés à Amazon Data Lifecycle Manager pour plus d'informations.

AWS CLI

Pour créer une politique par défaut pour les instantanés EBS

Utilisez la commande create-lifecycle-policy. Vous pouvez spécifier les paramètres de la requête selon l'une des deux méthodes suivantes, en fonction de votre cas d'utilisation ou de vos préférences :

- Méthode 1 :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeBootVolumes=true | false,
 ExcludeTags=[{Key=tag_key,Value=tag_value}], ExcludeVolumeTypes="standard | gp2 |
 gp3 | io1 | io2 | st1 | sc1"
```

Par exemple, pour créer une politique par défaut pour les instantanés EBS qui cible tous les volumes de la région, qui utilise le rôle IAM par défaut, qui s'exécute quotidiennement (par défaut) et qui conserve les instantanés pendant 7 jours (par défaut), vous devez spécifier les paramètres suivants :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default snapshot policy" \
```

```
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRole \
--default-policy VOLUME
```

- Méthode 2 :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--policy-details file://policyDetails.json
```

Où `policyDetails.json` inclut les éléments suivants :

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceType": "VOLUME",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
    "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeBootVolume": true | false,
  "ExcludeVolumeTypes": ["standard | gp2 | gp3 | io1 | io2 | st1 | sc1"],
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Créer une politique par défaut pour EBS Backed AMIs

La procédure suivante explique comment créer une politique par défaut pour EBS Based AMIs.

Console

Pour créer une politique par défaut pour EBS Backed AMIs

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie.
3. Pour Type de stratégie, choisissez Stratégie par défaut, puis Politique d'AMI basée sur volume EBS.
4. Pour Description, saisissez une brève description pour la stratégie.
5. Pour le rôle IAM, choisissez le rôle IAM qui dispose des autorisations de gestion. AMIs

   Nous vous recommandons de choisir Par défaut pour utiliser le rôle IAM par défaut fourni par Amazon Data Lifecycle Manager. Toutefois, vous pouvez également utiliser un rôle IAM personnalisé que vous avez créé précédemment.
6. Pour Fréquence de création, spécifiez la fréquence à laquelle vous souhaitez que la politique soit exécutée et créée AMIs à partir de vos instances.

   La fréquence que vous spécifiez détermine également les instances sauvegardées. La politique ne sauvegardera que les instances qui n'ont pas été sauvegardées par un autre moyen selon la fréquence spécifiée. Par exemple, si vous spécifiez une fréquence de création de 3 jours, la politique ne sera créée qu' AMIs à partir d'instances qui n'ont pas été sauvegardées au cours des 3 derniers jours.
7. Pour Période de conservation, spécifiez la durée pendant laquelle vous souhaitez AMIs que la politique conserve ce qu'elle crée. Lorsqu'une AMI atteint le seuil de conservation, son inscription est automatiquement annulée et ses instantanés associés sont supprimés. La période de conservation doit être supérieure ou égale à la fréquence de création.
8. (Facultatif) Configurez les Paramètres d'exclusion pour exclure des instances spécifiques des sauvegardes planifiées. Les instances exclues ne seront pas sauvegardées lors de l'exécution de la politique.

   - Pour exclure les instances dotées de balises spécifiques, choisissez Ajouter une balise, puis spécifiez les clés et les valeurs des balises. La politique ne sera pas créée AMIs à partir d'instances possédant l'une des balises spécifiées.
9. (Facultatif) Dans les Paramètres avancés, spécifiez les actions supplémentaires que la politique doit effectuer.

a. Pour copier les balises attribuées depuis les instances source vers leurs instances AMIs, sélectionnez Copier les balises depuis les instances.

b. Lorsque l'option Étendre la suppression est désactivée :

- Si une instance source est résiliée, Amazon Data Lifecycle Manager continue de désenregistrer la dernière instance AMIs créée précédemment, mais sans inclure, la dernière en fonction de la période de rétention. Si vous souhaitez qu'Amazon Data Lifecycle Manager annule tous les enregistrements AMIs, y compris le dernier, sélectionnez Étendre la suppression.
- Si une politique est supprimée ou passe à l'`disabled`état `error` ou, Amazon Data Lifecycle Manager arrête de se AMIs désinscrire. Si vous souhaitez qu'Amazon Data Lifecycle Manager continue à se désinscrire AMIs, y compris le dernier, sélectionnez Étendre la suppression.

> **Note**
>
> Si vous activez la suppression étendue, vous remplacez simultanément les deux comportements décrits ci-dessus.

c. Pour copier la AMIs création créée par la politique vers d'autres régions, sélectionnez Créer une copie interrégionale, puis sélectionnez jusqu'à 3 régions de destination.

- Si l'AMI source est chiffrée ou si le chiffrement est activé par défaut pour la région de destination, les copies AMIs sont chiffrées à l'aide de la clé KMS par défaut pour le chiffrement EBS dans la région de destination.
- Si l'AMI source n'est pas chiffrée et que le chiffrement est désactivé par défaut pour la région de destination, les copies ne AMIs sont pas chiffrées.

10. (Facultatif) Pour ajouter une balise à la politique, choisissez Ajouter une balise et saisissez la paire de clé et de valeur de la balise.
11. Choisissez Créer une politique par défaut.

> **Note**
>
> Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already`

`exists`, consultez Résoudre les problèmes liés à Amazon Data Lifecycle Manager pour plus d'informations.

AWS CLI

Pour créer une politique par défaut pour EBS Backed AMIs

Utilisez la commande create-lifecycle-policy. Vous pouvez spécifier les paramètres de la requête selon l'une des deux méthodes suivantes, en fonction de votre cas d'utilisation ou de vos préférences :

- Méthode 1 :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeTags=[{Key=tag_key,Value=tag_value}]
```

Par exemple, pour créer une politique par défaut pour EBS AMIs qui cible toutes les instances de la région, utilise le rôle IAM par défaut, s'exécute quotidiennement (par défaut) et est conservée AMIs pendant 7 jours (par défaut), vous devez spécifier les paramètres suivants :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default AMI policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--default-policy INSTANCE
```

- Méthode 2 :

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
```

```
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--policy-details file://policyDetails.json
```

Où `policyDetails.json` inclut les éléments suivants :

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceType": "INSTANCE",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
 "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

Activez les politiques par défaut de Data Lifecycle Manager pour tous les comptes et toutes les régions

Vous pouvez ainsi activer les politiques par défaut d'Amazon Data Lifecycle Manager sur plusieurs comptes et AWS régions en une seule opération. AWS CloudFormation StackSets

Vous pouvez utiliser des ensembles de piles pour activer les politiques par défaut de l'une des manières suivantes :

- Au sein d'une AWS organisation : garantit que les politiques par défaut sont activées et configurées de manière cohérente dans AWS l'ensemble de l'organisation ou dans des unités organisationnelles spécifiques d'une organisation. Cela se fait à l'aide d'autorisations gérées par le service. AWS CloudFormation StackSets crée les rôles IAM requis en votre nom.
- Sur des AWS comptes spécifiques : garantit que les politiques par défaut sont activées et configurées de manière cohérente sur des comptes cibles spécifiques. Cela nécessite des

autorisations autogérées. Vous créez les rôles IAM nécessaires pour établir la relation de confiance entre le compte administrateur du stack set et les comptes cibles.

Pour plus d'informations, consultez la section Modèles d'autorisation pour les ensembles de piles dans le Guide de AWS CloudFormation l'utilisateur.

Utilisez les procédures suivantes pour activer les politiques par défaut d'Amazon Data Lifecycle Manager dans AWS l'ensemble de l'organisation OUs, sur des comptes cibles spécifiques ou spécifiques.

Prérequis

Procédez de l'une des manières suivantes, en fonction de la manière dont vous activez les politiques par défaut :

- (Dans toutes AWS les organisations) Vous devez activer toutes les fonctionnalités de votre organisation et activer l'accès sécurisé avec AWS Organizations. Vous devez également utiliser le compte de gestion de l'organisation ou un compte d'administrateur délégué.
- (Pour des comptes cibles spécifiques) Vous devez accorder des autorisations autogérées en créant les rôles nécessaires pour établir une relation de confiance entre le compte administrateur du stack set et les comptes cibles.

Console

Pour activer les politiques par défaut au sein d'une AWS organisation ou pour des comptes cibles spécifiques

1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation.
2. Dans le volet de navigation, choisissez StackSets, puis choisissez Create StackSet.
3. Pour les autorisations, effectuez l'une des opérations suivantes, en fonction de la manière dont vous activez les politiques par défaut :
   - (Au sein d'une AWS organisation) Choisissez les autorisations gérées par le service.
   - (Sur des comptes cibles spécifiques) Choisissez les autorisations en libre-service. Ensuite, pour l'ARN du rôle d'administrateur IAM, sélectionnez le rôle de service IAM que vous avez créé pour le compte administrateur, et pour le nom du rôle d'exécution IAM, entrez le nom du rôle de service IAM que vous avez créé dans les comptes cibles.

4. Pour Préparer le modèle, choisissez Utiliser un exemple de modèle.
5. Pour les exemples de modèles, effectuez l'une des opérations suivantes :
   - (Politique par défaut pour les instantanés EBS) Sélectionnez Create Amazon Data Lifecycle Manager politiques par défaut pour les instantanés EBS.
   - (Politique par défaut pour EBS AMIs) Sélectionnez Create Amazon Data Lifecycle Manager politiques par défaut pour EBS Based. AMIs
6. Choisissez Suivant.
7. Pour StackSet le nom et StackSet la description, entrez un nom descriptif et une brève description.
8. Dans la section Paramètres, configurez les paramètres de politique par défaut selon vos besoins.

   > **Note**
   >
   > Pour les charges de travail critiques, nous CreateInterval recommandons 1 jour et RetainInterval 7 jours.

9. Choisissez Suivant.
10. (Facultatif) Pour les balises, spécifiez des balises pour vous aider à identifier StackSet et à empiler les ressources.
11. Pour Exécution gérée, choisissez Active.
12. Choisissez Suivant.
13. Pour Add stacks to stack set (Ajouter des piles à un ensemble de piles), sélectionnez Deploy new stacks (Déployer de nouvelles piles).
14. Procédez de l'une des manières suivantes, en fonction de la manière dont vous activez les politiques par défaut :
    - (Dans AWS l'ensemble de l'organisation) Pour les cibles de déploiement, choisissez l'une des options suivantes :
      - Pour déployer dans l'ensemble d'une AWS organisation, choisissez Déployer dans l'organisation.
      - Pour effectuer un déploiement vers des unités organisationnelles (UO) spécifiques, choisissez Déployer vers des unités organisationnelles, puis saisissez l'ID de l'UO dans

le champ ID de l'unité organisationnelle. Pour en ajouter d'autresOUs, choisissez Ajouter une autre UO.

- (Sur des comptes cibles spécifiques) Pour les comptes, effectuez l'une des opérations suivantes :
  - Pour effectuer un déploiement sur des comptes cibles spécifiques, choisissez Déployer des piles dans les comptes, puis pour les numéros IDs de compte, entrez les comptes cibles.
  - Pour effectuer le déploiement sur tous les comptes d'une unité organisationnelle spécifique, choisissez Déployer la pile sur tous les comptes d'une unité organisationnelle, puis dans Numéros d'organisation, entrez l'ID de l'unité d'organisation cible.

15. Pour le déploiement automatique, choisissez Activé.
16. Pour le comportement de suppression du compte, choisissez Conserver les piles.
17. Pour Spécifier les régions, sélectionnez les régions spécifiques dans lesquelles vous souhaitez activer les politiques par défaut, ou choisissez Ajouter toutes les régions pour activer les politiques par défaut dans toutes les régions.
18. Choisissez Suivant.
19. Passez en revue les paramètres du stack set, sélectionnez Je reconnais que cela AWS CloudFormation pourrait créer des ressources IAM, puis choisissez Soumettre.

AWS CLI

Pour activer les politiques par défaut au sein d'une AWS organisation

1. Créez l'ensemble de piles. Utilisez la commande create-stack-set.

   Pour `--permission-model`, spécifiez `SERVICE_MANAGED`.

   Pour`--template-url`, spécifiez l'un des modèles suivants URLs :

   - (Politiques par défaut pour EBS Backed AMIs) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
   - (Politiques par défaut pour les instantanés EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

Pour `--parameters`, spécifiez les paramètres des politiques par défaut. Pour connaître les paramètres pris en charge, les descriptions des paramètres et les valeurs valides, téléchargez le modèle à l'aide de l'URL, puis visualisez-le à l'aide d'un éditeur de texte.

Pour `--auto-deployment`, spécifiez `Enabled=true, RetainStacksOnAccountRemoval=true`.

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--permission-model SERVICE_MANAGED \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Déployez le stack set. Utilisez la commande create-stack-instances.

   Pour `--stack-set-name`, spécifiez le nom de l'ensemble de piles que vous avez créé à l'étape précédente.

   Pour `--deployment-targets OrganizationalUnitIds`, spécifiez l'ID de l'unité d'organisation racine à déployer dans l'ensemble d'une organisation, ou l'unité d'organisation IDs à déployer OUs dans une organisation spécifique.

   Pour `--regions`, spécifiez les AWS régions dans lesquelles vous souhaitez activer les politiques par défaut.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--deployment-targets OrganizationalUnitIds='["root_ou_id"]' | '["ou_id_1",
 "ou_id_2]' \
--regions '["region_1", "region_2"]'
```

Pour activer les politiques par défaut sur des comptes cibles spécifiques

1. Créez l'ensemble de piles. Utilisez la commande create-stack-set.

   Pour `--template-url`, spécifiez l'un des modèles suivants URLs :

- (Politiques par défaut pour EBS Backed AMIs) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`
- (Politiques par défaut pour les instantanés EBS) `https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml`

Pour `--administration-role-arn`, spécifiez l'ARN du rôle de service IAM que vous avez créé précédemment pour l'administrateur du stack set.

Pour `--execution-role-name`, spécifiez le nom du rôle de service IAM que vous avez créé dans les comptes cibles.

Pour `--parameters`, spécifiez les paramètres des politiques par défaut. Pour connaître les paramètres pris en charge, les descriptions des paramètres et les valeurs valides, téléchargez le modèle à l'aide de l'URL, puis visualisez-le à l'aide d'un éditeur de texte.

Pour `--auto-deployment`, spécifiez `Enabled=true, RetainStacksOnAccountRemoval=true`.

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
--administration-role-arn administrator_role_arn \
--execution-role-name target_account_role \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. Déployez le stack set. Utilisez la commande create-stack-instances.

Pour `--stack-set-name`, spécifiez le nom de l'ensemble de piles que vous avez créé à l'étape précédente.

Pour `--accounts`, spécifiez IDs les AWS comptes cibles.

Pour `--regions`, spécifiez les AWS régions dans lesquelles vous souhaitez activer les politiques par défaut.

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--accounts '["account_ID_1","account_ID_2"]' \
--regions '["region_1", "region_2"]'
```

Création d'une politique personnalisée Amazon Data Lifecycle Manager pour les instantanés EBS

La procédure suivante montre comment utiliser Amazon Data Lifecycle Manager pour automatiser les cycles de vie des instantanés Amazon EBS.

Rubriques

Pour créer une stratégie de cycle de vie d'instantané

Suivez l'une des procédures suivantes pour créer une politique de cycle de vie des instantanés.

Console

Pour créer une politique d'instantané

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans la page Sélectionner un type de stratégie, choisissez Stratégie d'instantané EBS, puis Suivant.

4. Dans la section Ressources cibles, effectuez les opérations suivantes :

   a. Pour Types de ressource cibles, choisissez le type de ressource à sauvegarder. Sélectionnez `Volume` pour créer des instantanés de volumes individuels, ou `Instance` pour créer des instantanés multi-volume à partir des volumes d'une instance.

   b. (Clients de AWS l'avant-poste et de la zone locale uniquement) Spécifiez où se trouvent les ressources cibles.

      Pour Emplacement de la ressource cible, spécifiez l'emplacement des ressources cibles.

      - Pour cibler les ressources d'une région, sélectionnez AWS Région. Amazon Data Lifecycle Manager sauvegardera toutes les ressources du type spécifié qui ont des balises cibles correspondantes dans la région actuelle uniquement. Les instantanés sont créés dans la même région.
      - Pour cibler les ressources dans les zones locales, choisissez AWS Local Zones. Amazon Data Lifecycle Manager sauvegardera toutes les ressources du type spécifié qui ont des balises cibles correspondantes dans toutes les Zones Locales de la région actuelle uniquement. Les instantanés peuvent être créés dans la même zone locale que la ressource source ou dans sa région parente.
      - Pour cibler les ressources de vos Outposts, choisissez AWS Outpost. Amazon Data Lifecycle Manager sauvegardera toutes les ressources du type spécifié qui ont des balises cibles correspondantes dans tous les Outposts de votre compte. Les instantanés peuvent être créés dans le même avant-poste que la ressource source ou dans sa région parente.

   c. Pour Etiquettes de ressources cibles, choisissez les étiquettes de ressources qui identifient les volumes ou les instances à sauvegarder. Seules les ressources qui ont la clé de balise et les paires de valeurs spécifiées sont sauvegardées par la politique.

5. Pour Description, saisissez une brève description pour la stratégie.

6. Pour Rôle IAM, choisissez le rôle IAM autorisé à gérer des instantanés, ainsi qu'à décrire des volumes et des instances. Pour utiliser le rôle par défaut fourni par Amazon Data Lifecycle Manager, choisissez Rôle par défaut. Autrement, pour utiliser un rôle IAM personnalisé que vous avez créé précédemment, sélectionnez Choisir un autre rôle, puis sélectionnez le rôle à utiliser.

7. Pour Etiquettes de stratégie, ajoutez les étiquettes à appliquer à la stratégie de cycle de vie. Vous pouvez utiliser ces étiquettes pour identifier et catégoriser vos politiques.

8. Pour Policy status (Statut de la politique), choisissez Enable (Activer) pour lancer l'exécution de la politique à la prochaine heure planifiée, ou Disable policy (Désactiver la politique) pour empêcher l'exécution de la politique. Si vous n'activez pas la politique maintenant, elle ne commencera à créer des instantanés que quand vous l'aurez activée manuellement après sa création.
9. (Politiques qui ciblent uniquement les instances) Excluez les volumes des ensembles d'instantanés multi-volumes.

   Par défaut, Amazon Data Lifecycle Manager créera des instantanés de tous les volumes attachés aux instances ciblées. Cependant, vous pouvez choisir de créer des instantanés d'un sous-ensemble des volumes attachés. Dans la section Parameters (Paramètres), procédez comme suit :

   - Si vous ne voulez pas créer d'instantanés des volumes racines attachés aux instances ciblées, sélectionnez Exclude root volume (Exclure le volume racine). Si vous sélectionnez cette option, seuls les volumes de données (non racine) attachés aux instances ciblées seront inclus dans les ensembles instantanés multi-volumes.
   - Si vous voulez créer des instantanés d'un sous-ensemble de volumes de données (non racine) attachés aux instances ciblées, sélectionnez Exclude specific data volumes (Exclure des volumes de données spécifiques), puis spécifiez les identifications à utiliser pour identifier les volumes de données qui ne doivent pas faire l'objet d'un instantané. Amazon Data Lifecycle Manager ne créera pas d'instantanés des volumes de données qui ont l'une des identifications spécifiées. Amazon Data Lifecycle Manager créera uniquement des instantanés des volumes de données qui n'ont aucune des identifications spécifiées.
10. Choisissez Suivant.
11. Dans l'écran Configurer une planification, configurez les planifications de stratégie. Une politique peut avoir jusqu'à 4 planifications. La planification 1 est obligatoire. Les planifications 2, 3 et 4 sont facultatives. Pour chaque planification de politique que vous ajoutez, procédez comme suit :

    a. Dans la section Détails de la planification, procédez comme suit :

       i. Pour Nom de la planification, spécifiez un nom descriptif pour la planification.

       ii. Pour Fréquence et les champs associés, configurez l'intervalle entre les exécutions de stratégie.

Vous pouvez configurer les exécutions de politique selon une planification quotidienne, hebdomadaire, mensuelle ou annuelle. Vous pouvez également sélectionner Expression cron personnalisée pour spécifier un intervalle allant jusqu'à un an. Pour plus d'informations, consultez les sections Cron et rate dans le guide de l' EventBridge utilisateur Amazon.

> **Note**
>
> Si vous devez activer l'archivage des instantanés pour la planification, vous devez sélectionner la fréquence mensuelle ou annuelle, ou vous devez spécifier une expression cron avec une fréquence de création d'au moins 28 jours.
> Si vous spécifiez une fréquence mensuelle qui crée des instantanés un jour spécifique d'une semaine spécifique (par exemple, le deuxième jeudi du mois), alors pour une planification basée sur le nombre, le nombre de rétention du niveau d'archivage doit être de 4 ou plus.

iii. Pour Démarrage à, spécifiez l'heure de démarrage planifiée des exécutions de la stratégie. La première exécution de politique commence dans l'heure qui suit l'heure programmée. L'heure doit être au format UTC `hh:mm`.

iv. Pour Type de rétention, spécifiez la stratégie de rétention des instantanés créés par la planification.

Vous pouvez retenir les instantanés en fonction de leur nombre total ou de leur âge.

- Rétention basée sur le nombre
  - Lorsque l'archivage des instantanés est désactivé, la plage s'étend de 1 à `1000`. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage.
  - Lorsque l'archivage des instantanés est activé, la plage s'étend de `0` (archiver immédiatement après la création) à `1000`. Une fois le seuil de rétention du niveau standard atteint, l'instantané est converti en instantané complet et est déplacé vers le niveau d'archivage.
- Rétention basée sur l'âge

- Lorsque l'archivage des instantanés est désactivé, la plage s'étend de 1 jour à 100 ans. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage.
- Lorsque l'archivage des instantanés est activé, la plage s'étend de 0 jour (archivage immédiat après la création) à 100 ans. Une fois le seuil de rétention du niveau standard atteint, l'instantané est converti en instantané complet et est déplacé vers le niveau d'archivage.

> **Note**
>
> - Toutes les planifications doivent avoir le même type de rétention (basé sur l'âge ou sur le nombre). Vous pouvez spécifier le type de conservation pour la planification 1 uniquement. Les planifications 2, 3 et 4 héritent du type de conservation de la planification 1. Chaque planification peut avoir son propre nombre ou sa propre période de conservation.
> - Si vous activez la restauration rapide des instantanés, la copie inter-régions ou le partage d'instantanés, vous devez spécifier un nombre de rétention de 1 ou plus, ou une durée de conservation de 1 jour ou plus.

v. (AWS Outposts et uniquement pour les clients de la zone locale) Spécifiez la destination du cliché.

Pour Destination des instantanés, spécifiez la destination des instantanés créés par la politique.

- Si la politique cible les ressources d'une région, les instantanés doivent être créés dans la même région. AWS La région est sélectionnée pour vous.
- Si la politique cible les ressources d'une zone locale, vous pouvez créer des instantanés dans la même zone locale que la ressource source ou dans sa région parent.
- Si la politique cible les ressources d'un avant-poste, vous pouvez créer des instantanés sur le même avant-poste que la ressource source, ou dans sa région parente.

b. Configurez le balisage pour les instantanés.

Dans la section Etiquetage, procédez comme suit :

i. Pour copier toutes les étiquettes définies par l'utilisateur à partir du volume source vers les instantanés créés par la planification, sélectionnez Copier les étiquettes à partir de la source.

ii. Pour spécifier des étiquettes supplémentaires à attribuer aux instantanés créés par cette planification, choisissez Ajouter des étiquettes.

c. Configurez les scripts pré-scripts et les post-scripts pour des instantanés cohérents avec les applications.

Pour de plus amples informations, veuillez consulter Automatisez les instantanés cohérents avec les applications avec Data Lifecycle Manager.

d. (Politiques ciblant uniquement les volumes) Configurez l'archivage des instantanés.

Dans la section Archivage des instantanés, procédez comme suit :

> **Note**
>
> Vous ne pouvez activer l'archivage des instantanés que pour une seule planification dans une politique.

i. Pour activer l'archivage des instantanés pour la planification, sélectionnez Archive snapshots created by this schedule (Instantanés d'archives créés selon cette planification).

> **Note**
>
> Vous pouvez activer l'archivage des instantanés uniquement si la fréquence de création des instantanés est mensuelle ou annuelle, ou si vous spécifiez une expression cron avec une fréquence de création d'au moins 28 jours.

ii. Spécifiez la règle de rétention pour les instantanés dans le niveau d'archivage.

- Pour les planifications basées sur le nombre, spécifiez le nombre d'instantanés à retenir dans le niveau d'archivage. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage. Par exemple, si vous spécifiez le chiffre 3, la planification retiendra un maximum de 3 instantanés dans le niveau d'archivage. Lorsque le quatrième instantané est

archivé, le plus ancien des trois instantanés existants dans le niveau d'archivage est supprimé.

- Pour les planifications basées sur l'âge, spécifiez la période pour laquelle il convient de retenir les instantanés dans le niveau d'archivage. Lorsque le seuil de rétention est atteint, l'instantané le plus ancien est définitivement supprimé du niveau d'archivage. Par exemple, si vous spécifiez une période de 120 jours, la planification supprimera automatiquement les instantanés du niveau d'archivage lorsqu'ils atteignent cet âge.

> **Important**
>
> La période de rétention minimale pour les instantanés archivés est de 90 jours. Vous devez spécifier une règle de rétention qui retient l'instantané pendant au moins 90 jours.

e. Activez la restauration rapide des instantanés.

Pour activer la restauration rapide des instantanés créés par la planification, dans la section Restauration d'instantané rapide, sélectionnez Activer la restauration d'instantané rapide. Si vous activez la restauration d'instantané rapide, vous devez choisir les zones de disponibilité dans lesquelles le faire. Si la planification utilise une planification de rétention basée sur l'âge, vous devez spécifier la période pendant laquelle activer la restauration d'instantané rapide pour chaque instantané. Si la planification utilise une rétention basée sur le nombre, vous devez spécifier le nombre maximum d'instantanés à activer pour la restauration d'instantané rapide.

Si la stratégie crée des instantanés sur un Outpost, vous ne pouvez pas activer la restauration d'instantané rapide. La restauration d'instantané rapide n'est pas prise en charge avec les instantanés locaux stockés sur un Outpost.

> **Note**
>
> Vous êtes facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée pour un instantané dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure.

f. Configurez la copie entre régions.

Pour copier les instantanés créés par la planification vers un Outpost ou une autre région, dans la section Copie entre régions, sélectionnez Activer de la copie entre régions.

Si la stratégie crée des instantanés dans une région, vous pouvez copier ceux-ci vers jusqu'à trois Outposts ou régions supplémentaires dans votre compte. Vous devez spécifier une règle de copie entre Régions distincte pour chaque Région ou Outpost de destination.

Pour chaque Région ou Outpost, vous pouvez choisir différentes politiques de conservation et indiquer s'il convient de copier toutes les balises ou de n'en copier aucune. Si l'instantané source est chiffré ou si le chiffrement par défaut est activé, les instantanés copiés sont chiffrés. Si l'instantané source n'est pas chiffré, vous pouvez activer le chiffrement. Si vous ne spécifiez pas de clé KMS, les instantanés sont chiffrés à l'aide de la clé KMS par défaut pour le chiffrement EBS dans chaque région de destination. Si vous spécifiez une clé KMS pour la Région de destination, le rôle IAM sélectionné doit avoir accès à la clé KMS.

> **Note**
>
> Vous devez vous assurer que vous ne dépassez pas le nombre de copies d'instantanés simultanées par région.

Si la politique crée des instantanés sur un Outpost, vous ne pouvez pas les copier dans une Région ou un autre Outpost et les paramètres de copie inter-régions ne sont pas disponibles.

g. Configurez le partage entre comptes.

Dans le partage entre comptes, configurez la politique pour partager automatiquement les instantanés créés par le planning avec d'autres AWS comptes. Procédez comme suit :

i. Pour activer le partage avec d'autres AWS comptes, sélectionnez Activer le partage entre comptes.

ii. Pour ajouter les comptes avec lesquels partager les instantanés, choisissez Ajouter un compte, entrez l'ID de compte AWS de 12 chiffres, puis choisissez Ajouter.

iii. Pour annuler automatiquement le partage d'instantanés partagés après une période spécifique, sélectionnez Unshare automatically (Annuler le partage automatiquement). Si vous choisissez d'annuler automatiquement le partage d'instantanés partagés, la période à l'issue de laquelle le partage est annulé ne peut pas être plus longue que la période pendant laquelle la politique retient ses instantanés. Par exemple, si la politique est configurée pour retenir les instantanés pendant 5 jours, vous pouvez configurer la politique de façon à ce qu'elle annule automatiquement le partage des instantanés partagés après jusqu'à 4 jours. Cela s'applique aux politiques avec des configurations de rétention d'instantanés basées sur l'âge et le nombre.

Si vous n'activez pas l'annulation automatique du partage, l'instantané est partagé jusqu'à sa suppression.

> **Note**
>
> Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être partagés. Vous ne pouvez pas partager d'instantanés chiffrés à l'aide de la clé KMS de chiffrement EBS par défaut. Si vous partagez des instantanés chiffrés, vous devez également partager la clé KMS utilisée pour chiffrer le volume source avec les comptes cibles. Pour plus d'informations, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur AWS Key Management Service .

h. Pour ajouter des planifications, choisissez l'option Ajouter une planification en haut de l'écran. Pour chaque planification supplémentaire, remplissez les champs comme décrit précédemment dans cette rubrique.

i. Après avoir ajouté les planifications requises, choisissez Examiner une stratégie.

12. Examinez le récapitulatif de la stratégie, puis choisissez Créer une stratégie.

> **Note**
>
> Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consultez

Résoudre les problèmes liés à Amazon Data Lifecycle Manager pour plus d'informations.

Command line

Utilisez la create-lifecycle-policycommande pour créer une politique de cycle de vie des instantanés. Pour `PolicyType`, spécifiez `EBS_SNAPSHOT_MANAGEMENT`.

> **Note**
>
> Pour simplifier la syntaxe, les exemples suivants utilisent un fichier JSON, `policyDetails.json`, qui comportent les détails de la stratégie.

Exemple 1 — Politique de cycle de vie des instantanés avec deux planifications

Cet exemple montre comment créer une stratégie de cycle de vie des instantanés qui crée des instantanés de tous les volumes dont la clé de balise `costcenter` comporte une valeur de `115`. La politique comprend deux planifications. La première planification crée un instantané tous les jours à 3h00 UTC. La deuxième planification crée un instantané hebdomadaire tous les vendredis à 17h00 UTC.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [{
        "Key": "costcenter",
        "Value": "115"
    }],
```

```
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    },
    {
        "Name": "WeeklySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myWeeklySnapshot"
        }],
        "CreateRule": {
            "CronExpression": "cron(0 17 ? * FRI *)"
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

Si la demande aboutit, la commande renvoie l'ID de la politique nouvellement créée. Voici un exemple de sortie.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Exemple 2 : politique de cycle de vie des instantanés qui cible les instances et crée des instantanés d'un sous-ensemble de volumes de données (non racine)

Cet exemple crée une politique de cycle de vie des instantanés qui crée des ensembles d'instantanés multi-volumes à partir d'instances ayant l'identification `code=production`. La politique ne comprend qu'une seule planification. La planification ne crée pas d'instantanés des volumes de données ayant l'identification `code=temp`.

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "code",
        "Value": "production"
    }],
    "Parameters": {
        "ExcludeDataVolumeTags": [{
            "Key": "code",
            "Value": "temp"
        }]
    },
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
```

```
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

Si la demande aboutit, la commande renvoie l'ID de la politique nouvellement créée. Voici un exemple de sortie.

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

Exemple 3 : politique de cycle de vie des instantanés qui automatise les instantanés locaux des ressources Outpost

Cet exemple montre comment créer une stratégie de cycle de vie des instantanés qui crée des instantanés de volumes balisés avec `team=dev` sur tous vos Outposts. La politique crée les instantanés sur les mêmes Outposts que les volumes source. La stratégie crée des instantanés toutes les 12 heures à partir de `00:00` UTC.

```
aws dlm create-lifecycle-policy \
    --description "My local snapshot policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
 "ResourceLocations": "OUTPOST",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CreateRule": {
```

```
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
 "Location": [
  "OUTPOST_LOCAL"
 ]
        },
        "RetainRule": {
            "Count": 1
        },
        "CopyTags": false
    }
]}
```

Exemple 4 : politique de cycle de vie des instantanés qui crée des instantanés dans une région et les copie dans un Outpost

L'exemple de stratégie suivant crée des instantanés de volumes balisés avec `team=dev`. Les instantanés sont créés dans la même Région que le volume source. Les instantanés sont créés toutes les 12 heures à partir de `00:00` UTC et conservent un maximum d'1 instantané. La stratégie copie également les instantanés dans Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`, chiffre les instantanés copiés à l'aide de la clé de chiffrement clé KMS par défaut et conserve les copies pendant 1 mois.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
    "ResourceLocations": "CLOUD",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
```

```
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CopyTags": false,
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
            "Location": "CLOUD"
        },
        "RetainRule": {
            "Count": 1
        },
        "CrossRegionCopyRules" : [
        {
            "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
            "Encrypted": true,
            "CopyTags": true,
            "RetainRule": {
                "Interval": 1,
                "IntervalUnit": "MONTHS"
            }
        }]
    }
]}
```

Exemple 5 – Politique de cycle de vie des instantanés avec une planification basée sur l'archivage et sur l'âge

Cet exemple montre comment créer une politique de cycle de vie des instantanés ciblant les volumes balisés avec `Name=Prod`. La politique comporte une planification basée sur l'âge qui crée des instantanés le premier jour de chaque mois à 9 h. La planification retient chaque instantané du niveau standard pendant un jour, après quoi elle les déplace vers le niveau d'archivage. Les instantanés sont stockés dans le niveau d'archivage pendant 90 jours avant d'être supprimés.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
```

```
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Interval": 1,
          "IntervalUnit": "DAYS"
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Interval": 90,
                 "IntervalUnit": "DAYS"
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Name",
        "Value": "Prod"
      }
    ]
}
```

Exemple 6 – Politique de cycle de vie des instantanés avec une planification basée sur l'archivage et sur le nombre

Cet exemple montre comment créer une politique de cycle de vie des instantanés ciblant les volumes balisés avec `Purpose=Test`. La politique comporte une planification basée sur le nombre qui crée des instantanés le premier jour de chaque mois à 9 h. La planification archive les instantanés immédiatement après leur création et retient un maximum de trois instantanés dans le niveau d'archivage.

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Count": 0
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Count": 3
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
```

```
        "Key": "Purpose",
        "Value": "Test"
      }
    ]
}
```

Considérations relatives aux stratégies de cycle de vie des instantanés

Les considérations générales suivantes s'appliquent aux politiques de cycle de vie des instantanés :

- Les politiques de cycle de vie des instantanés ciblent uniquement les instances ou les volumes qui se trouvent dans la même région que la politique.
- La première opération de création d'instantané démarre dans l'heure suivant l'heure de début spécifiée. Les opérations suivantes de création d'instantanés démarrent dans l'heure suivant leur heure planifiée.
- Vous pouvez créer plusieurs stratégies pour sauvegarder un volume ou une instance . Par exemple, si un volume EBS comporte deux identifications, l'identification A étant la cible de la politique A qui permet de créer un instantané toutes les 12 heures et l'identification B étant la cible de la politique B qui permet de créer un instantané toutes les 24 heures, Amazon Data Lifecycle Manager crée des instantanés en fonction des planifications des deux politiques. Vous pouvez également obtenir le même résultat en créant une seule politique comportant plusieurs planifications. Par exemple, vous pouvez créer une politique unique qui cible uniquement la balise A et spécifier deux planifications : l'une pour toutes les 12 heures et l'autre pour toutes les 24 heures.
- Les balises de ressource cible sont sensibles à la casse.
- Si vous supprimez les balises cibles d'une ressource ciblée par une politique, Amazon Data Lifecycle Manager ne gère plus les instantanés existants dans le niveau standard et le niveau d'archivage. Vous devez les supprimer manuellement s'ils ne sont plus nécessaires.
- Si vous créez une politique qui cible des instances et que de nouveaux volumes sont attachés à l'instance après la création de la politique, les volumes nouvellement ajoutés sont inclus dans la sauvegarde lors de la prochaine exécution de la politique. Tous les volumes attachés à l'instance au moment de l'exécution de la politique sont inclus.
- Si une politique avec une planification personnalisée basée sur les crons est configurée pour créer un seul instantané, la politique ne supprime pas automatiquement cet instantané lorsque le seuil de rétention est atteint. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

- Si vous créez une politique basée sur l'âge dans laquelle la période de conservation est plus courte que la fréquence de création, Amazon Data Lifecycle Manager conservera toujours le dernier instantané jusqu'à la création du suivant. Par exemple, si une politique basée sur l'âge crée un instantané par mois avec une période de conservation de sept jours, Amazon Data Lifecycle Manager conservera chaque pendant un mois, même si la période de conservation est de sept jours.

Les considérations suivantes s'appliquent à l'archivage des instantanés :

- Vous pouvez activer l'archivage des instantanés uniquement pour les politiques d'instantanés qui ciblent les volumes
- Vous ne pouvez spécifier une règle d'archivage que pour une seule planification par politique.
- Si vous utilisez la console, vous pouvez activer l'archivage des instantanés uniquement si la planification possède une fréquence de création mensuelle ou annuelle, ou si elle possède une expression cron avec une fréquence de création d'au moins 28 jours.

  Si vous utilisez l' AWS API ou le AWS CLI AWS SDK, vous ne pouvez activer l'archivage des instantanés que si le planning comporte une expression cron avec une fréquence de création d'au moins 28 jours.
- La période de rétention minimale dans le niveau d'archivage est de 90 jours.
- Lorsqu'un instantané est archivé, il est converti en instantané complet lorsqu'il est déplacé vers le niveau d'archivage. Cela peut entraîner des coûts de stockage d'instantanés plus élevés. Pour de plus amples informations, veuillez consulter Tarification et facturation pour l'archivage des instantanés Amazon EBS.
- La restauration rapide d'instantané et le partage d'instantanés sont désactivés pour les instantanés lorsqu'ils sont archivés.
- Si, dans le cas d'une année bissextile, votre règle de rétention résulte en une période de rétention d'archivage inférieure à 90 jours, Amazon Data Lifecycle Manager garantit la rétention des instantanés pendant la période minimale de 90 jours.
- Si vous archivez manuellement un instantané créé par Amazon Data Lifecycle Manager et que l'instantané est toujours archivé lorsque le seuil de rétention de la planification est atteint, Amazon Data Lifecycle Manager ne gère plus cet instantané. Toutefois, si vous restaurez l'instantané au niveau standard avant que le seuil de rétention de la planification ne soit atteint, la planification continuera à gérer l'instantané conformément aux règles de rétention.

- Si vous restaurez de façon permanente ou temporaire un instantané archivé par Amazon Data Lifecycle Manager et que l'instantané se trouve toujours dans le niveau standard lorsque le seuil de rétention de la planification est atteint, Amazon Data Lifecycle Manager ne gère plus l'instantané. Toutefois, si vous réarchivez l'instantané avant que le seuil de rétention de la planification soit atteint, la planification supprime l'instantané lorsque le seuil de rétention est atteint.
- Les instantanés archivés par Amazon Data Lifecycle Manager sont comptabilisés dans vos quotas `Archived snapshots per volume` et `In-progress snapshot archives per account`.
- Si une planification ne parvient pas à archiver un instantané après de nouvelles tentatives pendant 24 heures, l'instantané reste au niveau standard et sa suppression est planifiée en fonction de l'heure à laquelle il aurait été supprimé du niveau d'archivage. Par exemple, si la planification archive les instantanés pendant 120 jours, ceux-ci restent au niveau standard pendant 120 jours après l'échec de l'archivage avant d'être supprimés définitivement. Pour les planifications basées sur le nombre, l'instantané n'est pas comptabilisé dans le nombre de rétention de la planification.
- Les instantanés doivent être archivés dans la région dans laquelle ils ont été créés. Si vous avez activé la copie inter-régions et l'archivage des instantanés, Amazon Data Lifecycle Manager n'archive pas la copie d'instantané.
- Les instantanés archivés par Amazon Data Lifecycle Manager sont balisés avec la balise système `aws:dlm:archived=true`. De plus, les instantanés créés par une planification basée sur l'archivage et sur l'âge sont balisés avec la balise système `aws:dlm:expirationTime`, qui indique la date et l'heure auxquelles l'archivage de l'instantané est prévu.

Les considérations suivantes s'appliquent à l'exclusion des volumes racine et des volumes de données (non racine) :

- Si vous choisissez d'exclure les volumes de démarrage et que vous spécifiez des balises qui excluent par conséquent tous les volumes de données supplémentaires attachés à une instance, Amazon Data Lifecycle Manager ne créera aucun instantané pour l'instance concernée et émettra une `SnapshotsCreateFailed` CloudWatch métrique. Pour de plus amples informations, veuillez consulter Surveillez les politiques à l'aide CloudWatch.

Les considérations suivantes s'appliquent à la suppression de volumes ou à la résiliation d'instances ciblées par les politiques de cycle de vie des instantanés :

- Si vous supprimez un volume ou résiliez une instance ciblée par une politique avec une planification de rétention basée sur le nombre, Amazon Data Lifecycle Manager ne gère plus les

instantanés dans le niveau standard et le niveau d'archivage créés à partir du volume supprimé ou de l'instance résiliée. Vous devez supprimer ces instantanés précédents manuellement lorsqu'ils ne sont plus nécessaires.

- Si vous supprimez un volume ou résiliez une instance ciblée par une politique avec une planification de rétention basée sur l'âge, la politique continue de supprimer les instantanés du niveau standard et du niveau d'archivage créés à partir du volume supprimé ou de l'instance résiliée selon la planification définie, jusqu'au dernier instantané, mais sans l'inclure. Vous devez supprimer manuellement le dernier instantané s'il n'est plus nécessaire.

Les considérations suivantes s'appliquent aux politiques de cycle de vie des instantanés et à la restauration d'instantané rapide :

- Amazon Data Lifecycle Manager peut activer la restauration rapide des instantanés uniquement pour les instantanés d'une taille inférieure ou égale à 16 Tio. Pour de plus amples informations, veuillez consulter Restauration d'instantané rapide Amazon EBS.
- Un instantané qui est activé pour la restauration d'instantané rapide reste activé, même si vous supprimez ou désactivez la politique, si vous désactivez la restauration d'instantané rapide pour la politique ou si vous désactivez la restauration d'instantané rapide pour la zone de disponibilité. Vous devez désactiver manuellement la restauration d'instantané rapide pour ces instantanés.
- Si vous activez la restauration d'instantané rapide pour une politique et que vous dépassez le nombre maximum d'instantanés pouvant être activés pour la restauration d'instantané rapide, Amazon Data Lifecycle Manager crée des instantanés comme prévu, mais ne les active pas pour la restauration d'instantané rapide. Une fois qu'un instantané activé pour la restauration d'instantané rapide est supprimé, l'instantané suivant créé par Amazon Data Lifecycle Manager est activé pour la restauration rapide d'instantané.
- Lorsque la restauration d'instantané rapide pour un instantané, l'optimisation de ce dernier dure 60 minutes par Tio. Nous vous recommandons de configurer vos planifications de stratégie qui assurent l'optimisation complète de chaque instantané avant que Amazon Data Lifecycle Manager ne crée l'instantané suivant.
- Si vous activez la restauration rapide des instantanés pour une stratégie ciblant les instances, Amazon Data Lifecycle Manager permet une restauration rapide des instantanés pour chaque instantané du cliché multivolume défini individuellement. Si Amazon Data Lifecycle Manager ne parvient pas à activer la restauration rapide des instantanés pour l'un des instantanés du jeu d'instantanés multi-volumes, il tentera toujours d'activer la restauration rapide des instantanés pour les instantanés restants du jeu de d'instantanés.

- Vous êtes facturé pour chaque minute pendant laquelle la restauration d'instantané rapide est activée pour un instantané dans une zone de disponibilité particulière. Les frais sont calculés au prorata avec un minimum d'une heure. Pour plus d'informations, consultez Tarification et facturation.

> **Note**
>
> Selon la configuration de vos politiques de cycle de vie, plusieurs instantanés peuvent être activés pour une restauration rapide dans de multiples zones de disponibilité en simultanée.

Les considérations suivantes s'appliquent aux politiques de cycle de vie des instantanés et aux volumes compatibles Multi-Attach :

- Lors de la création d'une politique de cycle de vie qui cible des instances qui ont les mêmes volumes activés par multi-Attach, Amazon Data Lifecycle Manager lance un instantané du volume pour chaque instance attachée. Utilisez la balise timestamp pour identifier l'ensemble d'instantanés temporels créés à partir des instances attachées.

Les considérations suivantes s'appliquent au partage des instantanés entre comptes :

- Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être partagés.
- Vous ne pouvez pas partager d'instantanés chiffrés à l'aide de la clé KMS de chiffrement EBS par défaut.
- Si vous partagez des instantanés chiffrés, vous devez également partager la clé KMS utilisée pour chiffrer le volume source avec les comptes cibles. Pour plus d'informations, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur AWS Key Management Service .

Les considérations suivantes s'appliquent aux politiques des instantanés et à l'archivage des instantanés :

- Si vous archivez manuellement un instantané créé par une politique et que cet instantané se trouve dans le niveau d'archivage lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager ne supprime pas l'instantané. Amazon Data Lifecycle Manager ne gère pas

les instantanés lorsqu'ils sont stockés dans le niveau d'archivage. Si vous n'avez plus besoin des instantanés qui sont stockés dans le niveau d'archivage, vous devez les supprimer manuellement.

Les considérations suivantes s'appliquent aux politiques relatives aux instantanés et à la corbeille :

- Si Amazon Data Lifecycle Manager supprime un instantané et l'envoie à la corbeille lorsque le seuil de rétention de la politique est atteint, et que vous restaurez manuellement l'instantané à partir de la corbeille, vous devez supprimer manuellement cet instantané s'il n'est plus nécessaire. Amazon Data Lifecycle Manager ne gérera plus l'instantané.
- Si vous supprimez manuellement un instantané créé par une politique et que cet instantané se trouve dans la corbeille lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager ne supprime pas l'instantané. Amazon Data Lifecycle Manager ne gère pas les instantanés lorsqu'ils sont stockés dans la corbeille.

  Si l'instantané est restauré à partir de la corbeille avant que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager supprime l'instantané lorsque le seuil de rétention de la politique est atteint.

  Si l'instantané est restauré à partir de la corbeille après que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager ne supprime plus l'instantané. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Les considérations suivantes s'appliquent aux politiques de cycle de vie des instantanés qui sont dans l'état d'erreur :

- Pour les politiques avec des planifications de rétention basées sur l'âge, les instantanés qui sont configurés pour expirer alors que la politique est dans l'état `error` sont conservés indéfiniment. Vous devez supprimer les instantanés manuellement. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la suppression des instantanés à mesure que leurs périodes de rétention expirent.
- Pour les politiques avec des planifications de rétention basée sur le nombre, la politique arrête de créer et de supprimer des instantanés pendant qu'elle est dans l'état `error`. Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la création d'instantanés, ainsi que la suppression d'instantanés lorsque le seuil de rétention est atteint.

Les considérations suivantes s'appliquent aux politiques d'instantanés et au verrouillage d'instantanés :

- Si vous verrouillez manuellement un instantané créé par Amazon Data Lifecycle Manager et que l'instantané est toujours verrouillé lorsque son seuil de conservation est atteint, Amazon Data Lifecycle Manager ne gère plus cet instantané. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.
- Si vous verrouillez manuellement un instantané qui a été créé par Amazon Data Lifecycle Manager avec la restauration rapide activée et que l'instantané est toujours verrouillé lorsque son seuil de conservation est atteint, Amazon Data Lifecycle Manager ne désactive pas la restauration rapide de l'instantané et ne supprime pas l'instantané. Vous devez désactiver la restauration d'instantané rapide et supprimer manuellement l'instantané s'il n'est plus nécessaire.
- Si vous inscrivez manuellement un instantané qui a été créé par Amazon Data Lifecycle Manager avec une AMI puis que vous verrouillez cet instantané, et que l'instantané est toujours verrouillé et associé à l'AMI lorsque son seuil de conservation est atteint, Amazon Data Lifecycle Manager continue de tenter de supprimer l'instantané. Lorsque l'inscription de l'AMI est annulée et que l'instantané est déverrouillé, Amazon Data Lifecycle Manager supprime automatiquement l'instantané.

Ressources supplémentaires

Pour plus d'informations, consultez le blog Automating Amazon EBS snapshot and AMI management using Amazon Data Lifecycle Manager AWS storage.

Automatisez les instantanés cohérents avec les applications avec Data Lifecycle Manager

Vous pouvez automatiser les instantanés cohérents par rapport à l'application avec Amazon Data Lifecycle Manager en activant les pré-scripts et les post-scripts dans vos politiques de cycle de vie des instantanés qui ciblent les instances.

Amazon Data Lifecycle Manager s'intègre à AWS Systems Manager (Systems Manager) pour prendre en charge des instantanés cohérents avec les applications. Amazon Data Lifecycle Manager utilise les documents de commande Systems Manager (SSM) qui incluent des pré-scripts et des post-scripts pour automatiser les actions nécessaires pour créer des instantanés cohérents par rapport à l'application. Avant qu'Amazon Data Lifecycle Manager ne lance la création d'instantanés, il exécute

les commandes de pré-script pour geler et vider les E/S. Une fois qu'Amazon Data Lifecycle Manager a lancé la création d'instantanés, il exécute les commandes du post-script pour dégeler les E/S.

Avec Amazon Data Lifecycle Manager, vous pouvez automatiser les instantanés cohérents par rapport à l'application pour les applications suivantes :

- applications Windows avec Volume Shadow Copy Service (VSS) ;
- SAP HANA à l'aide d'un AWS document SSDM géré. pour plus d'informations, consultez Amazon EBS snapshots for SAP HANA.
- Bases de données autogérées, telles que MySQL, PostgreSQL InterSystems ou IRIS, à l'aide de modèles de documents SSM

Rubriques

Exigences relatives à l'utilisation des pré-scripts et post-scripts

Le tableau suivant décrit les exigences relatives à l'utilisation des pré-scripts et des post-scripts avec Amazon Data Lifecycle Manager.

	Instantanés cohérents par rapport à l'application		
Exigence	Sauvegarde VSS	Document SSM personnalisé	Autres cas d'utilisation
Agent SSM installé et exécuté sur les instances cibles	✓	✓	✓
Les exigences du système VSS sont	✓		

	Instantanés cohérents par rapport à l’application		
satisfaites sur les instances cibles			
Profil d'instance compatible VSS associé aux instances cibles	✓		
Composants VSS installés sur les instances cibles	✓		
Préparer un document SSM avec des commandes de script pré et post		✓	✓
Préparer le rôle IAM d'Amazon Data Lifecycle Manager, exécuter des scripts avant et après	✓	✓	✓
Créez une politique de capture instantanée qui cible les instances et qui est configurée pour les pré-scripts et les post-scripts	✓	✓	✓

Démarrage avec les instantanés cohérents par rapport à l’application

Cette section explique les étapes à suivre pour automatiser les instantanés cohérents par rapport à l’application à l’aide d’Amazon Data Lifecycle Manager.

Étape 1 : Préparer les instances cibles

Vous devez préparer les instances ciblées pour les instantanés cohérents par rapport à l'application à l'aide d'Amazon Data Lifecycle Manager. Effectuez l'une des actions suivantes en fonction de votre cas d'utilisation.

Prepare for VSS Backups

Pour préparer vos instances cibles pour les sauvegardes VSS

1. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.

   Pour plus d'informations, consultez la section Utilisation de l'agent SSM sur les EC2 instances de Windows Server.
2. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez Vérification du statut de l'SSM Agent et démarrage de l'agent.
3. Configurez Systems Manager pour les EC2 instances Amazon. Pour plus d'informations, consultez la section Configuration de Systems Manager pour les EC2 instances Amazon dans le Guide de AWS Systems Manager l'utilisateur.
4. Assurez-vous que la configuration système requise pour les sauvegardes VSS est respectée.
5. Attachez un profil d'instance compatible avec VSS aux instances cibles.
6. Installez les composants VSS.

Prepare for SAP HANA backups

Pour préparer vos instances cibles pour les sauvegardes SAP HANA

1. Préparez l'environnement SAP HANA sur vos instances cibles.

   a. Configurez votre instance avec SAP HANA. Si vous ne possédez pas encore d'environnement SAP HANA, vous pouvez consulter la rubrique SAP HANA Environment Setup on AWS.

   b. Connectez-vous à SystemDB en tant qu'utilisateur administrateur approprié.

   c. Créez un utilisateur de sauvegarde de base de données à utiliser avec Amazon Data Lifecycle Manager.

```
CREATE USER username PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

Par exemple, la commande suivante crée un utilisateur nommé `dlm_user` avec le mot de passe `password`.

```
CREATE USER dlm_user PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
```

d. Attribuez le rôle `BACKUP OPERATOR` à l'utilisateur de sauvegarde de base de données que vous avez créé à l'étape précédente.

```
GRANT BACKUP OPERATOR TO username
```

Par exemple, la commande suivante attribue le rôle à un utilisateur nommé `dlm_user`.

```
GRANT BACKUP OPERATOR TO dlm_user
```

e. Connectez-vous au système d'exploitation en tant qu'administrateur, par exemple *sid*`adm`.

f. Créez une entrée `hdbuserstore` pour stocker les informations de connexion afin que le document SSM SAP HANA puisse se connecter à SAP HANA sans que les utilisateurs aient à saisir ces informations.

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER
 localhost:3hana_instance_number13 username password
```

Par exemple :

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER localhost:30013 dlm_user password
```

g. Testez la connexion.

```
hdbsql -U DLM_HANADB_SNAPSHOT_USER "select * from dummy"
```

2. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.

Pour plus d'informations, voir Installation manuelle de l'agent SSM sur les EC2 instances pour Linux.

3. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez Vérification du statut de l'SSM Agent et démarrage de l'agent.
4. Configurez Systems Manager pour les EC2 instances Amazon. Pour plus d'informations, consultez la section Configuration de Systems Manager pour les EC2 instances Amazon dans le Guide de AWS Systems Manager l'utilisateur.

Prepare for custom SSM documents

Pour préparer les documents SSM personnalisés de vos instances cibles

1. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.
   - (Instances Linux) Installation manuelle de l'agent SSM sur les EC2 instances pour Linux
   - (instances Windows) Utilisation de l'agent SSM sur les EC2 instances pour Windows Server
2. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez Vérification du statut de l'SSM Agent et démarrage de l'agent.
3. Configurez Systems Manager pour les EC2 instances Amazon. Pour plus d'informations, consultez la section Configuration de Systems Manager pour les EC2 instances Amazon dans le Guide de AWS Systems Manager l'utilisateur.

Étape 2 : Préparer le document SSM

> **Note**
>
> Cette étape est requise uniquement pour les documents SSM personnalisés. Elle n'est pas nécessaire pour les sauvegardes VSS ou SAP HANA. Pour les sauvegardes VSS et SAP HANA, Amazon Data Lifecycle Manager utilise le document AWS SSM géré.

Si vous automatisez des instantanés cohérents avec les applications pour une base de données autogérée, telle que MySQL, PostgreSQL ou InterSystems IRIS, vous devez créer un document de commande SSM qui inclut un pré-script pour geler et vider les E/S avant le lancement de la création du snapshot, et un post-script pour dégeler les E/S après le lancement de la création de snapshots.

Si votre base de données MySQL, PostgreSQL InterSystems ou IRIS utilise des configurations standard, vous pouvez créer un document de commande SSM à l'aide de l'exemple de contenu du document SSM ci-dessous. Si votre base de données MySQL, PostgreSQL InterSystems ou IRIS utilise une configuration non standard, vous pouvez utiliser l'exemple de contenu ci-dessous comme point de départ pour votre document de commande SSM, puis le personnaliser en fonction de vos besoins. Si vous souhaitez créer un nouveau document SSM à partir de zéro, vous pouvez également utiliser le modèle de document SSM vide ci-dessous et ajouter vos commandes pré et post dans les sections de document appropriées.

⚠ Remarques :

- Il est de votre responsabilité de vous assurer que le document SSM exécute les actions correctes et requises pour la configuration de votre base de données.
- La cohérence des instantanés par rapport à l'application est garantie uniquement si les pré-scripts et les post-scripts de votre document SSM parviennent à geler, à vider et à dégeler les E/S.
- Le document SSM doit inclure les champs obligatoires pour `allowedValues`, notamment `pre-script`, `post-script` et `dry-run`. Amazon Data Lifecycle Manager exécutera des commandes sur votre instance en fonction du contenu de ces sections. Si votre document SSM ne contient pas ces sections, Amazon Data Lifecycle Manager le considérera comme un échec d'exécution.

MySQL sample document content

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
```

```
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###========================================================================###
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for MySQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run MySQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash
```

```
###============================================================================###
     ### Error Codes

###============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206

     ###====================================================================###
     ### Global variables
     ###====================================================================###
     START=$(date +%s)
     # For testing this script locally, replace the below with OPERATION=$1.
     OPERATION={{ command }}
     FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
     FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
     FS_BUSY_ERROR='mount point is busy'

     # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
     # duration specified in the global variable below. Choose the duration based
on your
     # database application's tolerance to freeze.
     export AUTO_THAW_DURATION_SECS="60"

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
         # Check if filesystem is already frozen. No error code indicates that
filesystem
         # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
         check_fs_freeze
         # Execute the DB commands to flush the DB in preparation for snapshot
```

```
        snap_db
        # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
        freeze_fs

        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen.
        unfreeze_fs
        thaw_db
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
```

```
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
```

```
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    sudo mysql -e 'UNLOCK TABLES;'
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                thaw_db
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
```

```
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Flush and Lock command."
            sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
            # If the MySQL Flush and Lock command did not succeed, return error
code 201 to indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: MySQL FLUSH TABLES WITH READ LOCK command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Flush and Lock command."
        fi
    }

    thaw_db() {
        # Run the unlock command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Unlock"
            sudo mysql -e 'UNLOCK TABLES;'
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Unlock command."
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs
    export -f thaw_db
```

```
      # Debug logging for parameters passed to the SSM document
      echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
          pre-script)
              execute_pre_script
              ;;
          post-script)
              execute_post_script
              execute_disable_auto_thaw
              ;;
          dry-run)
              echo "INFO: dry-run option invoked - taking no action"
              ;;
          *)
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

PostgreSQL sample document content

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.
```

```
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###############################################################################
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for PostgreSQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run PostgreSQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
```

```
   runCommand:
   - |
     #!/bin/bash


###============================================================================###
     ### Error Codes

###============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206


###============================================================================###
     ### Global variables

###============================================================================###
     START=$(date +%s)
     OPERATION={{ command }}
     FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
     FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
     FS_BUSY_ERROR='mount point is busy'

     # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
     # duration specified in the global variable below. Choose the duration based
on your
     # database application's tolerance to freeze.
     export AUTO_THAW_DURATION_SECS="60"

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
         # Check if filesystem is already frozen. No error code indicates that
filesystem
```

```
        # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
        check_fs_freeze
        # Execute the DB commands to flush the DB in preparation for snapshot
        snap_db
        # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
        freeze_fs

        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen
        unfreeze_fs
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
```

```
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
```

```
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
```

```
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when PostgreSQL DB service is up and running
        sudo systemctl is-active --quiet postgresql
        if [ $? -eq 0 ]; then
            echo "INFO: Execute Postgres CHECKPOINT"
            # PostgreSQL command to flush the transactions in memory to disk
            sudo -u postgres psql -c 'CHECKPOINT;'
            # If the PostgreSQL Command did not succeed, return error code 201 to
indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: Postgres CHECKPOINT command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: PostgreSQL service is inactive. Skipping execution of
CHECKPOINT command."
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
```

```
          post-script)
              execute_post_script
              execute_disable_auto_thaw
              ;;
          dry-run)
              echo "INFO: dry-run option invoked - taking no action"
              ;;
          *)
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

InterSystems IRIS sample document content

```
###============================================================================###
# MIT License
#
# Copyright (c) 2024 InterSystems
#
# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in all
# copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
```

```
###=====================================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature for InterSystems IRIS.
parameters:
  executionId:
    type: String
    default: None
    description: Specifies the unique identifier associated with a pre and/or post
 execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    type: String
    # Data Lifecycle Manager will trigger the pre-script and post-script actions.
 You can also use this SSM document with 'dry-run' for manual testing purposes.
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    #The following allowedValues will allow Data Lifecycle Manager to successfully
 trigger pre and post script actions.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run InterSystems IRIS Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

 ###=====================================================================================###
      ### Global variables

 ###=====================================================================================###
      DOCKER_NAME=iris
```

```
     LOGDIR=./
     EXIT_CODE=0
     OPERATION={{ command }}
     START=$(date +%s)

     # Check if Docker is installed
     # By default if Docker is present, script assumes that InterSystems IRIS is
running in Docker
     # Leave only the else block DOCKER_EXEC line, if you run InterSystems IRIS
non-containerised (and Docker is present).
     # Script assumes irissys user has OS auth enabled, change the OS user or
supply login/password depending on your configuration.
     if command -v docker &> /dev/null
     then
       DOCKER_EXEC="docker exec $DOCKER_NAME"
     else
       DOCKER_EXEC="sudo -i -u irissys"
     fi


     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
       echo "INFO: Start execution of pre-script"

       # find all iris running instances
       iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
'^up' | cut -c5-  | awk '{print $1}')
       echo "`date`: Running iris instances $iris_instances"

       # Only for running instances
       for INST in $iris_instances; do

         echo "`date`: Attempting to freeze $INST"

         # Detailed instances specific log
         LOGFILE=$LOGDIR/$INST-pre_post.log

         #check Freeze status before starting
         $DOCKER_EXEC irissession $INST -U '%SYS'
"##Class(Backup.General).IsWDSuspendedExt()"
         freeze_status=$?
         if [ $freeze_status -eq 5 ]; then
           echo "`date`:   ERROR: $INST IS already FROZEN"
           EXIT_CODE=204
```

```
          else
            echo "`date`:   $INST is not frozen"
            # Freeze
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).ExternalFreeze(\"$LOGFILE\",,,,,,600,,,300)"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS FROZEN"
                ;;
              3) echo "`date`:   $INST FREEZE FAILED"
                EXIT_CODE=201
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                EXIT_CODE=201
                ;;
            esac
            echo "`date`:   Completed freeze of $INST"
          fi
        done
        echo "`date`: Pre freeze script finished"
      }

      # Add all post-script actions to be performed within the function below
      execute_post_script() {
        echo "INFO: Start execution of post-script"

        # find all iris running instances
        iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
 '^up' | cut -c5-  | awk '{print $1}')
        echo "`date`: Running iris instances $iris_instances"

        # Only for running instances
        for INST in $iris_instances; do

          echo "`date`: Attempting to thaw $INST"

          # Detailed instances specific log
          LOGFILE=$LOGDIR/$INST-pre_post.log

          #check Freeze status befor starting
```

```
          $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).IsWDSuspendedExt()"
          freeze_status=$?
          if [ $freeze_status -eq 5 ]; then
            echo "`date`:  $INST is in frozen state"
            # Thaw
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS THAWED"
                  $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalSetHistory(\"$LOGFILE\")"
                ;;
              3) echo "`date`:   $INST THAW FAILED"
                  EXIT_CODE=202
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                  EXIT_CODE=202
                ;;
            esac
            echo "`date`:   Completed thaw of $INST"
          else
            echo "`date`:   ERROR: $INST IS already THAWED"
            EXIT_CODE=205
          fi
        done
        echo "`date`: Post thaw script finished"
      }

      # Debug logging for parameters passed to the SSM document
        echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
        pre-script)
          execute_pre_script
          ;;
        post-script)
```

```
          execute_post_script
            ;;
        dry-run)
          echo "INFO: dry-run option invoked - taking no action"
          ;;
        *)
          echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
          # return failure
          EXIT_CODE=1
          ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
      exit $EXIT_CODE
```

Pour plus d'informations, consultez le GitHub référentiel.

Empty document template

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###############################################################################
schemaVersion: '2.2'
```

```
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes
```

```
###============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206


###============================================================================###
     ### Global variables

###============================================================================###
     START=$(date +%s)
     # For testing this script locally, replace the below with OPERATION=$1.
     OPERATION={{ command }}

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
     }

     # Add all post-script actions to be performed within the function below
     execute_post_script() {
         echo "INFO: Start execution of post-script"
     }

     # Debug logging for parameters passed to the SSM document
     echo "INFO: ${OPERATION} starting at $(date) with executionId:
${EXECUTION_ID}"

     # Based on the command parameter value execute the function that supports
     # pre-script/post-script operation
     case ${OPERATION} in
         pre-script)
             execute_pre_script
             ;;
         post-script)
```

```
            execute_post_script
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
    echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Une fois que vous avez obtenu le contenu de votre document SSM, utilisez l'une des procédures suivantes pour créer le document SSM personnalisé.

Console

Pour créer un document de commande SSM

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com//systems-manager/.
2. Dans le volet de navigation, choisissez Documents, puis sélectionnez Créer un document, Commande ou session.
3. Pour Name (Nom), saisissez un nom évocateur pour le document.
4. Pour Type de cible, sélectionnez/AWS::EC2::Instance.
5. Pour Type de document, sélectionnez Commande.
6. Dans le champ Contenu, sélectionnez YAML, puis collez le contenu du document.
7. Dans la section Balises du document, ajoutez une balise avec une clé de balise `DLMScriptsAccess` et une valeur de balise `true`.

> **Important**
>
> La `DLMScriptsAccess:true` balise est requise par la politique de AWS gestion des AWSDataLifecycleManagerSSMFullaccès utilisée à l'étape 3 : préparation du

rôle IAM Amazon Data Lifecycle Manager. La politique utilise la clé de condition `aws:ResourceTag` pour limiter l'accès aux documents SSM dotés de cette balise.

8. Sélectionnez Créer un document.

AWS CLI

Pour créer un document de commande SSM

Utilisez la commande create-document. Pour `--name`, saisissez un nom descriptif pour le document Pour `--document-type`, spécifiez `Command`. Pour `--content`, spécifiez le chemin d'accès au fichier .yaml avec le contenu du document SSM. Pour `--tags`, spécifiez `"Key=DLMScriptsAccess,Value=true"`.

```
$ aws ssm create-document \
--content file://path/to/file/documentContent.yaml \
--name "document_name" \
--document-type "Command" \
--document-format YAML \
--tags "Key=DLMScriptsAccess,Value=true"
```

Étape 3 : Préparer le rôle IAM d'Amazon Data Lifecycle Manager

Note

Cette étape est nécessaire si :

- vous créez ou mettez à jour une politique d'instantanés avec pré/post-scripts activés qui utilise un rôle IAM personnalisé ;
- vous utilisez la ligne de commande pour créer ou mettre à jour une politique d'instantanés avec pré/post-scripts activés qui utilise la valeur par défaut.

Si vous utilisez la console pour créer ou mettre à jour une politique de capture d'écran activée avant ou après le script qui utilise le rôle par défaut pour la gestion des instantanés (AWSDataLifecycleManagerDefaultRole), ignorez cette étape. Dans ce cas, nous associons automatiquement la politique AWSDataLifecycleManagerSSMFulld'accès à ce rôle.

Vous devez vous assurer que le rôle IAM que vous utilisez pour la politique accorde à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions SSM requises pour exécuter les pré-scripts et les post-scripts sur les instances ciblées par la politique.

Amazon Data Lifecycle Manager fournit une politique gérée (AWSDataLifecycleManagerSSMFullAccess) qui inclut les autorisations requises. Vous pouvez associer cette politique à votre rôle IAM pour gérer les instantanés afin de vous assurer qu'elle inclut les autorisations.

> **Important**
>
> La politique AWSData LifecycleManager SSMFull d'accès géré utilise la clé de `aws:ResourceTag` condition pour restreindre l'accès à des documents SSM spécifiques lors de l'utilisation de scripts pré et post. Pour autoriser Amazon Data Lifecycle Manager à accéder aux documents SSM, vous devez vous assurer que vos documents SSM sont balisés avec `DLMScriptsAccess:true`.

Vous pouvez également créer manuellement une politique personnalisée ou attribuer les autorisations requises directement au rôle IAM que vous utilisez. Vous pouvez utiliser les mêmes autorisations que celles définies dans la politique AWSData LifecycleManager SSMFull d'accès géré, mais la clé de `aws:ResourceTag` condition est facultative. Si vous décidez de ne pas inclure cette clé de condition, vous n'avez pas besoin de baliser vos documents SSM avec `DLMScriptsAccess:true`.

Utilisez l'une des méthodes suivantes pour ajouter la politique AWSDataLifecycleManagerSSMFulld'accès à votre rôle IAM.

Console

Pour attacher la politique gérée à votre rôle personnalisé

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Recherchez et sélectionnez votre rôle personnalisé pour la gestion des instantanés.
4. Sous l'onglet Permissions (Autorisations), choisissez Add Permissions (Ajouter des autorisations), Attach policies (Attacher des politiques).

5. Recherchez et sélectionnez la politique AWSDataLifecycleManagerSSMFulld'accès géré, puis choisissez Ajouter des autorisations.

AWS CLI

Pour attacher la politique gérée à votre rôle personnalisé

Utilisez la commande attach-role-policy. Pour `---role-name`, spécifiez le nom de votre rôle personnalisé. Pour `--policy-arn`, spécifiez `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Étape 4 : Créer une politique de cycle de vie des instantanés

Pour automatiser les instantanés cohérents par rapport à l'application, vous devez créer une politique de cycle de vie des instantanés qui cible les instances, et configurer des pré-scripts et post-scripts pour cette politique.

Console

Pour créer la politique de cycle de vie des instantanés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans la page Sélectionner un type de stratégie, choisissez Stratégie d'instantané EBS, puis Suivant.
4. Dans la section Ressources cibles, effectuez les opérations suivantes :
   a. Pour Types de ressources cibles, choisissez `Instance`.
   b. Pour Balises de ressource cible, spécifiez les balises de ressource qui identifient les instances à sauvegarder. Seules les ressources possédant les balises spécifiées seront sauvegardées.

5. Pour le rôle IAM, choisissez AWSDataLifecycleManagerDefaultRole(le rôle par défaut pour la gestion des instantanés) ou choisissez un rôle personnalisé que vous avez créé et préparé pour les pré-scripts et les post-scripts.
6. Configurez les planifications et les options supplémentaires selon les besoins. Nous vous recommandons de planifier les heures de création des instantanés pour des périodes correspondant à votre charge de travail, par exemple pendant les fenêtres de maintenance.

   Pour SAP HANA, nous vous recommandons d'activer la restauration d'instantané rapide.

   > **Note**
   >
   > Si vous activez une planification pour les sauvegardes VSS, vous ne pouvez pas activer Exclure des volumes de données spécifiques ou Copier les balises depuis la source.

7. Dans la section Pré-scripts et post-scripts, sélectionnez Activer les pré-scripts et post-scripts, puis effectuez les opérations suivantes, en fonction de votre charge de travail :

   - Pour créer des instantanés cohérents par rapport à l'application de vos applications Windows, sélectionnez Sauvegarde VSS.
   - Pour créer des instantanés cohérents par rapport à l'application de vos charges de travail SAP HANA, sélectionnez SAP HANA.
   - Pour créer des instantanés cohérents avec les applications de toutes les autres bases de données et charges de travail, y compris vos bases de données MySQL, PostgreSQL ou InterSystems IRIS autogérées, à l'aide d'un document SSM personnalisé, sélectionnez Document SSM personnalisé.
     1. Pour Option d'automatisation, choisissez Pré-scripts et post-scripts.
     2. Pour Document SSM, sélectionnez le document SSM que vous avez préparé.

8. En fonction de l'option que vous avez sélectionnée, configurez les options supplémentaires suivantes :

   - Délai d'expiration du script : (document SSM personnalisé uniquement) délai d'expiration au terme duquel Amazon Data Lifecycle Manager échoue à exécuter le script si celui-ci n'est pas terminé. Si un script ne s'exécute pas dans le délai imparti, Amazon Data Lifecycle Manager échoue. Le délai d'expiration s'applique aux pré-scripts et post-scripts individuellement. Le délai d'expiration minimum et par défaut est de 10 secondes. Et le délai d'expiration maximum est de 120 secondes.

- Relancer les scripts en échec : sélectionnez cette option pour relancer les scripts qui ne se terminent pas dans le délai imparti. En cas d'échec du pré-script, Amazon Data Lifecycle Manager relance l'intégralité du processus de création d'instantanés, y compris l'exécution des pré-scripts et post-scripts. Si le post-script échoue, Amazon Data Lifecycle Manager relance uniquement le post-script ; dans ce cas, le pré-script sera terminé et l'instantané aura peut-être été créé.
- Prise par défaut d'instantanés en cas de panne : sélectionnez cette option pour utiliser par défaut des instantanés en cas de panne si le pré-script ne s'exécute pas. Il s'agit du comportement de création d'instantanés par défaut pour Amazon Data Lifecycle Manager si les pré-scripts et post-scripts ne sont pas activés. Si vous avez activé les relances, Amazon Data Lifecycle Manager utilise par défaut des instantanés en cas de panne uniquement une fois que toutes les relances ont été épuisées. Si le pré-script échoue et que vous n'utilisez pas par défaut des instantanés en cas de panne, Amazon Data Lifecycle Manager ne crée pas d'instantanés pour l'instance pendant cette exécution planifiée.

> **Note**
>
> Si vous créez des instantanés pour SAP HANA, vous souhaiterez peut-être désactiver cette option. Les instantanés en cas de panne des charges de travail SAP HANA ne peuvent pas être restaurés de la même manière.

9. Choisissez Créer une politique par défaut.

> **Note**
>
> Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consultez Résoudre les problèmes liés à Amazon Data Lifecycle Manager pour plus d'informations.

AWS CLI

Pour créer la politique de cycle de vie des instantanés

Utilisez la create-lifecycle-policycommande et incluez les `Scripts` paramètres dans`CreateRule`. Pour plus d'informations sur les paramètres, consultez la référence d'API Amazon Data Lifecycle Manager.

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

Lorsque `policyDetails.json` inclut l'un des éléments suivants, selon votre cas d'utilisation :

- Sauvegarde VSS

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "ExecutionHandler":"AWS_VSS_BACKUP",
                "ExecuteOperationOnScriptFailure":true|false,
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- Sauvegardes SAP HANA

```
{
```

```
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- Document SSM personnalisé

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
```

```
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

Considérations relatives aux sauvegardes VSS avec Amazon Data Lifecycle Manager

Avec Amazon Data Lifecycle Manager, vous pouvez sauvegarder et restaurer des applications Windows compatibles VSS (Volume Shadow Copy Service) exécutées sur des instances Amazon EC2 . Si l'application possède un enregistreur VSS enregistré auprès de Windows VSS, Amazon Data Lifecycle Manager crée un instantané qui sera cohérent avec l'application pour cette application.

> **Note**
>
> Amazon Data Lifecycle Manager prend actuellement en charge les instantanés cohérents avec les applications des ressources exécutées sur Amazon EC2 uniquement, en particulier pour les scénarios de sauvegarde dans lesquels les données d'application peuvent être restaurées en remplaçant une instance existante par une nouvelle instance créée à partir de la sauvegarde. Les types d'instances ou applications ne sont pas tous pris en charge pour les sauvegardes VSS. Pour plus d'informations, consultez la section Instantanés Windows VSS cohérents avec les applications dans le guide de l'utilisateur Amazon. EC2

Types d'instance non pris en charge

Les types d' EC2 instances Amazon suivants ne sont pas pris en charge pour les sauvegardes VSS. Si votre politique cible l'un de ces types d'instances, Amazon Data Lifecycle Manager peut toujours créer des sauvegardes VSS, mais les instantanés risquent de ne pas être balisés avec les balises système requises. Sans ces balises, les instantanés ne seront pas gérés par Amazon Data

Lifecycle Manager après leur création. Vous aurez peut-être besoin de supprimer ces instantanés manuellement.

- T3 : `t3.nano` | `t3.micro`
- T3a : `t3a.nano` | `t3a.micro`
- T2 : `t2.nano` | `t2.micro`

Responsabilité partagée pour les instantanés cohérents par rapport à l'application

Vous devez vous assurer que :

- L'agent SSM est installé et up-to-date s'exécute sur vos instances cibles
- Systems Manager est autorisé à effectuer les actions requises sur les instances cibles
- Amazon Data Lifecycle Manager est autorisé à effectuer les actions Systems Manager requises pour exécuter des pré-scripts et des post-scripts sur les instances cibles.
- Pour les charges de travail personnalisées, telles que les bases de données MySQL, PostgreSQL ou InterSystems IRIS autogérées, le document SSM que vous utilisez inclut les actions correctes et requises pour geler, vider et dégeler les E/S pour la configuration de votre base de données.
- Les délais de création d'instantanés correspondent à votre planification de charge de travail. Par exemple, essayez de planifier la création d'instantanés pendant les fenêtres de maintenance planifiées.

Amazon Data Lifecycle Manager garantit que :

- la création d'instantanés démarre dans les 60 minutes suivant l'heure de création d'instantanés prévue ;
- les pré-scripts s'exécutent avant le lancement de la création d'instantanés ;
- les post-scripts s'exécutent une fois que le pré-script a réussi et que la création d'instantanés a été lancée ; Amazon Data Lifecycle Manager exécute le post-script uniquement si le pré-script aboutit ; si le pré-script échoue, Amazon Data Lifecycle Manager n'exécute pas le post-script ;
- les instantanés sont balisés avec les balises appropriées lors de leur création ;
- CloudWatch les métriques et les événements sont émis lorsque les scripts sont lancés et lorsqu'ils échouent ou réussissent.

Autres cas d'utilisation des scripts antérieurs et postérieurs à Data Lifecycle Manager

Outre l'automatisation des instantanés cohérents par rapport à l'application, vous pouvez utiliser les pré-scripts et les post-scripts ensemble ou séparément pour automatiser d'autres tâches administratives avant ou après la création des instantanés. Par exemple :

- Utilisation d'un pré-script pour appliquer des correctifs avant la création d'instantanés. Cela peut vous aider à créer des instantanés après avoir appliqué vos mises à jour logicielles hebdomadaires ou mensuelles régulières.

  > **Note**
  >
  > Si vous choisissez d'exécuter uniquement un pré-script, l'option Prise par défaut d'instantanés en cas de panne est activée par défaut.

- Utilisation d'un post-script pour appliquer des correctifs après la création d'instantanés. Cela peut vous aider à créer des instantanés avant d'appliquer vos mises à jour logicielles hebdomadaires ou mensuelles régulières.

Démarrage pour d'autres cas d'utilisation

Cette section explique les étapes à suivre lorsque vous utilisez des pré-scripts et/ou des post-scripts pour des cas d'utilisation autres que des instantanés cohérents par rapport à l'application.

Étape 1 : Préparer les instances cibles

Pour préparer vos instances cibles pour les pré-scripts et/ou les post-scripts

1. Installez l'agent SSM sur vos instances cibles, s'il n'est pas déjà installé. Si l'agent SSM est déjà installé sur vos instances cibles, ignorez cette étape.
   - (Instances Linux) Installation manuelle de l'agent SSM sur les EC2 instances pour Linux
   - (instances Windows) Utilisation de l'agent SSM sur les EC2 instances pour Windows Server
2. Assurez-vous que l'agent SSM est en cours d'exécution. Pour plus d'informations, consultez Vérification du statut de l'SSM Agent et démarrage de l'agent.

3. Configurez Systems Manager pour les EC2 instances Amazon. Pour plus d'informations, consultez la section Configuration de Systems Manager pour les EC2 instances Amazon dans le Guide de AWS Systems Manager l'utilisateur.

Étape 2 : Préparer le document SSM

Vous devez créer un document de commande SSM qui inclut les pré-scripts et/ou les post-scripts avec les commandes que vous souhaitez exécuter.

Vous pouvez créer un document SSM à l'aide du modèle de document SSM vide ci-dessous et ajouter vos commandes pré-script et post-script dans les sections de document appropriées.

⚠ Remarques :

- Il est de votre responsabilité de vous assurer que le document SSM exécute les actions correctes et requises pour votre charge de travail.
- Le document SSM doit inclure les champs obligatoires pour `allowedValues`, notamment `pre-script`, `post-script` et `dry-run`. Amazon Data Lifecycle Manager exécutera des commandes sur votre instance en fonction du contenu de ces sections. Si votre document SSM ne contient pas ces sections, Amazon Data Lifecycle Manager le considérera comme un échec d'exécution.

```
###============================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###============================================================================###
```

```
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre and/
or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-
[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions during
 policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager to
 successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should be
 executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes
```

```
###============================================================================###
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the 'cause'
field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206


###============================================================================###
     ### Global variables

###============================================================================###
     START=$(date +%s)
     # For testing this script locally, replace the below with OPERATION=$1.
     OPERATION={{ command }}

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
     }

     # Add all post-script actions to be performed within the function below
     execute_post_script() {
         echo "INFO: Start execution of post-script"
     }

     # Debug logging for parameters passed to the SSM document
     echo "INFO: ${OPERATION} starting at $(date) with executionId: ${EXECUTION_ID}"

     # Based on the command parameter value execute the function that supports
     # pre-script/post-script operation
     case ${OPERATION} in
         pre-script)
             execute_pre_script
             ;;
         post-script)
             execute_post_script
```

```
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
    echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

Étape 3 : Préparer le rôle IAM d'Amazon Data Lifecycle Manager

> **Note**
>
> Cette étape est nécessaire si :
>
> - vous créez ou mettez à jour une politique d'instantanés avec pré/post-scripts activés qui utilise un rôle IAM personnalisé ;
> - vous utilisez la ligne de commande pour créer ou mettre à jour une politique d'instantanés avec pré/post-scripts activés qui utilise la valeur par défaut.
>
> Si vous utilisez la console pour créer ou mettre à jour une politique de capture d'écran activée avant ou après le script qui utilise le rôle par défaut pour la gestion des instantanés (AWSDataLifecycleManagerDefaultRole), ignorez cette étape. Dans ce cas, nous associons automatiquement la politique AWSDataLifecycleManagerSSMFulld'accès à ce rôle.

Vous devez vous assurer que ce rôle IAM que vous utilisez pour la politique accorde à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions SSM requises pour exécuter les pré-scripts et les post-scripts sur les instances ciblées par la politique.

Amazon Data Lifecycle Manager fournit une politique gérée (AWSDataLifecycleManagerSSMFullAccess) qui inclut les autorisations requises. Vous pouvez

associer cette politique à votre rôle IAM pour gérer les instantanés afin de vous assurer qu'elle inclut les autorisations.

> **Important**
>
> La politique AWSData LifecycleManager SSMFull d'accès géré utilise la clé de `aws:ResourceTag` condition pour restreindre l'accès à des documents SSM spécifiques lors de l'utilisation de scripts pré et post. Pour autoriser Amazon Data Lifecycle Manager à accéder aux documents SSM, vous devez vous assurer que vos documents SSM sont balisés avec `DLMScriptsAccess:true`.

Vous pouvez également créer manuellement une politique personnalisée ou attribuer les autorisations requises directement au rôle IAM que vous utilisez. Vous pouvez utiliser les mêmes autorisations que celles définies dans la politique AWSData LifecycleManager SSMFull d'accès géré, mais la clé de `aws:ResourceTag` condition est facultative. Si vous décidez de ne pas utiliser cette clé de condition, vous n'avez pas besoin de baliser vos documents SSM avec `DLMScriptsAccess:true`.

Utilisez l'une des méthodes suivantes pour ajouter la politique AWSDataLifecycleManagerSSMFulld'accès à votre rôle IAM.

Console

Pour attacher la politique gérée à votre rôle personnalisé

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Recherchez et sélectionnez votre rôle personnalisé pour la gestion des instantanés.
4. Sous l'onglet Permissions (Autorisations), choisissez Add Permissions (Ajouter des autorisations), Attach policies (Attacher des politiques).
5. Recherchez et sélectionnez la politique AWSDataLifecycleManagerSSMFulld'accès géré, puis choisissez Ajouter des autorisations.

AWS CLI

Pour attacher la politique gérée à votre rôle personnalisé

Utilisez la commande attach-role-policy. Pour `---role-name`, spécifiez le nom de votre rôle personnalisé. Pour `--policy-arn`, spécifiez `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`.

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

Création d'une politique de cycle de vie des instantanés

Console

Pour créer la politique de cycle de vie des instantanés

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans la page Sélectionner un type de stratégie, choisissez Stratégie d'instantané EBS, puis Suivant.
4. Dans la section Ressources cibles, effectuez les opérations suivantes :
   a. Pour Types de ressources cibles, choisissez `Instance`.
   b. Pour Balises de ressource cible, spécifiez les balises de ressource qui identifient les instances à sauvegarder. Seules les ressources possédant les balises spécifiées seront sauvegardées.
5. Pour le rôle IAM, choisissez AWSDataLifecycleManagerDefaultRole(le rôle par défaut pour la gestion des instantanés) ou choisissez un rôle personnalisé que vous avez créé et préparé pour les pré-scripts et les post-scripts.
6. Configurez les planifications et les options supplémentaires selon les besoins. Nous vous recommandons de planifier les heures de création des instantanés pour des périodes correspondant à votre charge de travail, par exemple pendant les fenêtres de maintenance.
7. Dans la section Pré-scripts et post-scripts, sélectionnez Activer les pré-scripts et post-scripts, puis effectuez les opérations suivantes :
   a. Sélectionnez Document SSM personnalisé.

b. Pour Option d'automatisation, choisissez l'option qui correspond aux scripts que vous souhaitez exécuter.

c. Pour Document SSM, sélectionnez le document SSM que vous avez préparé.

8. Configurez les options supplémentaires suivantes au besoin :

- Délai d'expiration du script : délai d'expiration au terme duquel Amazon Data Lifecycle Manager échoue à exécuter le script si celui-ci n'est pas terminé. Si un script ne s'exécute pas dans le délai imparti, Amazon Data Lifecycle Manager échoue. Le délai d'expiration s'applique aux pré-scripts et post-scripts individuellement. Le délai d'expiration minimum et par défaut est de 10 secondes. Et le délai d'expiration maximum est de 120 secondes.
- Relancer les scripts en échec : sélectionnez cette option pour relancer les scripts qui ne se terminent pas dans le délai imparti. En cas d'échec du pré-script, Amazon Data Lifecycle Manager relance l'intégralité du processus de création d'instantanés, y compris l'exécution des pré-scripts et post-scripts. Si le post-script échoue, Amazon Data Lifecycle Manager relance uniquement le post-script ; dans ce cas, le pré-script sera terminé et l'instantané aura peut-être été créé.
- Prise par défaut d'instantanés en cas de panne : sélectionnez cette option pour utiliser par défaut des instantanés en cas de panne si le pré-script ne s'exécute pas. Il s'agit du comportement de création d'instantanés par défaut pour Amazon Data Lifecycle Manager si les pré-scripts et post-scripts ne sont pas activés. Si vous avez activé les relances, Amazon Data Lifecycle Manager utilise par défaut des instantanés en cas de panne uniquement une fois que toutes les relances ont été épuisées. Si le pré-script échoue et que vous n'utilisez pas par défaut des instantanés en cas de panne, Amazon Data Lifecycle Manager ne crée pas d'instantanés pour l'instance pendant cette exécution planifiée.

9. Choisissez Créer une politique par défaut.

> **Note**
>
> Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists`, consultez Résoudre les problèmes liés à Amazon Data Lifecycle Manager pour plus d'informations.

AWS CLI

Pour créer la politique de cycle de vie des instantanés

Utilisez la create-lifecycle-policycommande et incluez les `Scripts` paramètres dans`CreateRule`. Pour plus d'informations sur les paramètres, consultez la référence d'API Amazon Data Lifecycle Manager.

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

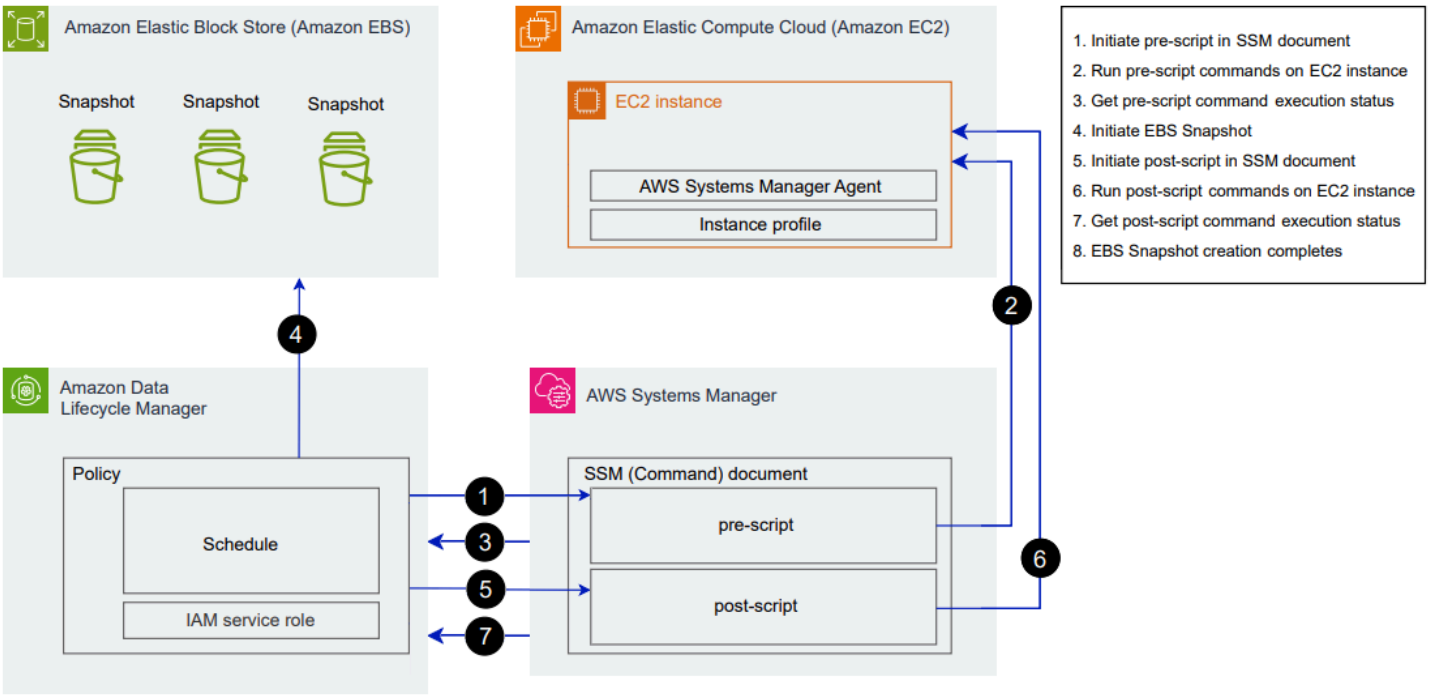
Où `policyDetails.json` inclut les éléments suivants.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE" | "POST" | "PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
```

```
}
```

Comment fonctionnent les scripts avant et après Amazon Data Lifecycle Manager

L'image suivante montre le flux de processus pour les pré-scripts et les post-scripts lors de l'utilisation de documents SSM personnalisés. Cela ne s'applique pas aux sauvegardes VSS.



Au moment prévu de la création d'instantanés, les actions et interactions entre services suivantes se produisent.

1. Amazon Data Lifecycle Manager lance l'action de pré-script en appelant le document SSM et en transmettant le paramètre `pre-script`.

   > **Note**
   >
   > Les étapes 1 à 3 se produisent uniquement si vous exécutez des pré-scripts. Si vous exécutez uniquement des post-scripts, les étapes 1 à 3 sont ignorées.

2. Systems Manager envoie des commandes de pré-script à l'agent SSM exécuté sur les instances cibles. L'agent SSM exécute les commandes sur l'instance et renvoie les informations sur les statuts à Systems Manager.

Par exemple, si le document SSM est utilisé pour créer des instantanés cohérents par rapport à l'application, le pré-script peut geler et vider les E/S afin de garantir que toutes les données mises en mémoire tampon sont écrites sur le volume avant la prise de l'instantané.

3. Systems Manager envoie des mises à jour du statut des commandes pré-script à Amazon Data Lifecycle Manager. Si le pré-script échoue, Amazon Data Lifecycle Manager effectue l'une des actions suivantes, en fonction de votre configuration des options de pré-script et de post-script :

Relances	Instantanés en cas de panne par défaut	Action
Activées avec des relances restantes	Activées	Relance du script jusqu'à ce qu'il réussisse ou que les relances soient épuisées
Épuisées sans exécution réussie	Activées	Création d'instantanés en cas de panne, sans exécution de post-script.
Activées avec des relances restantes	Désactivées	Relance du script jusqu'à ce qu'il réussisse ou que les relances soient épuisées
Épuisées sans exécution réussie	Désactivées	Création d'instantanés ignorée pour l'instance cible, sans exécution de post-script.
Désactivées	Activées	Création d'instantanés en cas de panne, sans exécution de post-script.
Désactivées	Désactivées	Création d'instantanés ignorée pour l'instance cible, sans exécution de post-script.

4. Amazon Data Lifecycle Manager lance la création d'instantanés.
5. Amazon Data Lifecycle Manager lance l'action de post-script en appelant le document SSM et en transmettant le paramètre `post-script`.

> **Note**
>
> Les étapes 5 à 7 se produisent uniquement si vous exécutez des pré-scripts. Si vous exécutez uniquement des post-scripts, les étapes 1 à 3 sont ignorées.

6. Systems Manager envoie des commandes de post-script à l'agent SSM exécuté sur les instances cibles. L'agent SSM exécute les commandes sur l'instance et renvoie les informations sur les statuts à Systems Manager.

   Par exemple, si le document SSM autorise les instantanés cohérents par rapport à l'application, ce post-script peut dégeler les E/S afin de garantir que vos bases de données reprennent leurs opérations d'E/S normales après la prise de l'instantané.

7. Si vous exécutez un post-script et que Systems Manager indique qu'il s'est correctement terminé, le processus se termine.

   Si le post-script échoue, Amazon Data Lifecycle Manager effectue l'une des actions suivantes, en fonction de votre configuration des options de pré-script et de post-script :

Nouvelle tentative	Action
Activées avec des relances restantes	Relance du post-script jusqu'à ce qu'il réussisse ou que les relances soient épuisées
Épuisées sans succès	Post-script ignoré
Désactivées	Post-script ignoré

   N'oubliez pas qu'en cas d'échec du post-script, le pré-script (s'il est activé) se termine avec succès et les instantanés ont peut-être été créés. Vous devrez peut-être prendre d'autres mesures sur l'instance pour vous assurer qu'elle fonctionne comme prévu. Par exemple, si le pré-script a suspendu et vidé les E/S, mais que le post-script n'a pas réussi à dégeler les E/S, vous devrez peut-être configurer votre base de données pour dégeler automatiquement les E/S ou vous devrez dégeler les E/S manuellement.

8. Le processus de création d'instantanés peut se terminer une fois le post-script terminé. Le temps nécessaire pour terminer l'instantané dépend de la taille de l'instantané.

Identifiez les instantanés créés avec les scripts pré et post de Data Lifecycle Manager

Amazon Data Lifecycle Manager attribue automatiquement les balises système suivantes aux instantanés créés à l'aide de pré-scripts et de post-scripts.

- Clé : `aws:dlm:pre-script` ; Valeur : `SUCCESS|FAILED`

  Une valeur de balise de `SUCCESS` indique que le pré-script a été exécuté correctement. Une valeur de balise de `FAILED` indique que le pré-script n'a pas été exécuté correctement.
- Clé : `aws:dlm:post-script` ; Valeur : `SUCCESS|FAILED`

  Une valeur de balise de `SUCCESS` indique que le post-script a été exécuté correctement. Une valeur de balise de `FAILED` indique que le post-script n'a pas été exécuté correctement.

Pour les documents SSM personnalisés et les sauvegardes SAP HANA, vous pouvez déduire la création réussie d'un instantané cohérent par rapport à l'application si l'instantané est balisé avec `aws:dlm:pre-script:SUCCESS` et `aws:dlm:post-script:SUCCESS`.

En outre, les instantanés cohérents par rapport à l'application créés à l'aide de la sauvegarde VSS sont automatiquement balisés avec :

- Clé : `AppConsistent tag` ; Valeur : `true|false`

  Une valeur de balise égale à `true` indique que la sauvegarde VSS a réussi et que les instantanés sont cohérents avec l'application. Une valeur de balise égale à `false` indique que la sauvegarde VSS n'a pas réussi et que les instantanés ne sont pas cohérents avec l'application.

Surveillez les scripts avant et après Amazon Data Lifecycle Manager

CloudWatch Métriques Amazon

Amazon Data Lifecycle Manager publie les CloudWatch indicateurs suivants lorsque les scripts pré et post échouent et réussissent et lorsque les sauvegardes VSS échouent et réussissent.

- `PreScriptStarted`
- `PreScriptCompleted`
- `PreScriptFailed`

- `PostScriptStarted`
- `PostScriptCompleted`
- `PostScriptFailed`
- `VSSBackupStarted`
- `VSSBackupCompleted`
- `VSSBackupFailed`

Pour de plus amples informations, veuillez consulter Surveillez les politiques de Data Lifecycle Manager à l'aide CloudWatch.

Amazon EventBridge

Amazon Data Lifecycle Manager émet l' EventBridge événement Amazon suivant lorsqu'un pré-script ou un post-script est lancé, réussit ou échoue

- `DLM Pre Post Script Notification`

Pour de plus amples informations, veuillez consulter Surveillez les politiques de Data Lifecycle Manager à l'aide EventBridge.

Créez une politique personnalisée Amazon Data Lifecycle Manager pour les applications soutenues par EBS AMIs

La procédure suivante montre comment utiliser Amazon Data Lifecycle Manager pour automatiser les cycles de vie des AMI Amazon EBS.

Rubriques

Pour créer une politique de cycle de vie d'AMI

Utilisez l'une des procédures suivantes pour créer une politique de cycle de vie d'AMI.

Console

Pour créer une politique d'AMI

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans l'écran Sélectionner un type de stratégie, choisissez Stratégie d'AMI EBS, puis Suivant.
4. Dans la section Ressources cibles, pour Etiquettes de ressources cibles, choisissez les étiquettes de ressources qui identifient les volumes ou les instances à sauvegarder. La politique sauvegarde uniquement les ressources ayant la clé de balise et les paires de valeurs spécifiées.
5. Pour Description, saisissez une brève description pour la stratégie.
6. Pour le rôle IAM, choisissez le rôle IAM autorisé à gérer, à créer des instantanés AMIs et à décrire les instances. Pour utiliser le rôle par défaut fourni par Amazon Data Lifecycle Manager, choisissez Rôle par défaut. Autrement, pour utiliser un rôle IAM personnalisé que vous avez créé précédemment, sélectionnez Choisir un autre rôle, puis sélectionnez le rôle à utiliser.
7. Pour Etiquettes de stratégie, ajoutez les étiquettes à appliquer à la stratégie de cycle de vie. Vous pouvez utiliser ces étiquettes pour identifier et catégoriser vos politiques.
8. Pour Statut de la stratégie après création, choisissez Activer la stratégie pour lancer l'exécutions de la stratégie lors de la prochaine heure planifiée ou Désactiver la stratégie pour empêcher l'exécution de la stratégie. Si vous n'activez pas la politique maintenant, elle ne commencera pas à être créée AMIs tant que vous ne l'aurez pas activée manuellement après sa création.
9. Dans la section Redémarrage d'instance, indiquez si les instances doivent être redémarrées avant la création de l'AMI. Pour empêcher le redémarrage des instances ciblées, choisissez Non. Le choix de Non peut occasionner des problèmes de cohérence des données. Pour redémarrer les instances avant la création de l'AMI, choisissez Oui. Ce choix garantit la cohérence des données, mais peut entraîner le redémarrage simultané de plusieurs instances ciblées.
10. Choisissez Suivant.
11. Dans l'écran Configurer une planification, configurez les planifications de stratégie. Une politique peut avoir jusqu'à quatre planifications. La planification 1 est obligatoire. Les

planifications 2, 3 et 4 sont facultatives. Pour chaque planification de politique que vous ajoutez, procédez comme suit :

a. Dans la section Détails de la planification, procédez comme suit :

   i. Pour Nom de la planification, spécifiez un nom descriptif pour la planification.

   ii. Pour Fréquence et les champs associés, configurez l'intervalle entre les exécutions de stratégie.

   Vous pouvez configurer les exécutions de politique selon une planification quotidienne, hebdomadaire, mensuelle ou annuelle. Vous pouvez également sélectionner Expression cron personnalisée pour spécifier un intervalle allant jusqu'à un an. Pour plus d'informations, consultez les sections Cron et rate dans le guide de l' EventBridge utilisateur Amazon.

   iii. Pour Démarrage à, spécifiez l'heure de démarrage des exécutions de la stratégie. La première exécution de la politique commence dans l'heure qui suit l'heure que vous planifiez. L'heure doit être au format UTC `hh:mm`.

   iv. Pour Type de rétention, spécifiez la politique de rétention AMIs créée par le planning.

   Vous pouvez les conserver AMIs en fonction de leur nombre total ou de leur âge.

   Pour la rétention basée sur le nombre, la plage s'étend de `1` à `1000`. Une fois le nombre maximum atteint, l'AMI la plus ancienne est supprimée lors de la création d'une nouvelle AMI.

   Pour la rétention basée sur l'âge, la plage s'étend de `1` jour à `100` ans. Une fois la période de rétention de chaque AMI expirée, celle-ci est supprimée.

   > **Note**
   >
   > Toutes les planifications doivent avoir le même type de conservation. Vous pouvez spécifier le type de conservation pour la planification 1 uniquement. Les planifications 2, 3 et 4 héritent du type de conservation de la planification 1. Chaque planification peut avoir son propre nombre ou sa propre période de conservation.

b. Configurez le balisage pour. AMIs

Dans la section Etiquetage, procédez comme suit :

i. Pour copier toutes les balises définies par l'utilisateur de l'instance source vers celle AMIs créée par le calendrier, sélectionnez Copier les balises depuis la source.

ii. Par défaut, les instances AMIs créées par le planning sont automatiquement étiquetées avec l'ID de l'instance source. Afin d’empêcher ce balisage automatique, pour Etiquettes de variables, supprimez la vignette `instance-id:$(instance-id)`.

iii. Pour spécifier des balises supplémentaires à attribuer à AMIs celles créées par ce calendrier, choisissez Ajouter des balises.

c. Configurez l’obsolescence des AMI.

Pour déterminer à quel AMIs moment ils ne doivent plus être utilisés, dans la section Obsolation de l'AMI, sélectionnez Activer la dépréciation de l'AMI pour ce calendrier, puis spécifiez la règle de dépréciation de l'AMI. La règle de dépréciation de l'AMI indique à quel moment AMIs la dépréciation doit être effectuée.

Si le calendrier utilise la rétention des AMI basée sur le dénombrement, vous devez spécifier le nombre des plus anciennes AMIs à déprécier. Le nombre d’obsolescences doit être inférieur ou égal au nombre de rétention d’AMI de la planification, et il ne peut être supérieur à 1 000. Par exemple, si le planning est configuré pour en conserver un maximum de 5 AMIs, vous pouvez configurer le planning pour qu'il soit déprécié jusqu'aux 5 plus anciens. AMIs

Si le calendrier utilise la rétention des AMI basée sur l'âge, vous devez spécifier la période après laquelle AMIs elles seront déconseillées. Le délai d’obsolescence doit être inférieur ou égal à la période de rétention d’AMI du planificateur, et il ne peut pas être supérieur à 10 ans (soit 120 mois, 520 semaines ou 3 650 jours). Par exemple, si le calendrier est configuré pour être conservé AMIs pendant 10 jours, vous pouvez le configurer pour qu'il soit déprécié AMIs après des périodes allant jusqu'à 10 jours après sa création.

d. Configurez la copie entre régions.

Pour copier les AMIs données créées par le calendrier vers différentes régions, dans la section Copie entre régions, sélectionnez Activer la copie entre régions. Vous pouvez AMIs effectuer une copie dans un maximum de trois régions supplémentaires dans votre

compte. Vous devez spécifier une règle de copie entre régions distincte pour chaque région de destination.

Pour chaque Région de destination, vous pouvez spécifier les informations suivantes :

- Règle de rétention pour les copies d'AMI. Lorsque la période de rétention expire, la copie dans la Région de destination est automatiquement supprimée.
- Statut de chiffrement des copies d'AMI. Si l'AMI source est chiffrée ou si le chiffrement est activé par défaut, les copies AMIs sont toujours chiffrées. Si l'AMI source n'est pas chiffrée et que le chiffrement par défaut est désactivé, vous pouvez activer le chiffrement. Si vous ne spécifiez pas de clé KMS, celles-ci AMIs sont chiffrées à l'aide de la clé KMS par défaut pour le chiffrement EBS dans chaque région de destination. Si vous spécifiez une clé KMS pour la Région de destination, le rôle IAM sélectionné doit avoir accès à la clé KMS.
- Règle d'obsolescence pour les copies d'AMI. Les copies d'AMI deviennent automatiquement obsolètes lorsque la période d'obsolescence expire. La période d'obsolescence doit être inférieure ou égale à la période de rétention de la copie et ne peut être supérieure à 10 ans.
- Que ce soit pour copier toutes les balises ou aucune balise de l'AMI source.

> **Note**
>
> Ne dépassez pas le nombre de copies d'AMI simultanées par région.

e. Pour ajouter des planifications, choisissez l'option Ajouter une planification en haut de l'écran. Pour chaque planification supplémentaire, remplissez les champs comme décrit précédemment dans cette rubrique.

f. Après avoir ajouté les planifications requises, choisissez Examiner une stratégie.

12. Examinez le récapitulatif de la stratégie, puis choisissez Créer une stratégie.

> **Note**
>
> Si vous obtenez l'erreur `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists`, consultez Résoudre les problèmes liés à Amazon Data Lifecycle Manager pour plus d'informations.

Command line

Utilisez la create-lifecycle-policycommande pour créer une politique de cycle de vie de l'AMI. Pour `PolicyType`, spécifiez `IMAGE_MANAGEMENT`.

> **Note**
>
> Pour simplifier la syntaxe, les exemples suivants utilisent un fichier JSON, `policyDetails.json`, qui comportent les détails de la stratégie.

Exemple 1 : rétention basée sur l'âge et obsolescence d'AMI

Cet exemple crée une politique de cycle de vie AMIs des AMI qui crée toutes les instances dont la clé `purpose` de balise a une valeur de `production` sans redémarrer les instances ciblées. La politique comporte une planification qui crée une AMI tous les jours à `01:00` (UTC). La politique est conservée AMIs pendant des 2 jours et les déprécie jour après 1 jour. Il copie également les balises de l'instance source vers celle AMIs qu'il crée.

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "purpose",
        "Value": "production"
    }],
    "Schedules": [{
            "Name": "DailyAMIs",
            "TagsToAdd": [{
                "Key": "type",
```

```
                "Value": "myDailyAMI"
            }],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "01:00"
                ]
            },
            RetainRule":{
                "Interval" : 2,
                "IntervalUnit" : "DAYS"
            },
            DeprecateRule": {
                "Interval" : 1,
                "IntervalUnit" : "DAYS"
            },
            "CopyTags": true
        }
    ],
    "Parameters" : {
        "NoReboot":true
    }
}
```

Si la demande aboutit, la commande renvoie l'ID de la politique nouvellement créée. Voici un exemple de sortie.

```
{
   "PolicyId": "policy-9876543210abcdef0"
}
```

Exemple 2 : rétention basée sur le nombre et obsolescence de l'AMI avec copie inter-Régions

Cet exemple crée une politique de cycle de vie AMIs de l'AMI qui crée toutes les instances dont la clé de `purpose` balise a la valeur de `production` et redémarre les instances cibles. La politique comporte une planification qui crée une AMI toutes les 6 heures à partir de `17:30` (UTC). La politique conserve 3 AMIs et déconseille automatiquement les plus anciennes. 2 AMIs Il dispose également d'une règle de copie entre régions qui copie`us-east-1`, conserve AMIs les copies de l'2AMI et déconseille automatiquement l'AMI la plus ancienne.

```
aws dlm create-lifecycle-policy \
```

```
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

Voici un exemple du fichier `policyDetails.json`.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes" : [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key":"purpose",
        "Value":"production"
    }],
    "Parameters" : {
          "NoReboot": true
    },
    "Schedules" : [{
        "Name" : "Schedule1",
        "CopyTags": true,
        "CreateRule" : {
            "Interval": 6,
            "IntervalUnit": "HOURS",
            "Times" : ["17:30"]
        },
        "RetainRule":{
            "Count" : 3
        },
        "DeprecateRule":{
            "Count" : 2
        },
        "CrossRegionCopyRules": [{
            "TargetRegion": "us-east-1",
            "Encrypted": true,
            "RetainRule":{
                "IntervalUnit": "DAYS",
                "Interval": 2
            },
            "DeprecateRule":{
                "IntervalUnit": "DAYS",
```

```
                "Interval": 1
            },
            "CopyTags": true
        }]
    }]
}
```

Considérations relatives aux stratégies de cycle de vie des AMI

Les considérations générales suivantes s'appliquent lors de la création de stratégies de cycle de vie d'AMI :

- Les politiques de cycle de vie des AMI ciblent uniquement les instances qui se trouvent dans la même région que la politique.
- La première opération de création d'AMI démarre dans l'heure suivant l'heure de début spécifiée. Les opérations suivantes de création d'AMI démarrent dans l'heure suivant leur heure planifiée.
- Lorsque Amazon Data Lifecycle Manager désenregistre une AMI, il la supprime automatiquement.
- Les balises de ressource cible sont sensibles à la casse.
- Si vous supprimez les balises cibles d'une instance ciblée par une politique, Amazon Data Lifecycle Manager ne gère plus les balises existantes AMIs dans le standard ; vous devez les supprimer manuellement si elles ne sont plus nécessaires.
- Vous pouvez créer plusieurs stratégies pour sauvegarder une instance . Par exemple, si une instance possède deux balises, la balise A étant la cible de la politique A visant à créer une AMI toutes les 12 heures, et la balise B étant la cible de la politique B visant à créer une AMI toutes les 24 heures, Amazon Data Lifecycle Manager crée AMIs conformément aux calendriers des deux politiques. Vous pouvez également obtenir le même résultat en créant une seule politique comportant plusieurs planifications. Par exemple, vous pouvez créer une politique unique qui cible uniquement la balise A et spécifier deux planifications : l'une pour toutes les 12 heures et l'autre pour toutes les 24 heures.
- Les nouveaux volumes attachés à une instance cible après la création de la stratégie sont automatiquement inclus dans la sauvegarde lors de la prochaine exécution de la stratégie. Tous les volumes attachés à l'instance au moment de l'exécution de la politique sont inclus.
- Si vous créez une stratégie avec une planification personnalisée basée sur les crons configurée pour créer une seule AMI, la stratégie ne désenregistrera pas automatiquement cette AMI lorsque le seuil de rétention est atteint. Vous devez désenregistrer manuellement l'AMI si elle n'est plus nécessaire.

- Si vous créez une politique basée sur l’âge dans laquelle la période de conservation est plus courte que la fréquence de création, Amazon Data Lifecycle Manager conservera toujours la dernière AMI jusqu’à la création de la suivante. Par exemple, si une politique basée sur l’âge crée une AMI par mois avec une période de conservation de sept jours, Amazon Data Lifecycle Manager conservera chaque AMI pendant un mois, même si la période de conservation est de sept jours.
- Pour les politiques basées sur le nombre, Amazon Data Lifecycle Manager crée toujours en AMIs fonction de la fréquence de création avant de tenter de désenregistrer l'AMI la plus ancienne conformément à la politique de rétention.
- Le désenregistrement d’une AMI et la suppression des instantanés de sauvegarde associés peuvent prendre plusieurs heures. Si Amazon Data Lifecycle Manager crée l'AMI suivante avant que l'AMI créée précédemment ne soit désenregistrée avec succès, vous pouvez conserver temporairement un nombre supérieur à votre nombre de AMIs rétention.

Les considérations suivantes s’appliquent à la résiliation des instances ciblées par une politique :

- Si vous mettez fin à une instance ciblée par une politique avec un calendrier de rétention basé sur le nombre, la politique ne gère plus AMIs ce qu'elle a créé précédemment à partir de l'instance résiliée. Vous devez les désenregistrer manuellement plus tôt AMIs s'ils ne sont plus nécessaires.
- Si vous mettez fin à une instance ciblée par une politique avec un calendrier de rétention basé sur l'âge, la politique continue de désenregistrer les instances précédemment créées à partir de l'instance résiliée selon le calendrier défini, jusqu'à la dernière AMI, mais sans inclure AMIs cette dernière. Vous devez désenregistrer manuellement la dernière AMI si elle n’est plus nécessaire.

Les considérations suivantes s’appliquent aux politiques d’AMI et à l’obsolescence des AMI :

- Si vous augmentez le nombre de dépréciations de l'AMI pour un calendrier dont la rétention est basée sur le décompte, la modification est appliquée à tous les programmes AMIs (existants et nouveaux) créés par le calendrier.
- Si vous augmentez la période d'obsolescence de l'AMI pour un calendrier avec rétention basée sur l'âge, la modification s'applique uniquement aux nouveaux. AMIs AMIs Les existants ne sont pas affectés.
- Si vous supprimez la règle de dépréciation de l'AMI d'un calendrier, Amazon Data Lifecycle Manager n'annulera pas la règle d'obsolescence précédemment déconseillée par AMIs ce calendrier.

- Si vous diminuez le nombre ou la période d'obsolescence des AMI pour une planification, Amazon Data Lifecycle Manager n'annulera pas la dépréciation de celles AMIs qui étaient précédemment déconseillées par cette planification.
- Si vous rendez manuellement obsolète une AMI créée par une politique d'AMI, Amazon Data Lifecycle Manager ne remplacera pas l'obsolescence.
- Si vous annulez manuellement l'obsolescence d'une AMI précédemment rendue obsolète par une politique AMI, Amazon Data Lifecycle Manager ne remplacera pas l'annulation.
- Si une AMI est créée par plusieurs planifications conflictuelles et qu'une ou plusieurs de ces planifications n'ont pas de règle d'obsolescence des AMI, Amazon Data Lifecycle Manager ne rendra pas cette AMI obsolète.
- Si une AMI est créée par plusieurs planifications conflictuelles et que toutes ces planifications disposent d'une règle d'obsolescence des AMI, Amazon Data Lifecycle Manager utilisera la règle d'obsolescence qui donne la date d'obsolescence la plus tardive.

Les considérations suivantes s'appliquent aux politiques de l'AMI et à la corbeille :

- Si Amazon Data Lifecycle Manager annule l'enregistrement d'une AMI et l'envoie à la corbeille lorsque le seuil de rétention de la politique est atteint, et que vous restaurez manuellement l'AMI à partir de la corbeille, vous devez annuler manuellement l'enregistrement de cette AMI lorsqu'elle n'est plus nécessaire. Amazon Data Lifecycle Manager ne gérera plus l'AMI.
- Si vous annulez manuellement l'enregistrement d'une AMI créée par une politique et que cette AMI se trouve dans la corbeille lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager n'annule pas l'enregistrement de l'AMI. Amazon Data Lifecycle Manager ne les gère pas AMIs lorsqu'ils sont dans la corbeille.

  Si l'AMI est restaurée à partir de la corbeille avant que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager annule l'enregistrement de l'AMI lorsque le seuil de rétention de la politique est atteint.

  Si l'AMI est restaurée à partir de la corbeille après que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager n'annule plus l'enregistrement de l'AMI. Vous devez la supprimer manuellement lorsqu'elle n'est plus nécessaire.

Les considérations suivantes s'appliquent aux politiques d'AMI qui sont à l'état d'erreur :

- Pour les politiques avec des calendriers de conservation basés sur l'âge, AMIs qui sont définis pour expirer alors que la politique est en vigueur, sont `error` conservées indéfiniment. Vous devez le désenregistrer manuellement. AMIs Lorsque vous réactivez cette politique, Amazon Data Lifecycle Manager recommence à se désinscrire à l'expiration de sa période de conservation AMIs .
- Pour les politiques dont les calendriers de rétention sont basés sur le nombre, la politique arrête de créer et de désenregistrer AMIs tant qu'elle est dans l'État. `error` Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager reprend la création AMIs, et le désenregistrement reprend lorsque le seuil de rétention est atteint AMIs .

Les considérations suivantes s'appliquent aux politiques d'AMI et à leur désactivation AMIs :

- Si vous désactivez une AMI créée par Amazon Data Lifecycle Manager et que cette AMI est désactivée lorsque son seuil de rétention est atteint, Amazon Data Lifecycle Manager désenregistre l'AMI et supprime les instantanés associés.
- Si vous désactivez une AMI créée par Amazon Data Lifecycle Manager et que vous archivez manuellement les instantanés associés, et que ces instantanés sont archivés lorsque leur seuil de rétention est atteint, Amazon Data Lifecycle Manager ne supprimera pas ces instantanés et ne les gérera plus.

Les considérations suivantes s'appliquent aux politiques de l'AMI et à la protection contre le désenregistrement de l'AMI :

- Si vous activez manuellement la protection de désenregistrement pour une AMI créée par Amazon Data Lifecycle Manager et qu'elle est toujours activée lorsque le seuil de rétention de l'AMI est atteint, Amazon Data Lifecycle Manager ne gère plus cette AMI. Vous devez annuler manuellement l'enregistrement de l'AMI et supprimer ses instantanés sous-jacents s'ils ne sont plus nécessaires.

Ressources supplémentaires

Pour plus d'informations, consultez le blog Automating Amazon EBS snapshot and AMI management using Amazon Data Lifecycle Manager AWS storage.

Automatisez les copies instantanées entre comptes avec Data Lifecycle Manager

L'automatisation des copies d'instantanés entre comptes vous permet de copier vos instantanés Amazon EBS vers des régions spécifiques dans un compte isolé et de chiffrer ces instantanés à l'aide d'une clé de chiffrement. Cela vous permet de vous protéger contre la perte de données en cas de compromission de votre compte.

L'automatisation des copies d'instantanés entre comptes implique deux comptes :

- Compte source : le compte source est le compte qui crée et partage les instantanés avec le compte cible. Dans ce compte, vous devez créer une politique de capture instantanée EBS qui crée des instantanés à intervalles définis, puis les partage avec d'autres AWS comptes.
- Compte cible : le compte cible est le compte avec le compte de destination avec lequel les instantanés sont partagés, et qui crée des copies des instantanés partagés. Dans ce compte, vous devez créer une politique d'événement de copie entre comptes qui copie automatiquement les instantanés qui sont partagés avec lui par un ou plusieurs comptes source spécifiés.

Rubriques

Créer des politiques de copie d'instantané entre comptes

Pour préparer les comptes source et cible pour la copie des instantanés entre comptes, vous devez procéder comme suit :

Étape 1 : créer la stratégie d'instantané EBS (compte source)

Dans le compte source, créez une politique d'instantanés EBS qui créera les instantanés et partagera ceux-ci avec les comptes cibles requis.

Lorsque vous créez la politique, assurez-vous d'activer le partage entre comptes et de spécifier les AWS comptes cibles avec lesquels partager les instantanés. Il s'agit des comptes avec lesquels les instantanés doivent être partagés. Si vous partagez des instantanés chiffrés, vous devez accorder

aux comptes cibles sélectionnés l'autorisation d'utiliser la clé KMS utilisée pour chiffrer le volume source. Pour plus d'informations, consultez Étape 2 : partager la clé clé gérée par le client (compte source).

> **Note**
>
> Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être partagés. Vous ne pouvez pas partager d'instantanés chiffrés à l'aide de la clé KMS de chiffrement EBS par défaut. Si vous partagez des instantanés chiffrés, vous devez également partager la clé KMS utilisée pour chiffrer le volume source avec les comptes cibles. Pour plus d'informations, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur la création d'une politique d'instantané EBS, consultez Création d'une politique personnalisée Amazon Data Lifecycle Manager pour les instantanés EBS.

Utilisez l'une des méthodes suivantes pour créer la politique d'instantanés EBS.

Étape 2 : partager la clé clé gérée par le client (compte source)

Si vous partagez des instantanés chiffrés, vous devez accorder au rôle IAM et aux comptes AWS cibles (que vous avez sélectionnés à l'étape précédente) les autorisations d'utiliser la clé clé gérée par le client utilisée pour chiffrer le volume source.

> **Note**
>
> Ne suivez cette étape que si vous partagez des instantanés chiffrés. Si vous partagez des instantanés non chiffrés, ignorez cette étape.

Console

1. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Dans le panneau de navigation, choisissez Clés gérées par le client, puis sélectionnez la clé CMK à partager avec les comptes cibles.

Prenez note de l'ARN de la clé KMS, car vous aurez besoin de celui-ci plus tard.

4. Sous l'onglet Stratégie de clé, faites défiler la page jusqu'à la section Utilisateurs de clé. Sélectionnez Ajouter, saisissez le nom du rôle IAM sélectionné à l'étape précédente, puis sélectionnez Ajouter.
5. Sous l'onglet Stratégie de clé, faites défiler la page jusqu'à la section Autres comptes AWS . Choisissez Ajouter d'autres AWS comptes, puis ajoutez tous les AWS comptes cibles avec lesquels vous avez choisi de partager les instantanés à l'étape précédente.
6. Sélectionnez Enregistrer les modifications.

Command line

Utilisez la get-key-policycommande pour récupérer la politique de clé actuellement attachée à la clé KMS.

Par exemple, la commande suivante récupère la stratégie d'une clé clé KMS présentant l'ID `9d5e2b3d-e410-4a27-a958-19e220d83a1e` et l'écrit dans un fichier nommé `snapshotKey.json`.

```
$ aws kms get-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --query Policy \
    --output text > snapshotKey.json
```

Ouvrez la politique de clé à l'aide de l'éditeur de texte de votre choix. Ajoutez l'ARN du rôle IAM que vous avez spécifié lors de la création de la politique de capture instantanée et celui ARNs des comptes cibles avec lesquels partager la clé KMS.

Par exemple, dans la stratégie suivante, nous avons ajouté l'ARN du rôle IAM par défaut et l'ARN du compte racine pour le compte cible `222222222222`.

> **Tip**
>
> Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour autoriser l'utilisateur à créer des autorisations sur la clé KMS uniquement lorsque

l'autorisation est créée en son nom par un AWS service, comme indiqué dans l'exemple suivant.

```
{
    "Sid" : "Allow use of the key",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Allow attachment of persistent resources",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
```

```
    }
}
```

Enregistrez et fermez le fichier . Utilisez ensuite la put-key-policycommande pour associer la politique de clé mise à jour à la clé KMS.

```
$ aws kms put-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --policy file://snapshotKey.json
```

Étape 3 : créer une stratégie d'événement de copie entre comptes (compte cible)

Dans le compte cible, vous devez créer une politique d'événement de copie entre comptes qui copiera automatiquement les instantanés partagés par les comptes source requis.

Cette politique s'exécute uniquement dans le compte cible lorsque l'un des comptes sources spécifiés partage l'instantané avec le compte.

Utilisez l'une des méthodes suivantes pour créer la politique d'événement de copie entre comptes.

Console

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Elastic Block Store, Gestionnaire de cycle de vie, puis Créer une stratégie de cycle de vie d'instantané.
3. Dans l'écran Sélectionner un type de stratégie, choisissez Stratégie d'événement de copie entre comptes, puis Suivant.
4. Pour Description de la stratégie, entrez une brève description de la stratégie.
5. Pour Etiquettes de stratégie, ajoutez les étiquettes à appliquer à la stratégie de cycle de vie. Vous pouvez utiliser ces étiquettes pour identifier et catégoriser vos politiques.
6. Dans la section Paramètres de l'événement, définissez l'événement de partage d'instantané qui entraînera l'exécution de la stratégie. Procédez comme suit :

    a. Pour Partage de comptes, spécifiez les AWS comptes sources à partir desquels vous souhaitez copier les instantanés partagés. Choisissez Ajouter un compte, entrez l'identifiant de AWS compte à 12 chiffres, puis sélectionnez Ajouter.

b. Pour Filtrer par description, saisissez la description d'instantané requise en utilisant une expression régulière. Seuls les instantanés partagés par les comptes sources spécifiés et dont les descriptions correspondent au filtre spécifié sont copiés par la politique. Pour plus d'informations, consultez Spécifier les filtres de description d'instantané.

7. Pour le rôle IAM, sélectionnez le rôle IAM autorisé à effectuer des actions de copie d'instantané. Pour utiliser le rôle par défaut fourni par Amazon Data Lifecycle Manager, choisissez Rôle par défaut. Autrement, pour utiliser un rôle IAM personnalisé que vous avez créé précédemment, sélectionnez Choisir un autre rôle, puis sélectionnez le rôle à utiliser.

   Si vous copiez des instantanés chiffrés, vous devez accorder au rôle IAM sélectionné les autorisations nécessaires pour utiliser la clé de chiffrement clé KMS utilisée pour chiffrer le volume source. De même, si vous chiffrez l'instantané dans la région de destination à l'aide d'une autre clé KMS, vous devez accorder au rôle IAM l'autorisation d'utiliser la clé KMS de destination. Pour plus d'informations, consultez Étape 4 : autoriser le rôle IAM à utiliser les clés Clés KMS requises (compte cible).

8. Dans la section Copier une action, définissez les actions de copie d'instantané que la stratégie doit exécuter quand elle est activée. La politique peut copier des instantanés vers jusqu'à trois régions. Vous devez spécifier une règle de copie distincte pour chaque région de destination. Pour chaque règle que vous ajoutez, procédez comme suit :

   a. Pour Nom, saisissez un nom descriptif pour la copie.

   b. Pour Région cible, sélectionnez la région dans laquelle copier les instantanés.

   c. Pour Expirer, spécifiez la durée de rétention des copies d'instantané dans la région cible après leur création.

   d. Pour chiffrer la copie d'instantané, pour Chiffrement, sélectionnez Activer le chiffrement. Si l'instantané source est chiffré ou si le chiffrement par défaut est activé pour votre compte, alors la copie d'instantané est toujours chiffrée, même si vous n'activez pas le chiffrement ici. Si l'instantané source n'est pas chiffré et que le chiffrement par défaut n'est pas activé pour votre compte, vous pouvez choisir d'activer ou de désactiver le chiffrement. Si vous activez le chiffrement, mais que vous ne spécifiez pas de clé KMS, les instantanés sont chiffrés à l'aide de la clé KMS de chiffrement par défaut dans chaque région de destination. Si vous spécifiez une clé KMS pour la région de destination, vous devez avoir accès à la clé KMS.

9. Pour ajouter des actions de copie d'instantané, choisissez Ajouter de nouvelles régions.

10. Pour Policy status after creation (Statut de la stratégie après création), choisissez Enable policy (Activer la stratégie) pour lancer les exécutions de stratégie lors de la prochaine heure

planifiée ou Disable policy (Désactiver la stratégie) pour empêcher l'exécution de la stratégie. Si vous n'activez pas la politique maintenant, elle ne commencera à copier des instantanés que quand vous l'aurez activée manuellement après sa création.

11. Choisissez Create Policy (Créer une politique).

Command line

Utilisez la create-lifecycle-policycommande pour créer une politique. Pour créer une stratégie d'événement de copie entre comptes, pour `PolicyType`, spécifiez `EVENT_BASED_POLICY`.

Par exemple, la commande suivante crée une stratégie d'événement de copie entre comptes dans le compte cible `222222222222`. La stratégie copie les instantanés qui sont partagés par le compte source `111111111111`. La stratégie copie les instantanés vers `sa-east-1` et `eu-west-2`. Les instantanés copiés vers `sa-east-1` ne sont pas chiffrés et sont retenus pendant 3 jours. Les instantanés copiés vers `eu-west-2` sont chiffrés à l'aide de la clé `8af79514-350d-4c52-bac8-8985e84171c7` clé KMS et sont conservés pendant 1 mois. La politique utilise le rôle IAM par défaut.

```
$ aws dlm create-lifecycle-policy \
    --description "Copy policy" \
    --state ENABLED \
    --execution-role-arn arn:aws:iam::222222222222:role/service-role/
AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

L'exemple suivant affiche le contenu du fichier `policyDetails.json`.

```
{
    "PolicyType" : "EVENT_BASED_POLICY",
    "EventSource" : {
        "Type" : "MANAGED_CWE",
        "Parameters": {
            "EventType" : "shareSnapshot",
            "SnapshotOwner": ["111111111111"]
        }
    },
    "Actions" : [{
        "Name" :"Copy Snapshot to Sao Paulo and London",
        "CrossRegionCopy" : [{
            "Target" : "sa-east-1",
```

```
             "EncryptionConfiguration" : {
                 "Encrypted" : false
             },
             "RetainRule" : {
             "Interval" : 3,
            "IntervalUnit" : "DAYS"
            }
        },
        {
            "Target" : "eu-west-2",
            "EncryptionConfiguration" : {
                 "Encrypted" : true,
                 "CmkArn" : "arn:aws:kms:eu-
west-2:222222222222:key/8af79514-350d-4c52-bac8-8985e84171c7"
            },
            "RetainRule" : {
                "Interval" : 1,
                "IntervalUnit" : "MONTHS"
            }
        }]
    }]
}
```

Si la demande aboutit, la commande renvoie l'ID de la politique nouvellement créée. Voici un exemple de sortie.

```
{
    "PolicyId": "policy-9876543210abcdef0"
}
```

Étape 4 : autoriser le rôle IAM à utiliser les clés Clés KMS requises (compte cible)

Si vous copiez des instantanés chiffrés, vous devez accorder au rôle IAM (que vous avez sélectionné à l'étape précédente) les autorisations d'utiliser la clé gérée par le client utilisée pour chiffrer le volume source.

> **Note**
>
> Suivez cette étape uniquement si vous copiez des instantanés chiffrés. Si vous copiez des instantanés non chiffrés, ignorez cette étape.

Utilisez l'une des méthodes suivantes pour ajouter les politiques requises au rôle IAM.

Console

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Rôles. Recherchez et sélectionnez le rôle IAM que vous avez sélectionné lors de la création de la politique d'événement de copie entre comptes à l'étape précédente. Si vous avez choisi d'utiliser le rôle par défaut, celui-ci est nommé AWSDataLifecycleManagerDefaultRole.
3. Sélectionnez Ajouter une stratégie en ligne, puis l'onglet JSON.
4. Remplacez la politique existante par ce qui suit et spécifiez l'ARN de clé KMS qui a été utilisé pour chiffrer les volumes sources et qui a été partagé avec vous par le compte source à l'étape 2.

> **Note**
>
> Si vous copiez à partir de plusieurs comptes sources, vous devez spécifier l'ARN de clé KMS correspondant à partir de chaque compte source.

Dans l'exemple suivant, la stratégie accorde au rôle IAM l'autorisation d'utiliser la clé `1234abcd-12ab-34cd-56ef-1234567890ab` clé KMS, qui a été partagée par le compte source `111111111111`, et la clé `4567dcba-23ab-34cd-56ef-0987654321yz` clé KMS, qui existe dans le compte cible `222222222222`.

> **Tip**
>
> Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour autoriser l'utilisateur à créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée en son nom par un AWS service, comme indiqué dans l'exemple suivant.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

5. Choisissez Review policy (Examiner la politique)
6. Dans Nom, saisissez un nom descriptif pour la stratégie, puis sélectionnez Créer une stratégie.

Command line

À l'aide de l'éditeur de texte de votre choix, créez un fichier JSON nommé `policyDetails.json`. Ajoutez la politique suivante et spécifiez l'ARN de clé KMS qui a été utilisé pour chiffrer les volumes sources et qui a été partagé avec vous par le compte source à l'étape 2.

> **Note**
>
> Si vous copiez à partir de plusieurs comptes sources, vous devez spécifier l'ARN de clé KMS correspondant à partir de chaque compte source.

Dans l'exemple suivant, la stratégie accorde au rôle IAM l'autorisation d'utiliser la clé `1234abcd-12ab-34cd-56ef-1234567890ab` clé KMS, qui a été partagée par le compte source `111111111111`, et la clé `4567dcba-23ab-34cd-56ef-0987654321yz` clé KMS, qui existe dans le compte cible `222222222222`.

> **Tip**
>
> Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour autoriser l'utilisateur à créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée en son nom par un AWS service, comme indiqué dans l'exemple suivant.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

Enregistrez et fermez le fichier . Utilisez ensuite la put-role-policycommande pour ajouter la politique au rôle IAM.

Par exemple

```
$ aws iam put-role-policy \
    --role-name AWSDataLifecycleManagerDefaultRole \
    --policy-name CopyPolicy \
    --policy-document file://AdminPolicy.json
```

Spécifier les filtres de description d'instantané

Lorsque vous créez la politique de copie de cliché dans le compte cible, vous devez spécifier un filtre de description d'instantané. Le filtre de description d'instantané vous permet de spécifier un niveau

de filtrage supplémentaire qui vous permet de contrôler quels instantanés sont copiés par la politique. Cela signifie qu'un instantané n'est copié par la politique que s'il est partagé par l'un des comptes source spécifiés et qu'il possède une description d'instantané qui correspond au filtre spécifié. En d'autres termes, si un instantané est partagé par l'un des comptes de cours spécifiés, mais qu'il n'a pas de description correspondant au filtre spécifié, il n'est pas copié par la politique.

La description du filtre d'instantané doit être spécifiée à l'aide d'une expression régulière. Il s'agit d'un champ obligatoire lors de la création de politiques d'événement de copie entre comptes à l'aide de la console et de la ligne de commande. Voici des exemples d'expressions régulières qui peuvent être utilisées :

- `.*` : ce filtre correspond à toutes les descriptions des instantanés. Si vous utilisez cette expression, la politique copiera tous les instantanés partagés par l'un des comptes source spécifiés.
- `Created for policy: policy-0123456789abcdef0.*`—ce filtre ne correspond qu'aux instantanés créés par une stratégie dont l'ID est de `policy-0123456789abcdef0`. Si vous utilisez une expression comme celle-ci, seuls les instantanés partagés avec votre compte par l'un des comptes source spécifiés et qui ont été créés par une politique avec l'ID spécifié sont copiés par la politique.
- `.*production.*` : ce filtre correspond à n'importe quel instantané dont le mot `production` est indiqué n'importe où dans sa description. Si vous utilisez cette expression, la politique copiera tous les instantanés partagés par l'un des comptes source spécifiés et dont la description contient le texte spécifié.

Remarques relatives aux stratégies de copie d'instantané entre comptes

Les considérations suivantes s'appliquent aux politiques d'événement de copie entre comptes :

- Seuls les instantanés non chiffrés ou chiffrés à l'aide d'une clé gérée par le client peuvent être copiés.
- Vous pouvez créer une politique d'événement de copie entre comptes pour copier les instantanés partagés en dehors de Amazon Data Lifecycle Manager.
- Si vous souhaitez chiffrer les instantanés dans le compte cible, le rôle IAM sélectionné pour la politique d'événement de copie entre comptes doit être autorisé à utiliser la clé KMS requise.

Ressources supplémentaires

Pour plus d'informations, consultez le blog Automatiser la copie des instantanés Amazon EBS chiffrés sur le stockage AWS des comptes AWS .

Modifier les politiques d'Amazon Data Lifecycle Manager

Tenez compte des points suivants lorsque vous modifiez les politiques d'Amazon Data Lifecycle Manager :

- Si vous modifiez une politique d'AMI ou d'instantané en supprimant ou en modifiant ses identifications cible, les volumes ou les instances de ces identifications ne sont plus gérées par la politique.
- Si vous modifiez le nom d'une planification, les instantanés ou AMIs créés sous l'ancien nom de planification ne sont plus gérés par la politique.
- Si vous modifiez un calendrier de conservation basé sur l'âge pour utiliser un nouvel intervalle de temps, le nouvel intervalle est utilisé uniquement pour les nouveaux instantanés ou AMIs créé après la modification. Le nouveau calendrier n'affecte pas le calendrier de conservation des instantanés ou des instantanés AMIs créés avant la modification.
- Vous ne pouvez pas modifier la planification de rétention d'une politique en passant d'une politique basée sur le nombre à une politique basée sur l'âge après la création de celle-ci. Pour pouvoir effectuer ce changement, vous devez créer une nouvelle politique.
- Si vous désactivez une politique avec un calendrier de conservation basé sur l'âge, les instantanés ou ceux AMIs qui sont conçus pour expirer alors que la politique est désactivée sont conservés indéfiniment. Vous devez supprimer les instantanés ou les désenregistrer manuellement. AMIs Lorsque vous réactivez cette politique, Amazon Data Lifecycle Manager recommence à supprimer des instantanés ou à annuler l'enregistrement à l'expiration de leur période de conservation. AMIs
- Si vous désactivez une politique avec un calendrier de conservation basé sur le nombre, la politique arrête de créer et de supprimer des instantanés ou. AMIs Lorsque vous réactivez la politique, Amazon Data Lifecycle Manager recommence à créer des instantanés et AMIs recommence à supprimer des instantanés ou lorsque le seuil de rétention est AMIs atteint.
- Si vous désactivez une politique pour laquelle l'archivage des instantanés est activé, les instantanés qui se trouvent dans le niveau d'archivage au moment de la désactivation de la politique ne sont plus gérés par Amazon Data Lifecycle Manager. Vous devez supprimer l'instantané manuellement lorsqu'il n'est plus nécessaire.

- Si vous activez l'archivage des instantanés selon une planification basée sur le nombre, la règle d'archivage s'applique à tous les nouveaux instantanés créés et archivés selon la planification, ainsi qu'aux instantanés existants qui ont été précédemment créés et archivés selon la planification.
- Si vous activez l'archivage des instantanés selon une planification basée sur l'âge, la règle d'archivage s'applique uniquement aux nouveaux instantanés créés après activation de l'archivage des instantanés. Les instantanés existants créés avant l'activation de l'archivage des instantanés continuent d'être supprimés de leurs niveaux de stockage respectifs, conformément à la planification définie lors de leur création et de leur archivage initiaux.
- Si vous désactivez l'archivage des instantanés d'une planification basée sur le nombre, la planification arrête immédiatement l'archivage des instantanés. Les instantanés précédemment archivés selon la planification restent dans le niveau d'archivage et ne seront pas supprimés par Amazon Data Lifecycle Manager.
- Si vous désactivez l'archivage des instantanés d'une planification basée sur l'âge, les instantanés créés par la politique et dont l'archivage est prévu sont définitivement supprimés à la date et à l'heure d'archivage planifiées, comme indiqué par la balise système `aws:dlm:expirationTime`.
- Si vous désactivez l'archivage des instantanés d'une planification, la planification arrête immédiatement l'archivage des instantanés. Les instantanés précédemment archivés selon la planification restent dans le niveau d'archivage et ne seront pas supprimés par Amazon Data Lifecycle Manager.
- Si vous modifiez le nombre de rétention d'archivage pour une planification basée sur le nombre, le nouveau nombre de rétention inclut les instantanés existants qui étaient précédemment archivés selon la planification.
- Si vous modifiez la période de rétention d'archivage selon une planification basée sur l'âge, la nouvelle période de rétention s'applique uniquement aux instantanés archivés après modification de la règle de rétention.

Utilisez l'une des procédures suivantes pour modifier une politique de cycle de vie.

Console

Pour modifier une politique de cycle de vie

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Elastic Block Store, Lifecycle Manager (Gestionnaire de cycle de vie).

3. Sélectionnez une politique de cycle de vie dans la liste.
4. Sélectionnez Actions, puis Modifier une stratégie de cycle de vie.
5. Modifiez les paramètres de politique selon vos besoins. Par exemple, vous pouvez modifier le programme, ajouter ou supprimer des balises, ou encore activer ou désactiver la politique.
6. Choisissez Modifier la stratégie.

Command line

Utilisez la update-lifecycle-policycommande pour modifier les informations d'une politique de cycle de vie. Pour simplifier la syntaxe, cet exemple fait référence à un fichier JSON, `policyDetailsUpdated.json`, qui inclut les détails de la stratégie.

```
aws dlm update-lifecycle-policy \
    --state DISABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" \
    --policy-details file://policyDetailsUpdated.json
```

Voici un exemple du fichier `policyDetailsUpdated.json`.

```
{
   "ResourceTypes":[
      "VOLUME"
   ],
   "TargetTags":[
      {
         "Key": "costcenter",
         "Value": "120"
      }
   ],
   "Schedules":[
      {
         "Name": "DailySnapshots",
         "TagsToAdd": [
            {
               "Key": "type",
               "Value": "myDailySnapshot"
            }
         ],
         "CreateRule": {
```

```
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
               "15:00"
            ]
         },
         "RetainRule": {
            "Count" :5
         },
         "CopyTags": false
      }
   ]
}
```

Pour afficher la stratégie mise à jour, utilisez la commande `get-lifecycle-policy`. Vous pouvez voir que l'état, la valeur de la balise, l'intervalle de prise d'instantané et l'heure de début de la prise d'instantané ont été modifiés.

Supprimer les politiques d'Amazon Data Lifecycle Manager

Tenez compte des points suivants lorsque vous supprimez les politiques d'Amazon Data Lifecycle Manager :

- Si vous supprimez une politique, les instantanés ou AMIs créés par cette politique ne sont pas automatiquement supprimés. Si vous n'avez plus besoin des instantanés ou AMIs si vous devez les supprimer manuellement.
- Si vous supprimez une politique pour laquelle l'archivage des instantanés est activé, les instantanés qui se trouvent dans le niveau d'archivage au moment de la suppression de la politique ne sont plus gérés par Amazon Data Lifecycle Manager. Vous devez supprimer l'instantané manuellement lorsqu'il n'est plus nécessaire.
- Si vous supprimez une politique avec une planification basée sur l'archivage et sur l'âge, les instantanés créés par la politique et dont l'archivage est prévu sont définitivement supprimés à la date et à l'heure d'archivage planifiées, comme indiqué par la balise système `aws:dlm:expiretime`.

Utilisez l'une des procédures suivantes pour supprimer une politique de cycle de vie.

Console

Pour supprimer une politique de cycle de vie

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, choisissez Elastic Block Store, Lifecycle Manager (Gestionnaire de cycle de vie).
3. Sélectionnez une politique de cycle de vie dans la liste.
4. Sélectionnez Actions, puis Supprimer une stratégie de cycle de vie.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer une stratégie de cycle de vie.

Command line

Utilisez la delete-lifecycle-policycommande pour supprimer une politique de cycle de vie et libérer les balises cibles spécifiées dans la stratégie pour les réutiliser.

> **Note**
>
> Vous pouvez supprimer les instantanés créés uniquement par Amazon Data Lifecycle Manager.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Le manuel Référence d'API Amazon Data Lifecycle Manager contient des descriptions et la syntaxe de chacune des actions et chacun des types de données de l'API de requête Amazon Data Lifecycle Manager.

Vous pouvez également utiliser l'un des AWS SDKs pour accéder à l'API d'une manière adaptée au langage de programmation ou à la plate-forme que vous utilisez. Pour de plus amples informations, veuillez consulter AWS SDKs.

Contrôlez l'accès à Amazon Data Lifecycle Manager à l'aide d'IAM

Des informations d'identification sont nécessaires pour accéder à Amazon Data Lifecycle Manager. Ces informations d'identification doivent être autorisées à accéder aux AWS ressources, telles que les instances, les volumes, les instantanés et AMIs.

Les autorisations IAM suivantes sont requises pour utiliser Amazon Data Lifecycle Manager.

> **Note**
>
> - Les autorisations `ec2:DescribeAvailabilityZones`, `ec2:DescribeRegions`, `kms:ListAliases` et `kms:DescribeKey` sont nécessaires pour les utilisateurs de la console uniquement. Si l'accès à la console n'est pas requis, vous pouvez supprimer les autorisations.
> - Le format ARN du AWSDataLifecycleManagerDefaultRolerôle varie selon qu'il a été créé à l'aide de la console ou du AWS CLI. Si le rôle a été créé à l'aide de la console, le format ARN est `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`. Si le rôle a été créé à l'aide de AWS CLI, le format ARN est`arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dlm:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::accound_id:role/AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::accound_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement",
       "arn:aws:iam::accound_id:role/service-role/AWSDataLifecycleManagerDefaultRole",
```

```
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement"
                ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

Autorisations pour le chiffrement

Tenez compte des éléments suivants lorsque vous travaillez avec Amazon Data Lifecycle Manager et des ressources chiffrées.

- Si le volume source est chiffré, assurez-vous que les rôles par défaut (AWSDataLifecycleManagerDefaultRoleet AWSDataLifecycleManagerDefaultRoleForAMIManagement) d'Amazon Data Lifecycle Manager sont autorisés à utiliser les clés KMS utilisées pour chiffrer le volume.
- Si vous activez la copie interrégionale pour les instantanés non chiffrés ou AMIs sauvegardés par des instantanés non chiffrés, et que vous choisissez d'activer le chiffrement dans la région de destination, assurez-vous que les rôles par défaut sont autorisés à utiliser la clé KMS nécessaire pour effectuer le chiffrement dans la région de destination.
- Si vous activez la copie interrégionale pour les instantanés chiffrés ou AMIs sauvegardés par des instantanés chiffrés, assurez-vous que les rôles par défaut sont autorisés à utiliser à la fois les clés KMS source et de destination.

- Si vous activez l'archivage des instantanés chiffrés, assurez-vous que le rôle par défaut d'Amazon Data Lifecycle Manager (AWSDataLifecycleManagerDefaultRoleest autorisé à utiliser la clé KMS utilisée pour chiffrer l'instantané).

Pour plus d'informations, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations, consultez Modification des autorisations d'un utilisateur dans le Guide de l'utilisateur IAM.

AWS politiques gérées pour Amazon Data Lifecycle Manager

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants. AWS les politiques gérées vous permettent d'attribuer plus efficacement les autorisations appropriées aux utilisateurs, aux groupes et aux rôles que si vous deviez rédiger les politiques vous-même.

Toutefois, vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. AWS met à jour de temps en temps les autorisations définies dans une politique AWS gérée. Dans ce cas, la mise à jour affecte toutes les entités de principaux (utilisateurs, groupes et rôles) auxquelles la politique est attachée.

Amazon Data Lifecycle Manager fournit des politiques AWS gérées pour les cas d'utilisation courants. Ces politiques facilitent la définition des autorisations appropriées et le contrôle de l'accès à vos ressources. Les politiques AWS gérées fournies par Amazon Data Lifecycle Manager sont conçues pour être associées aux rôles que vous transmettez à Amazon Data Lifecycle Manager.

Rubriques

- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFullAccès
- AWS mises à jour des politiques gérées

AWSDataLifecycleManagerServiceRole

La AWSDataLifecycleManagerServiceRolepolitique fournit les autorisations appropriées à Amazon Data Lifecycle Manager pour créer et gérer les politiques relatives aux snapshots Amazon EBS et les politiques relatives aux événements de copie entre comptes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
```

```
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
        }
    ]
}
```

AWSDataLifecycleManagerServiceRoleForAMIManagement

La AWSDataLifecycleManagerServiceRoleForAMIManagementpolitique fournit les autorisations appropriées à Amazon Data Lifecycle Manager pour créer et gérer les politiques AMI basées sur Amazon EBS-AMI.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

AWSDataLifecycleManagerSSMFullAccès

Fournit à Amazon Data Lifecycle Manager l'autorisation d'effectuer les actions de Systems Manager requises pour exécuter des pré-scripts et des post-scripts sur toutes les EC2 instances Amazon.

> **Important**
>
> La politique utilise la clé de condition `aws:ResourceTag` pour restreindre l'accès à des documents SSM spécifiques lors de l'utilisation de pré-scripts et de post-scripts. Pour autoriser Amazon Data Lifecycle Manager à accéder aux documents SSM, vous devez vous assurer que vos documents SSM sont balisés avec `DLMScriptsAccess:true`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSMReadOnlyAccess",
            "Effect": "Allow",
```

```
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTaggedSSMDocumentsOnly",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Sid": "AllowSpecificAWSOwnedSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
                "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA"
            ]
        },
        {
            "Sid": "AllowAllEC2Instances",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ]
        }
    ]
}
```

AWS mises à jour des politiques gérées

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent parfois des autorisations supplémentaires à une politique AWS gérée pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont plus susceptibles de mettre à jour une politique AWS gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

Le tableau suivant fournit des informations sur les mises à jour des politiques AWS gérées pour Amazon Data Lifecycle Manager depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique du document pour le guide de l'utilisateur Amazon EBS.

Modification	Description	Date
AWSDataLifecycleManagerServiceRole— Mise à jour des autorisations de politique.	Amazon Data Lifecycle Manager a ajouté l'`ec2:DescribeAvailabilityZones` action permettant d'autoriser les politiques relatives aux instantanés	16 décembre 2024

Modification	Description	Date
	à obtenir des informations sur les Zones Locales.	
AWSDataLifecycleManagerSSMFullAccès — Les autorisations de politique ont été mises à jour.	Mise à jour de la politique afin de prendre en charge les instantanés cohérents par rapport à l'application pour SAP HANA à l'aide du document SSM `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA` .	17 novembre 2023
AWSDataLifecycleManagerSSMFullAccès — Ajout d'une nouvelle politique AWS gérée.	Amazon Data Lifecycle Manager a ajouté la politique de AWS gestion des AWSData Lifecycle Manager SSMFull accès.	7 novembre 2023

Modification	Description	Date
AWSDataLifecycleManagerServiceRole— Des autorisations ont été ajoutées pour prendre en charge l'archivage des instantanés.	Amazon Data Lifecycle Manager a ajouté les actions `ec2:ModifySnapshotTier` et `ec2:DescribeSnapshotTierStatus` visant à accorder aux politiques d'instantanés l'autorisation d'archiver des instantanés et de vérifier l'état d'archivage des instantanés.	30 septembre 2022

Modification	Description	Date
AWSDataLifecycleManagerServiceRoleForAMIManagement— Des autorisations ont été ajoutées pour prendre en charge la dépréciation des AMI.	Amazon Data Lifecycle Manager a ajouté les actions `ec2:EnableImageDeprecation` et `ec2:DisableImageDeprecation` pour accorder aux politiques d'AMI EBS l'autorisation d'activer et de désactiver l'obsolescence d'AMI.	23 août 2021
Début du suivi des modifications par Amazon Data Lifecycle Manager	Amazon Data Lifecycle Manager a commencé à suivre les modifications apportées AWS à ses politiques gérées.	23 août 2021

Rôles de service IAM pour Amazon Data Lifecycle Manager

Un rôle AWS Identity and Access Management (IAM) est similaire à un utilisateur, dans la mesure où il s'agit d'une AWS identité dotée de politiques d'autorisation qui déterminent ce que l'identité peut

et ne peut pas faire. AWS En revanche, au lieu d'être associé de manière unique à une personne, un rôle est conçu pour être assumé par tout utilisateur qui en a besoin. Un rôle de service est un rôle qu'un AWS service assume pour effectuer des actions en votre nom. Amazon Data Lifecycle Manager étant le service qui effectue des opérations de sauvegarde en votre nom, vous devez lui transmettre un rôle à assumer lorsqu'il effectue des opérations de politique en votre nom. Pour plus d'informations sur les rôles IAM, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

Le rôle que vous transmettez à Amazon Data Lifecycle Manager doit disposer d'une politique IAM avec les autorisations permettant à Amazon Data Lifecycle Manager d'effectuer des actions associées aux opérations de politique, telles que la création de snapshots, la copie de snapshots AMIs, la suppression de snapshots et AMIs le désenregistrement. AMIs Chaque type de politique Amazon Data Lifecycle Manager nécessite des autorisations différentes. Amazon Data Lifecycle Manager doit également être répertorié comme entité approuvée par le rôle, ce qui permet à Amazon Data Lifecycle Manager d'assumer ce rôle.

Rubriques

- Fonctions du service par défaut pour Amazon Data Lifecycle Manager
- Fonctions du service personnalisées pour Amazon Data Lifecycle Manager

Fonctions du service par défaut pour Amazon Data Lifecycle Manager

Amazon Data Lifecycle Manager utilise les fonctions du service par défaut suivantes :

- AWSDataLifecycleManagerDefaultRole: rôle par défaut pour la gestion des instantanés. Il ne fait confiance qu'au service `dlm.amazonaws.com` pour assumer ce rôle et il permet à Amazon Data Lifecycle Manager d'effectuer en votre nom les actions requises par les politiques d'instantané et de copie d'instantané inter-comptes. Ce rôle utilise la politique `AWSDataLifecycleManagerServiceRole` AWS gérée.

> **Note**
>
> Le format ARN du rôle diffère selon qu'il a été créé à l'aide de la console ou de l' AWS CLI. Si le rôle a été créé à l'aide de la console, le format ARN est `arn:aws:iam::`*`account_id`*`:role/service-role/AWSDataLifecycleManagerDefaultRole`. Si le rôle a été créé à l'aide de AWS CLI, le format ARN est`arn:aws:iam::`*`account_id`*`:role/AWSDataLifecycleManagerDefaultRole`.

- AWSDataLifecycleManagerDefaultRoleForAMIManagement: rôle par défaut pour la gestion AMIs. Il ne fait confiance qu'au service `dlm.amazonaws.com` pour assumer ce rôle et il permet à Amazon Data Lifecycle Manager d'effectuer en votre nom les actions requises par les politiques d'AMI EBS. Ce rôle utilise la politique `AWSDataLifecycleManagerServiceRoleForAMIManagement` AWS gérée.

Si vous utilisez la console Amazon Data Lifecycle Manager, Amazon Data Lifecycle Manager crée automatiquement le rôle de AWSDataLifecycleManagerDefaultRoleservice la première fois que vous créez une politique de capture instantanée ou de copie instantanée entre comptes, et crée automatiquement le rôle de AWSDataLifecycleManagerDefaultRoleForAMIManagementservice la première fois que vous créez une politique AMI basée sur EBS.

Si vous n'utilisez pas la console, vous pouvez créer manuellement les rôles de service à l'aide de la create-default-rolecommande. Pour`--resource-type`, spécifiez `snapshot` créer AWSData LifecycleManagerDefaultRole ou `image` créer AWSData LifecycleManagerDefaultRoleForAMIManagement.

```
$ aws dlm create-default-role --resource-type snapshot|image
```

Si vous supprimez les fonctions du service par défaut et que par la suite vous avez besoin de les recréer, vous pourrez utiliser la même procédure pour recréer les rôles dans votre compte.

Fonctions du service personnalisées pour Amazon Data Lifecycle Manager

Vous pouvez également choisir de créer des rôles IAM personnalisés possédant les autorisations requises et les sélectionner lors de la création d'une politique de cycle de vie, comme alternative aux fonctions du service par défaut.

Pour créer un rôle IAM personnalisé

1. Créez des rôles avec les autorisations suivantes.

   - Autorisations requises pour la gestion des politiques de cycle de vie des instantanés

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

```
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-
cwe.*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
```

```
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringNotLike": {
                    "aws:ResourceTag/DLMScriptsAccess": "false"
                }
```

```
            }
        }
    ]
}
```

- Autorisations pour la gestion des politiques de cycle de vie des AMI

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

Pour plus d'informations, consultez Création d'un rôle dans le IAM Guide de l'utilisateur.

2. Ajoutez une relation d'approbation aux rôles.

   a. Dans la console IAM, choisissez Rôles.

   b. Sélectionnez les rôles que vous avez créés, puis sélectionnez Trust relationships (Relations d'approbation).

   c. Choisissez Modifier la relation d'approbation, ajoutez la stratégie suivante, puis choisissez Mettre à jour la stratégie d'approbation.

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

   Nous vous recommandons d'utiliser les clés de condition `aws:SourceAccount` et `aws:SourceArn` pour vous protéger contre le problème du député confus. Par exemple, vous pouvez ajouter le bloc de condition suivant à la stratégie d'approbation précédente. `aws:SourceAccount` est propriétaire de la politique de cycle de vie et `aws:SourceArn` est l'ARN de la politique de cycle de vie. Si vous ne connaissez pas l'ID de politique de cycle de vie, vous pouvez remplacer cette partie de l'ARN par un caractère générique (`*`), puis mettre à jour la politique d'approbation après avoir créé la politique de cycle de vie.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"
    }
}
```

Surveillez les politiques d'Amazon Data Lifecycle Manager

Vous pouvez utiliser les fonctionnalités suivantes pour surveiller le cycle de vie de vos instantanés et AMIs.

Fonctionnalités

- Console et AWS CLI
- AWS CloudTrail
- Surveillez les politiques de Data Lifecycle Manager à l'aide EventBridge
- Surveillez les politiques de Data Lifecycle Manager à l'aide CloudWatch

Console et AWS CLI

Vous pouvez consulter vos politiques de cycle de vie à l'aide de la EC2 console Amazon ou du AWS CLI. Chaque instantané et AMI créé par une politique possède un horodatage et des balises liées à la politique. Vous pouvez filtrer les instantanés et AMIs utiliser ces balises pour vérifier que vos sauvegardes sont créées comme vous le souhaitez.

AWS CloudTrail

Vous pouvez ainsi suivre l'activité des utilisateurs et l'utilisation des API pour démontrer la conformité aux politiques internes et aux normes réglementaires. AWS CloudTrail Pour plus d'informations, consultez le AWS CloudTrail Guide de l'utilisateur .

Surveillez les politiques de Data Lifecycle Manager à l'aide EventBridge

Amazon EBS et Amazon Data Lifecycle Manager émettent des événements liés aux actions de la politique de cycle de vie. Vous pouvez utiliser AWS Lambda Amazon CloudWatch Events pour gérer les notifications d'événements par programmation. Les événements sont générés dans la mesure du possible. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Les événements suivants sont disponibles :

> **Note**
>
> Aucun événement n'est émis pour les actions de politique de cycle de vie des AMI.

- `createSnapshot` : événement Amazon EBS émis en cas de réussite ou d'échec d'une action `CreateSnapshot`. Pour de plus amples informations, veuillez consulter EventBridge Événements Amazon pour Amazon EBS.
- `DLM Policy State Change` : événement Amazon Data Lifecycle Manager émis lorsqu'une politique de cycle de vie passe en mode erreur. L'événement contient une description de la cause de l'erreur.

  Vous trouverez ci-après un exemple d'événement émis lorsque les autorisations accordées par le rôle IAM sont insuffisantes.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail": {
        "state": "ERROR",
        "cause": "Role provided does not have sufficient permissions",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
```

```
    }
}
```

Voici un exemple d'événement émis lorsqu'une limite est dépassée.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail":{
        "state": "ERROR",
        "cause": "Maximum allowed active snapshot limit exceeded",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

- `DLM Pre Post Script Notification` : événement émis lorsqu'un pré-script ou un post-script est lancé, réussit ou échoue.

  Voici un exemple d'événement émis lorsqu'une sauvegarde VSS réussit.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "DLM Pre Post Script Notification",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2023-10-27T22:04:52Z",
    "region": "us-east-1",
    "resources": ["arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef"],
    "detail": {
        "script_stage": "",
        "result": "success",
        "cause": "",
```

```
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef",
        "execution_handler": "AWS_VSS_BACKUP",
        "source": "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef",
        "resource_type": "EBS_SNAPSHOT",
        "resources": [{
            "status": "pending",
            "resource_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
            "source": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-01234567890abcdef"
        }],
        "request_id": "a1b2c3d4-a1b2-a1b2-a1b2-a1b2c3d4e5f6",
        "start_time": "2023-10-27T22:03:29.370Z",
        "end_time": "2023-10-27T22:04:51.370Z",
        "timeout_time": ""
    }
}
```


Surveillez les politiques de Data Lifecycle Manager à l'aide CloudWatch

Vous pouvez surveiller les politiques de cycle de vie de votre Amazon Data Lifecycle Manager à l'aide CloudWatch d'un outil qui collecte les données brutes et les transforme en indicateurs lisibles quasiment en temps réel. Vous pouvez utiliser ces statistiques pour savoir exactement combien de snapshots Amazon EBS et sauvegardés par EBS AMIs sont créés, supprimés et copiés par vos politiques au fil du temps. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints.

Les métriques sont enregistrées pour une durée de 15 mois. Vous pouvez, par conséquent, accéder aux informations historiques et mieux comprendre la façon dont vos politiques de cycle de vie s'exécute sur une durée prolongée.

Pour plus d'informations sur Amazon CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Rubriques

- Métriques prises en charge
- Afficher CloudWatch les statistiques relatives à vos politiques
- Graphique de métriques de vos politiques
- Création d'une CloudWatch alarme pour une politique

- Exemples de cas d'utilisation
- Gestion des politiques qui signalent les actions ayant échoué

Métriques prises en charge

L'espace de nom `Data Lifecycle Manager` inclut les métriques suivantes pour les politiques de cycle de vie Amazon Data Lifecycle Manager. Les métriques prises en charge diffèrent selon le type de politique.

Toutes les métriques peuvent être mesurées dans la dimension `DLMPolicyId`. Les statistiques les plus utiles sont `sum` et `average`, et l'unité de mesure est `count`.

Sélectionnez un onglet pour afficher les métriques prises en charge par le type de politique correspondant.

EBS snapshot policies

Métrique	Description
`ResourcesTargeted`	Nombre de ressources ciblées par les étiquettes spécifiées dans un instantané ou une politique d'AMI basée sur EBS.
`SnapshotsCreateStarted`	Nombre d'actions de création d'instantanés lancées par une politique d'instantané. Chaque action n'est enregistrée qu'une seule fois, même s'il y a plusieurs tentatives ultérieures. Si une action de création d'instantanés échoue, Amazon Data Lifecycle Manager envoie une métrique `SnapshotsCreateFailed` .
`SnapshotsCreateCompleted`	Nombre d'instantanés créés par une politique d'instantané. Cela inclut les tentatives réussies dans les 60 minutes suivant l'heure prévue.
`SnapshotsCreateFailed`	Nombre d'instantanés qui n'ont pas pu être créés par une politique d'instantané. Cela inclut les tentatives infructueuses dans les 60 minutes suivant l'heure prévue.

Métrique	Description
`SnapshotsSharedCompleted`	Nombre d'instantanés partagés entre les comptes par une politique d'instantané.
`SnapshotsDeleteCompleted`	Nombre d'instantanés supprimés par une politique d'AMI basée sur un instantané ou une politique d'AMI basée sur EBS. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique. Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique AMI basée sur EBS annule l'enregistrement. AMIs
`SnapshotsDeleteFailed`	Nombre d'instantanés n'ayant pas pu être supprimés par une politique d'AMI basée sur un instantané ou une politique d'AMI basée sur EBS. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique. Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique AMI basée sur EBS annule l'enregistrement. AMIs
`SnapshotsCopiedRegionStarted`	Nombre d'actions de copie d'instantanés inter-régions lancées par une politique d'instantané.
`SnapshotsCopiedRegionCompleted`	Nombre de copies d'instantanés inter-régions créées par une politique d'instantané. Cela inclut les tentatives réussies dans les 24 heures suivant l'heure prévue.
`SnapshotsCopiedRegionFailed`	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être créées par une politique d'instantané. Cela inclut les tentatives infructueuses dans les 24 heures suivant l'heure prévue.

Métrique	Description
`SnapshotsCopiedRegionDeleteCompleted`	Nombre de copies d'instantanés inter-régions supprimées, conformément à la règle de rétention, par une politique d'instantané.
`SnapshotsCopiedRegionDeleteFailed`	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être supprimées, conformément à la règle de rétention, par une politique d'instantané.
`snapshotsArchiveDeletionFailed`	Nombre d'instantanés archivés qui n'ont pas pu être supprimés du niveau d'archivage par une politique d'instantané.
`snapshotsArchiveScheduled`	Nombre d'instantanés dont l'archivage a été prévu par une politique d'instantané.
`snapshotsArchiveCompleted`	Nombre d'instantanés qui ont été archivés correctement par une politique d'instantané.
`snapshotsArchiveFailed`	Nombre d'instantanés qui n'ont pas pu être archivés par une politique d'instantané.
`snapshotsArchiveDeletionCompleted`	Nombre d'instantanés archivés qui ont été supprimés correctement du niveau d'archivage par une politique d'instantané.
`PreScriptStarted`	Nombre d'instances pour lesquelles un pré-script a été lancé avec succès. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.

Métrique	Description
`PreScriptCompleted`	Nombre d'instances pour lesquelles un pré-script a été terminé avec succès. La métrique est émise même si le pré-script se termine après le délai d'expiration spécifié. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.
`PreScriptFailed`	Nombre d'instances pour lesquelles un pré-script n'a pas été terminé avec succès. La métrique est émise même si le pré-script se termine après le délai d'expiration spécifié. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.
`PostScriptStarted`	Nombre d'instances pour lesquelles un post-script a été lancé avec succès. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.
PostScriptCompleted	Nombre d'instances pour lesquelles un post-script a été terminé avec succès. La métrique est émise même si le post-script se termine après le délai d'expiration spécifié. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.
PostScriptFailed	Nombre d'instances pour lesquelles un post-script n'a pas été terminé avec succès. La métrique est émise même si le post-script se termine après le délai d'expiration spécifié. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.

Métrique	Description
`VSSBackup Started`	Nombre d'instances pour lesquelles une sauvegarde VSS a été lancée avec succès. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.
`VSSBackup Completed`	Nombre d'instances pour lesquelles une sauvegarde VSS a été terminée avec succès. La métrique est émise même si la sauvegarde VSS se termine après le délai d'expiration spécifié. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.
`VSSBackup Failed`	Nombre d'instances pour lesquelles une sauvegarde VSS n'a pas été terminée avec succès. La métrique est émise même si la sauvegarde VSS se termine après le délai d'expiration spécifié. Si les relances de scripts sont activées, cette métrique peut être émise plusieurs fois lors de chaque exécution de la politique.

EBS-backed AMI policies

Les métriques suivantes peuvent être utilisées avec les politiques d'AMI basées sur EBS :

Métrique	Description
`Resources Targeted`	Nombre de ressources ciblées par les étiquettes spécifiées dans un instantané ou une politique d'AMI basée sur EBS.
`Snapshots DeleteCompleted`	Nombre d'instantanés supprimés par une politique d'AMI basée sur un instantané ou une politique d'AMI basée sur EBS. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique.

Métrique	Description
	Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique AMI basée sur EBS annule l'enregistrement. AMIs
`SnapshotsDeleteFailed`	Nombre d'instantanés n'ayant pas pu être supprimés par une politique d'AMI basée sur un instantané ou une politique d'AMI basée sur EBS. Cette métrique s'applique uniquement aux instantanés créés par la politique. Elle ne s'applique pas aux copies d'instantanés inter-régions créées par la politique. Cette métrique inclut les instantanés qui sont supprimés lorsqu'une politique AMI basée sur EBS annule l'enregistrement. AMIs
`SnapshotsCopiedRegionDeleteCompleted`	Nombre de copies d'instantanés inter-régions supprimées, conformément à la règle de rétention, par une politique d'instantané.
`SnapshotsCopiedRegionDeleteFailed`	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être supprimées, conformément à la règle de rétention, par une politique d'instantané.
`ImagesCreateStarted`	Le nombre d'CreateImageactions initiées par une politique AMI soutenue par EBS.
`ImagesCreateCompleted`	Le nombre de AMIs créés par une politique AMI basée sur EBS.
`ImagesCreateFailed`	Le numéro n' AMIs a pas pu être créé par une politique AMI basée sur EBS.

Métrique	Description
`ImagesDeregisterCompleted`	Le nombre de personnes AMIs désenregistrées par une politique AMI soutenue par EBS.
`ImagesDeregisterFailed`	Le numéro de AMIs ce numéro n'a pas pu être désenregistré par une politique d'AMI soutenue par EBS.
`ImagesCopiedRegionStarted`	Nombre d'actions de copie inter-régions lancées par une politique d'AMI basée sur EBS.
`ImagesCopiedRegionCompleted`	Nombre de copies d'AMI inter-régions créées par une politique d'AMI basée sur EBS.
`ImagesCopiedRegionFailed`	Nombre de copies d'AMI inter-régions qui n'ont pas pu être créées par une politique d'AMI basée sur EBS.
`ImagesCopiedRegionDeregisterCompleted`	Nombre de copies d'AMI inter-régions annulées, conformément à la règle de rétention, par une politique d'AMI basée sur EBS.
`ImagesCopiedRegionDeregisteredFailed`	Nombre de copies d'AMI inter-régions qui n'ont pas pu être annulées, conformément à la règle de rétention, par une politique d'AMI basée sur EBS.

Métrique	Description
`EnableImageDeprecationCompleted`	Le nombre d'entre AMIs eux ont été marqués comme obsolètes par une politique d'AMI soutenue par EBS.
`EnableImageDeprecationFailed`	Le numéro n' AMIs a pas pu être marqué comme obsolète par une politique d'AMI soutenue par EBS.
`EnableCopiedImageDeprecationCompleted`	Nombre de copies d'AMI inter-Régions marquées pour obsolescence par une politique d'AMI EBS.
`EnableCopiedImageDeprecationFailed`	Nombre de copies d'AMI inter-Régions n'ayant pas pu être marquées pour obsolescence par une politique d'AMI EBS.

Cross-account copy event policies

Les métriques suivantes peuvent être utilisées avec les politiques d'événement de copie entre comptes :

Métrique	Description
`SnapshotsCopiedAccountStarted`	Nombre d'actions de copie d'instantané entre comptes initiées par une politique d'événement de copie entre comptes.

Métrique	Description
`SnapshotsCopiedAccountCompleted`	Nombre d'instantanés copiés à partir d'un autre compte par une politique d'événement de copie entre comptes. Cela inclut les tentatives réussies dans les 24 heures suivant l'heure prévue.
`SnapshotsCopiedAccountFailed`	Nombre d'instantanés qui n'ont pas pu être copiés à partir d'un autre compte par une politique d'événement de copie entre comptes. Cela inclut les tentatives infructueuses dans les 24 heures suivant l'heure prévue.
`SnapshotsCopiedAccountDeleteCompleted`	Nombre de copies d'instantanés inter-régions supprimées, conformément à la règle de rétention, par une politique d'événement de copie entre comptes.
`SnapshotsCopiedAccountDeleteFailed`	Nombre de copies d'instantanés inter-régions qui n'ont pas pu être supprimées, conformément à la règle de rétention, par une politique d'événement de copie entre comptes.

Afficher CloudWatch les statistiques relatives à vos politiques

Vous pouvez utiliser les outils de ligne de commande AWS Management Console ou les outils de ligne de commande pour répertorier les métriques qu'Amazon Data Lifecycle Manager envoie à Amazon CloudWatch.

Amazon EC2 console

Pour consulter les métriques à l'aide de la EC2 console Amazon

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sélectionnez Lifecycle Manager (Gestionnaire de cycle de vie).
3. Sélectionnez une politique dans la grille, puis sélectionnez l'onglet Monitoring(Surveillance).

CloudWatch console

Pour consulter les métriques à l'aide de la CloudWatch console Amazon

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de nom EBS, puis sélectionnez Data Lifecycle Manager metrics (Métriques Data Lifecycle Manager).

AWS CLI

Pour répertorier toutes les métriques disponibles pour Amazon Data Lifecycle Manager

Utilisez la commande list-metrics.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS
```

Pour répertorier toutes les métriques d'une politique spécifique

Utilisez la commande list-metrics et spécifiez la dimension `DLMPolicyId`.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

Pour répertorier une métrique unique dans toutes les politiques

Utilisez la commande list-metrics et spécifiez l'option `--metric-name`.

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --metric-name SnapshotsCreateCompleted
```

Graphique de métriques de vos politiques

Après avoir créé une politique, vous pouvez ouvrir la EC2 console Amazon et consulter les graphiques de surveillance de la politique dans l'onglet Surveillance. Chaque graphique est basé sur l'une des EC2 statistiques Amazon disponibles.

Les graphiques de métriques suivants sont disponibles :

- Ressources ciblées (basées sur `ResourcesTargeted`)
- Création d'instantané démarrée (basé sur `SnapshotsCreateStarted`)
- Création d'instantané terminée (basé sur `SnapshotsCreateCompleted`)
- Échec de la création d'instantané (basé sur `SnapshotsCreateFailed`)
- Partage d'instantané terminé (basé sur `SnapshotsSharedCompleted`)
- Suppression d'instantané terminée (basé sur `SnapshotsDeleteCompleted`)
- Échec de la suppression d'instantané (basé sur `SnapshotsDeleteFailed`)
- Copie d'instantané inter-Régions démarrée (basé sur `SnapshotsCopiedRegionStarted`)
- Copie d'instantané inter-Régions terminée (basé sur `SnapshotsCopiedRegionCompleted`)
- Échec de la copie d'instantané inter-Région (basé sur `SnapshotsCopiedRegionFailed`)
- Suppression de copie d'instantané inter-Région terminée (basé sur `SnapshotsCopiedRegionDeleteCompleted`)
- Échec de suppression de copie d'instantané inter-Région (basé sur `SnapshotsCopiedRegionDeleteFailed`)
- Copie d'instantané inter-comptes démarrée (basé sur `SnapshotsCopiedAccountStarted`)
- Copie d'instantané inter-comptes terminée (basé sur `SnapshotsCopiedAccountCompleted`)
- Échec de la copie d'instantané inter-comptes (basé sur `SnapshotsCopiedAccountFailed`)
- Suppressions de copie d'instantané inter-comptes terminées (basé sur `SnapshotsCopiedAccountDeleteCompleted`)
- Échecs de suppression de copie d'instantané inter-comptes (basé sur `SnapshotsCopiedAccountDeleteFailed`)
- Création de l'AMI démarrée (basé sur `ImagesCreateStarted`)
- Créations d'AMI terminées (basé sur `ImagesCreateCompleted`)
- Échec de la création de l'AMI (basé sur `ImagesCreateFailed`)
- Annulations d'enregistrement d'AMI terminées (basé sur `ImagesDeregisterCompleted`)
- Échecs d'annulation d'enregistrement d'AMI (basé sur `ImagesDeregisterFailed`)
- Copie de l'AMI inter-Région commencée (basé sur `ImagesCopiedRegionStarted`)
- Copie de l'AMI inter-Régions terminée (basé sur `ImagesCopiedRegionCompleted`)
- Échec de la copie de l'AMI inter-Régions (basé sur `ImagesCopiedRegionFailed`)

- Annulation de l’enregistrement de la copie inter-Régions de l’AMI terminée (basé sur `ImagesCopiedRegionDeregisterCompleted`)
- Échec de l’annulation de l’enregistrement de la copie inter-Régions AMI (basé sur `ImagesCopiedRegionDeregisteredFailed`)
- Obsolescence de l’option AMI terminée (basé sur `EnableImageDeprecationCompleted`)
- Échec d’activation de l’obsolescence de l’AMI (basé sur `EnableImageDeprecationFailed`)
- Copie de l’AMI inter-Régions pour activer l’obsolescence terminée (basé sur `EnableCopiedImageDeprecationCompleted`)
- Échec de l’activation de l’obsolescence de la copie inter-région AMI (basé sur `EnableCopiedImageDeprecationFailed`)

Création d'une CloudWatch alarme pour une politique

Vous pouvez créer une CloudWatch alarme qui surveille CloudWatch les indicateurs de vos politiques. CloudWatch vous enverra automatiquement une notification lorsque la métrique atteindra un seuil que vous spécifiez. Vous pouvez créer une CloudWatch alarme à l'aide de la CloudWatch console.

Pour plus d'informations sur la création d'alarmes à l'aide de la CloudWatch console, consultez la rubrique suivante du guide de CloudWatch l'utilisateur Amazon.

- Création d'une CloudWatch alarme basée sur un seuil statique
- Création d'une CloudWatch alarme basée sur la détection d'anomalies

Exemples de cas d’utilisation

Voici des exemples de cas d’utilisation :

Rubriques

- Exemple 1 : ResourcesTargeted métrique
- Exemple 2 : SnapshotDeleteFailed métrique
- Exemple 3 : SnapshotsCopiedRegionFailed métrique

Exemple 1 : ResourcesTargeted métrique

Vous pouvez utiliser la métrique `ResourcesTargeted` pour surveiller le nombre total de ressources ciblées par une politique spécifique chaque fois qu'elle est exécutée. Cela vous permet de déclencher une alarme lorsque le nombre de ressources ciblées est inférieur ou supérieur à un seuil attendu.

Par exemple, si vous attendez à ce que votre politique quotidienne crée des sauvegardes ne dépassant pas `50` volumes, vous pouvez créer une alarme qui envoie une notification par e-mail lorsque la `sum` pour `ResourcesTargeted` est supérieure à`50` sur une période de 1 heure. De cette façon, vous pouvez vous assurer qu'aucun instantané n'a été créé de manière inattendue à partir de volumes qui ont été mal étiquetés.

Vous pouvez utiliser la commande suivante pour créer cette alarme :

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name resource-targeted-monitor \
    --alarm-description "Alarm when policy targets more than 50 resources" \
    --metric-name ResourcesTargeted \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 50 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Exemple 2 : SnapshotDeleteFailed métrique

Vous pouvez utiliser la métrique `SnapshotDeleteFailed` pour surveiller les échecs de suppression des instantanés conformément à la règle de rétention des instantanés de la politique.

Par exemple, si vous avez créé une politique qui doit supprimer automatiquement les instantanés toutes les douze heures, vous pouvez créer une alarme qui avertit votre équipe d'ingénierie lorsque la `sum` pour `SnapshotDeletionFailed` est supérieure à `0` sur une période de 1 heure. Cela peut vous aider à comprendre les causes d'une rétention incorrecte des instantanés et à vous assurer que vos coûts de stockage ne sont pas augmentés par des instantanés inutiles.

Vous pouvez utiliser la commande suivante pour créer cette alarme :

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-deletion-failed-monitor \
    --alarm-description "Alarm when snapshot deletions fail" \
    --metric-name SnapshotsDeleteFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Exemple 3 : SnapshotsCopiedRegionFailed métrique

Utilisez la métrique `SnapshotsCopiedRegionFailed` pour identifier lorsque vos politiques ne parviennent pas à copier des instantanés vers d'autres régions.

Par exemple, si votre politique copie quotidiennement des instantanés entre régions, vous pouvez créer une alarme qui envoie un SMS à votre équipe d'ingénierie lorsque la `sum` pour `SnapshotCrossRegionCopyFailed` est supérieure à `0` sur une période de 1 heure. Cela peut être utile pour vérifier si les instantanés suivants de la lignée ont été copiés avec succès par la politique.

Vous pouvez utiliser la commande suivante pour créer cette alarme :

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-copy-region-failed-monitor \
    --alarm-description "Alarm when snapshot copy fails" \
    --metric-name SnapshotsCopiedRegionFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

Gestion des politiques qui signalent les actions ayant échoué

Pour plus d'informations sur la marche à suivre lorsque l'une de vos politiques indique une valeur inattendue différente de zéro pour une mesure d'action ayant échoué, consultez l'article Que dois-

je faire si Amazon Data Lifecycle Manager signale des actions ayant échoué dans les CloudWatch métriques ?

Résoudre les problèmes liés à Amazon Data Lifecycle Manager

La documentation suivante peut vous aider à résoudre les problèmes que vous pouvez rencontrer.

Rubriques

Erreur: `Role with name already exists`

Description

Vous recevez l'erreur `Role with name AWSDataLifecycleManagerDefaultRole already exists` ou `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` lorsque vous essayez de créer une politique à l'aide de la console.

Cause

Le format ARN du rôle par défaut diffère selon qu'il a été créé à l'aide de la console ou de l' AWS CLI. Bien qu' ARNs ils soient différents, les rôles utilisent le même nom de rôle, ce qui entraîne un conflit de dénomination des rôles entre la console et le AWS CLI.

Solution

Pour résoudre ce problème, procédez comme suit :

1. (Pour les politiques de capture d'écran activées pour les pré-scripts et les post-scripts uniquement) Attachez manuellement la politique AWS gérée AWSDataLifecycleManagerSSMFullAccess au rôle AWSDataLifecycleManagerDefaultRoleIAM. Pour plus d'informations, consultez Ajout des autorisations d'identité IAM.
2. Lorsque vous créez votre politique Amazon Data Lifecycle Manager, pour le rôle IAM, sélectionnez Choisir un autre rôle, puis sélectionnez soit AWSDataLifecycleManagerDefaultRole(pour une politique de capture instantanée), soit AWSDataLifecycleManagerDefaultRoleForAMIManagement(pour une politique AMI).
3. Continuez à créer la politique comme d'habitude.

Utiliser EBS direct APIs pour accéder au contenu d'un instantané EBS

Vous pouvez utiliser Amazon Elastic Block Store (Amazon EBS) APIs directement pour créer des instantanés EBS, écrire des données directement dans vos instantanés, lire des données sur vos instantanés et identifier les différences ou les modifications entre deux instantanés. Si vous êtes un fournisseur de logiciels indépendant (ISV) qui propose des services de sauvegarde pour Amazon EBS, EBS direct APIs permet de suivre les modifications incrémentielles apportées à vos volumes EBS de manière plus efficace et plus rentable par le biais de snapshots. Cela peut être fait sans avoir à créer de nouveaux volumes à partir d'instantanés, puis à utiliser des instances Amazon Elastic Compute Cloud (Amazon EC2) pour comparer les différences.

Vous pouvez créer des instantanés incrémentiels directement à partir de données locales dans des volumes EBS et dans le cloud afin de les utiliser pour une reprise après sinistre rapide. Avec la possibilité d'écrire et de lire des instantanés, vous pouvez écrire vos données locales dans un instantané EBS lors d'un sinistre. Ensuite, après la restauration, vous pouvez le restaurer vers AWS ou sur site à partir du snapshot. Vous n'avez plus besoin de créer et de gérer des mécanismes complexes pour copier des données depuis et vers Amazon EBS.

Ce guide de l'utilisateur fournit une vue d'ensemble des éléments qui constituent l'EBS direct APIs, ainsi que des exemples de leur utilisation efficace. Pour plus d'informations sur les actions, les types de données, les paramètres et les erreurs du APIs, consultez la APIs référence directe EBS. Pour plus d'informations sur les AWS régions, les points de terminaison et les quotas de service pris en charge pour EBS direct APIs, consultez la section Points de terminaison et quotas Amazon EBS dans le. Références générales AWS

Rubriques

- Garantir l'idempuissance des demandes d'API StartSnapshot
- Rétentatives d'erreur pour EBS Direct APIs
- Optimisez les performances pour EBS Direct APIs
- Points de terminaison de service pour EBS Direct APIs
- AWS Exemples de code SDK pour EBS direct APIs
- Création d'une connexion privée entre un VPC et EBS direct APIs
- Enregistrez les APIs appels directs EBS à l'aide de AWS CloudTrail
- Questions fréquemment posées sur EBS direct APIs

Tarification d'EBS Direct APIs

Tarification pour APIs

Le prix que vous payez pour utiliser l'EBS direct APIs dépend des demandes que vous faites. Pour plus d'informations, consultez la section Tarification d'Amazon EBS.

- ListChangedBlockset ListSnapshotBlocks APIs sont facturés par demande. Par exemple, si vous effectuez 100 000 demandes d' ListSnapshotBlocks API dans une région qui facture 0,0006$ par 1 000 demandes, vous serez facturé 0,06$ (0,0006$ par 1 000 demandes x 100).
- GetSnapshotBlockest facturé par bloc retourné. Par exemple, si vous effectuez 100 000 demandes d' GetSnapshotBlock API dans une région qui facture 0,003$ par 1 000 blocs renvoyés, vous serez facturé 0,30$ (0,003$ par 1 000 blocs renvoyés x 100).
- PutSnapshotBlockest facturé par bloc écrit. Par exemple, si vous effectuez 100 000 demandes d' PutSnapshotBlock API dans une région qui facture 0,006$ par 1 000 blocs écrits, vous serez facturé 0,60$ (0,006$ par 1 000 blocs écrits x 100).

Coûts de mise en réseau

Coûts de transfert des données

Les données transférées directement entre les EC2 instances EBS direct APIs et Amazon d'une même AWS région sont gratuites lorsque vous utilisez des points de terminaison non FIPS. Pour plus d'informations, consultez Points de terminaison du service AWS. Si d'autres AWS services sont en cours de transfert de données, les frais de traitement des données associés vous seront facturés.

Ces services incluent, sans toutefois s'y limiter, les PrivateLink points de terminaison, NAT Gateway et Transit Gateway.

Points de terminaison de l'interface d'un VPC

Si vous utilisez EBS directement APIs depuis des EC2 instances Amazon ou des AWS Lambda fonctions dans des sous-réseaux privés, vous pouvez utiliser des points de terminaison d'interface VPC, au lieu d'utiliser des passerelles NAT, afin de réduire les coûts de transfert de données réseau. Pour de plus amples informations, veuillez consulter Création d'une connexion privée entre un VPC et EBS direct APIs.

Concepts pour EBS direct APIs

Voici les concepts clés que vous devez comprendre avant de commencer à utiliser l'EBS direct APIs.

Instantanés

Les instantanés représentent le principal moyen de sauvegarde des données de vos volumes EBS. Avec EBS direct APIs, vous pouvez également sauvegarder les données de vos disques locaux sur des instantanés. Afin d'économiser les frais de stockage, les instantanés successifs sont incrémentiels ; ils contiennent uniquement les données du volume ayant changé depuis l'instantané précédent. Pour de plus amples informations, veuillez consulter Instantanés Amazon EBS.

> **Note**
>
> EBS direct APIs ne prend pas en charge les instantanés publics ni les instantanés locaux sur Outposts.

Blocs

Un bloc est un fragment de données au sein d'un instantané. Chaque instantané peut contenir des milliers de blocs. Tous les blocs d'un instantané sont de taille fixe.

Index de bloc

Un index de blocs est un index logique en unités de 512 blocs Kio. Pour identifier l'index de blocs, divisez le décalage logique des données dans le volume logique par la taille de bloc (décalage logique des données/524288). Le décalage logique des données doit être 512 aligné en Kio.

Jetons de bloc

Un jeton de bloc est le hachage d'identification d'un bloc dans un instantané. Il est utilisé pour localiser les données de bloc. Les jetons de blocage renvoyés par EBS direct APIs sont temporaires. Ils changent à l'heure d'expiration spécifiée pour eux, ou si vous en exécutez un autre ListSnapshotBlocks ou si vous ListChangedBlocks demandez le même instantané.

Total de contrôle

Une somme de contrôle est une référence de petite taille dérivée d'un bloc de données dans le but de détecter les erreurs introduites lors de sa transmission ou de son stockage. L'EBS Direct APIs utilise des checksums pour valider l'intégrité des données. Lorsque vous lisez des données à partir d'un instantané EBS, le service fournit des SHA256 sommes de contrôle codées en Base64 pour chaque bloc de données transmis, que vous pouvez utiliser pour la validation. Lorsque vous écrivez des données dans un instantané EBS, vous devez fournir une SHA256 somme de contrôle codée en Base64 pour chaque bloc de données transmis. Le service valide les données reçues à l'aide de la somme de contrôle fournie. Pour plus d'informations, consultez Utilisez les APIs sommes de contrôle directes d'EBS pour valider les données des instantanés plus loin dans ce guide.

Chiffrement

Le chiffrement protège vos données en les convertissant en code illisible qui ne peut être déchiffré que par les personnes ayant accès à la clé KMS utilisée pour les chiffrer. Vous pouvez utiliser l'EBS direct APIs pour lire et écrire des instantanés chiffrés, mais il existe certaines limites. Pour plus d'informations, consultez Résultats du chiffrement pour EBS Direct APIs plus loin dans ce guide.

Actions d'API

L'EBS direct APIs comprend six actions. Il y a trois actions de lecture et trois actions d'écriture. Les actions de lecture sont :

- ListSnapshotBlocks— renvoie les index des blocs et les jetons des blocs dans l'instantané spécifié
- ListChangedBlocks— renvoie les index de blocs et les jetons de blocs qui sont différents entre deux instantanés spécifiés du même volume et de la même lignée d'instantanés.
- GetSnapshotBlock— renvoie les données dans un bloc pour l'ID d'instantané, l'index de bloc et le jeton de bloc spécifiés.

Les actions d'écriture sont :

- StartSnapshot— démarre un instantané, soit sous la forme d'un instantané incrémentiel d'un instantané existant, soit sous la forme d'un nouvel instantané. Le snapshot démarré reste en attente jusqu'à ce qu'il soit terminé à l'aide de l' CompleteSnapshot action.
- PutSnapshotBlock— ajoute des données à un instantané démarré sous forme de blocs individuels. Vous devez spécifier une SHA256 somme de contrôle codée en Base64 pour le bloc de données transmis. Le service valide le total de contrôle après la fin de la transmission des données. La requête échoue lorsque le total de contrôle calculé par le service ne correspond pas à la valeur que vous avez spécifiée.
- CompleteSnapshot— termine un instantané démarré qui est en attente. L'instantané passe alors à l'état terminé.

Signature Version 4 : signature

Signature Version 4 est le processus permettant d'ajouter des informations d'authentification aux AWS demandes envoyées par HTTP. Pour des raisons de sécurité, la plupart des demandes AWS doivent être signées avec une clé d'accès, qui consiste en un identifiant de clé d'accès et une clé d'accès secrète. Ces deux clés sont généralement appelées informations d'identification de sécurité. Pour plus d'informations sur la façon d'obtenir les informations d'identification permettant d'accéder à votre compte, reportez-vous à Informations d'identification de sécurité AWS.

Si vous avez l'intention de créer manuellement des requêtes HTTP, vous devez apprendre à les signer. Lorsque vous utilisez le AWS Command Line Interface (AWS CLI) ou l'un des AWS SDKs pour faire des demandes AWS, ces outils signent automatiquement les demandes à votre place avec la clé d'accès que vous spécifiez lors de la configuration des outils. Lorsque vous utilisez ces derniers, vous n'avez pas besoin d'apprendre à signer vous-même les demandes.

Pour plus d'informations, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Contrôlez l'accès à EBS direct à APIs l'aide d'IAM

Un utilisateur doit disposer des politiques suivantes pour utiliser l'EBS direct APIs. Pour plus d'informations, consultez Modification des autorisations d'un utilisateur.

Pour plus d'informations sur les APIs ressources directes, les actions et les clés contextuelles de condition EBS à utiliser dans les politiques d'autorisation IAM, consultez la section Actions,

ressources et clés de condition pour Amazon Elastic Block Store dans le Service Authorization Reference.

> **Important**
>
> Soyez prudent lorsque vous affectez les stratégies suivantes aux utilisateurs . En attribuant ces politiques, vous pouvez donner accès à un utilisateur qui se voit refuser l'accès à la même ressource par le biais d'Amazon EC2 APIs, par exemple aux CreateVolume actions CopySnapshot or.

Autorisations de lire des instantanés

La politique suivante permet d'utiliser la lecture directe APIs EBS sur tous les instantanés d'une région spécifique AWS . Dans la politique, remplacez *<Region>* par la région de l'instantané.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
}
```

La politique suivante permet d'utiliser la lecture directe EBS sur APIs les instantanés dotés d'une balise clé-valeur spécifique. Dans la politique, remplacez *<Key>* par la valeur clé de la balise et *<Value>* par la valeur de la balise.

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

```
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

La politique suivante permet d'utiliser l'intégralité de la lecture directe APIs EBS sur tous les instantanés du compte uniquement dans un intervalle de temps spécifique. Cette politique autorise l'utilisation de l'EBS direct sur la APIs base de la clé de condition `aws:CurrentTime` globale. Dans la politique, veillez à remplacer la plage de dates et d'heures affichée par la plage de dates et d'heures de votre politique.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez Modification des autorisations d'un utilisateur dans le Guide de l'utilisateur IAM.

Autorisations d'écrire des instantanés

La politique suivante permet d'utiliser l'écriture directe APIs EBS sur tous les instantanés d'une région spécifique AWS . Dans la politique, remplacez *<Region>* par la région de l'instantané.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
}
```

La politique suivante permet d'utiliser l'écriture directe EBS sur APIs les instantanés dotés d'une balise clé-valeur spécifique. Dans la politique, remplacez *<Key>* par la valeur clé de la balise et *<Value>* par la valeur de la balise.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
```

```
            }
        }
    ]
}
```

La politique suivante autorise l'utilisation de tous les EBS Direct APIs . Elle n'autorise également l'action `StartSnapshot` que si un ID d'instantané parent est spécifié. Par conséquent, cette politique bloque la possibilité de démarrer de nouveaux instantanés sans utiliser un instantané parent.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
                }
            }
        }
    ]
}
```

La politique suivante autorise l'utilisation de tous les EBS Direct APIs . Il permet également de créer uniquement la clé de balise `user` pour un nouvel instantané. Cette politique garantit également que l'utilisateur dispose de l'accès approprié pour créer des balises. L'action `StartSnapshot` est la seule action qui peut spécifier des balises.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "user"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

La politique suivante permet d'utiliser l'intégralité de l'écriture directe APIs EBS sur tous les instantanés du compte uniquement dans un intervalle de temps spécifique. Cette politique autorise l'utilisation de l'EBS direct sur la APIs base de la clé de condition `aws:CurrentTime` globale. Dans la politique, veillez à remplacer la plage de dates et d'heures affichée par la plage de dates et d'heures de votre politique.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez Modification des autorisations d'un utilisateur dans le Guide de l'utilisateur IAM.

Autorisations d'utilisation AWS KMS keys

La politique suivante accorde les autorisations permettant de déchiffrer un instantané chiffré à l'aide d'une clé KMS spécifique. Elle permet également de chiffrer de nouveaux instantanés à l'aide de la clé KMS par défaut pour le chiffrement EBS. Dans la politique, remplacez *<Region>* par la région de la clé KMS, *<AccountId>* par l'ID du AWS compte associé à la clé KMS et *<KeyId>* par l'ID de la clé KMS.

> **Note**
>
> Par défaut, tous les principaux du compte ont accès à la clé KMS AWS gérée par défaut pour le chiffrement Amazon EBS, et ils peuvent l'utiliser pour les opérations de chiffrement et de déchiffrement EBS. Si vous utilisez une clé gérée par le client, vous devez créer une nouvelle politique de clé ou modifier la politique de clé existante pour la clé gérée par le client afin d'accorder au principal l'accès à la clé gérée par le client. Pour plus d'informations, consultez Politiques de clé dans AWS KMS dans le Guide du développeur AWS Key Management Service .

> **Tip**
>
> Pour suivre le principe du moindre privilège, n'autorisez pas l'accès complet à `kms:CreateGrant`. Utilisez plutôt la clé de `kms:GrantIsForAWSResource` condition pour autoriser l'utilisateur à créer des autorisations sur la clé KMS uniquement lorsque l'autorisation est créée en son nom par un AWS service, comme indiqué dans l'exemple suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
```

```
                "kms:ReEncrypt*",
                "kms:CreateGrant",
                "ec2:CreateTags",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

Pour plus d'informations, consultez Modification des autorisations d'un utilisateur dans le Guide de l'utilisateur IAM.

Lisez les instantanés d'Amazon EBS avec EBS direct APIs

Les étapes suivantes décrivent comment utiliser l'EBS direct APIs pour lire des instantanés :

1. Utilisez cette ListSnapshotBlocks action pour afficher tous les index de blocs et les jetons de bloc des blocs dans un instantané. Vous pouvez également utiliser cette ListChangedBlocks action pour afficher uniquement les index de blocs et les jetons de blocs différents entre deux instantanés du même volume et de la même lignée de clichés. Ces actions vous aident à identifier les jetons de bloc et les index de bloc des blocs pour lesquels vous pouvez obtenir des données.
2. Utilisez l' GetSnapshotBlock action et spécifiez l'index du bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données.

> **Note**
>
> Vous ne pouvez pas utiliser EBS direct APIs avec des instantanés archivés.

Les exemples suivants montrent comment lire des instantanés à l'aide de l'EBS direct. APIs

Rubriques

- Liste des blocs dans un instantané

- Liste des blocs qui sont différents entre deux instantanés
- Obtenir des données de bloc à partir d'un instantané

Liste des blocs dans un instantané

AWS CLI

L'list-snapshot-blocksexemple de commande suivant renvoie les index de blocs et les jetons de bloc des blocs qui se trouvent dans un instantanésnap-0987654321. Le paramètre `--starting-block-index` limite les résultats aux index de blocs supérieurs à `1000`, et le paramètre `--max-results` limite les résultats aux premiers blocs `100`.

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-
index 1000 --max-results 100
```

L'exemple de réponse suivant pour la commande précédente répertorie les index de bloc et les jetons de bloc dans l'instantané. Utilisez la commande `get-snapshot-block` et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```
{
      "Blocks": [
          {
              "BlockIndex": 1001,
              "BlockToken": "AAABAV3/
PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"
          },
          {
              "BlockIndex": 1002,
              "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
          },
          {
              "BlockIndex": 1007,
              "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07eOgTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
          },
          {
              "BlockIndex": 1012,
```

```
            "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
        },
        {
            "BlockIndex": 1030,
            "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
        },
        {
            "BlockIndex": 1031,
            "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBClkw6spzCxJVqDVaTskJ"
        },
        ...
    ],
    "ExpiryTime": 1576287332.806,
    "VolumeSize": 32212254720,
    "BlockSize": 524288
}
```

AWS API

L'ListSnapshotBlocksexemple de demande suivant renvoie les index de blocs et les jetons de bloc des blocs qui se trouvent dans un instantané`snap-0acEXAMPLEcf41648`. Le paramètre `startingBlockIndex` limite les résultats aux index de blocs supérieurs à `1000`, et le paramètre `maxResults` limite les résultats aux premiers blocs `100`.

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T231953Z
  Authorization: <Authentication parameter>
```

L'exemple de réponse suivant pour la demande précédente répertorie les index de bloc et les jetons de bloc dans l'instantané. Utilisez l' GetSnapshotBlock action et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
```

```
  Content-Type: application/json
  Content-Length: 2472
  Date: Wed, 17 Jun 2020 23:19:56 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "Blocks": [
          {
              "BlockIndex": 0,
              "BlockToken": "AAUBAcuWqOCnDNuKle11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
          },
          {
              "BlockIndex": 1536,
              "BlockToken":
 "AAUBAWudwfmofcrQhGVlLwuRKm2b8ZXPiyrgoykTRC6IU1NbxKWDY1pPjvnV"
          },
          {
              "BlockIndex": 3072,
              "BlockToken":
 "AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
          },
          {
              "BlockIndex": 3073,
              "BlockToken":
 "AAUBAbqt9zpqBUEvtO2HINAfFaWToOwlPjbIsQOlx6JUN/0+iMQl0NtNbnX4"
          },
          ...
      ],
      "ExpiryTime": 1.59298379649E9,
      "VolumeSize": 3
  }
```

Liste des blocs qui sont différents entre deux instantanés

Tenez compte des points suivants lorsque vous effectuez des demandes paginées pour répertorier les blocs modifiés entre deux instantanés :

- La réponse peut inclure un ou plusieurs tableaux `ChangedBlocks` vides. Par exemple :
  - Instantané 1 – instantané complet avec 1 000 blocs avec des index de blocs `0` – 999.

- Instantané 2 – instantané incrémentiel avec un seul bloc modifié avec l'index de bloc 999.

La liste des blocs modifiés pour ces instantanés avec `StartingBlockIndex = 0` et `MaxResults = 100` renvoie un tableau vide de `ChangedBlocks`. Vous devez demander les autres résultats en utilisant `nextToken` jusqu'à ce que le bloc modifié soit retourné dans le dixième jeu de résultats, qui comprend les blocs avec les index de bloc `900` – 999.

- La réponse peut ignorer les blocs non écrits dans les instantanés. Par exemple :
  - Instantané 1 – instantané complet avec 1 000 blocs avec des index de blocs `2000` – 2999.
  - Instantané 2 – instantané incrémentiel avec un seul bloc modifié avec l'index de bloc `2000`.

  En listant les blocs modifiés pour ces instantanés avec `StartingBlockIndex = 0` et `MaxResults = 100`, la réponse ignore les index de bloc `0` – 1999 et inclut l'index de bloc `2000`. La réponse n'inclura pas les tableaux `ChangedBlocks` vides.

AWS CLI

L'list-changed-blocksexemple de commande suivant renvoie les index de blocs et les jetons de bloc des blocs qui sont différents entre les instantanés `snap-1234567890` et. `snap-0987654321` Le paramètre `--starting-block-index` limite les résultats aux index de blocs supérieurs à `0`, et le paramètre `--max-results` limite les résultats aux premiers blocs `500`.

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-
id snap-0987654321 --starting-block-index 0 --max-results 500
```

L'exemple de réponse suivant pour la commande précédente montre que les index de bloc 0, 6000, 6001, 6002 et 6003 sont différents entre les deux instantanés. De plus, les index de bloc 6001, 6002 et 6003 existent uniquement dans le premier ID d'instantané spécifié, et pas dans le second ID d'instantané car la réponse ne répertorie aucun second jeton de bloc.

Utilisez la commande `get-snapshot-block` et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```
{
      "ChangedBlocks": [
          {
```

```
            "BlockIndex": 0,
            "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/
KN3uygGlS0QOYWesbzBbDnX2dGpmC",
            "SecondBlockToken":
 "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGSr"
        },
        {
            "BlockIndex": 6000,
            "FirstBlockToken": "AAABAbYSiZvJ0/
R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
            "SecondBlockToken":
 "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"
        },
        {
            "BlockIndex": 6001,
            "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/
T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
        },
        {
            "BlockIndex": 6002,
            "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1576308931.973,
    "VolumeSize": 32212254720,
    "BlockSize": 524288,
    "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//
O6Mdi/BbJarBnp8h"
  }
```

AWS API

L'ListChangedBlocksexemple de demande suivant renvoie les index de blocs et les jetons de bloc des blocs qui sont différents entre les instantanés `snap-0acEXAMPLEcf41648` et. `snap-0c9EXAMPLE1b30e2f` Le paramètre `startingBlockIndex` limite les résultats aux index de blocs supérieurs à `0`, et le paramètre `maxResults` limite les résultats aux premiers blocs `500`.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232546Z
  Authorization: <Authentication parameter>
```

L'exemple de réponse suivant pour la requête précédente montre que les index de bloc `0`, `3072`, `6002` et `6003` sont différents entre les deux instantanés. De plus, les index de bloc `6002` et `6003` existent uniquement dans le premier ID d'instantané spécifié, et pas dans le second ID d'instantané car la réponse ne répertorie aucun second jeton de bloc.

Utilisez l'action `GetSnapshotBlock` et spécifiez l'index de bloc et le jeton de bloc du bloc pour lequel vous souhaitez obtenir des données. Les jetons de bloc sont valides jusqu'au délai d'expiration indiqué.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
  Content-Type: application/json
  Content-Length: 1456
  Date: Wed, 17 Jun 2020 23:25:47 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAUBAVaWqOCnDNuKle11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+OJkL",
              "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3NOresCxn5RO+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
          },
          {
              "BlockIndex": 3072,
              "FirstBlockToken":
 "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZOLEmeXLmHBf2R/Yb24MaS",
              "SecondBlockToken":
 "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid"
          },
          {
```

```
            "BlockIndex": 6002,
            "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1.592976647009E9,
    "VolumeSize": 3
 }
```

Obtenir des données de bloc à partir d'un instantané

AWS CLI

L'get-snapshot-blockexemple de commande suivant renvoie les données de l'index du bloc `6001` avec le jeton de blocAAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR, sous forme d'instantané`snap-1234567890`. Les données binaires seront générées dans le fichier `data` dans le répertoire `C:\Temp` sur un ordinateur Windows. Si vous exécutez la commande sur un ordinateur Linux ou Unix, remplacez le chemin de sortie par `/tmp/data` pour générer les données dans le fichier `data` du répertoire `/tmp`.

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-
token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

L'exemple de réponse suivant pour la commande précédente montre la taille des données renvoyées, la somme de contrôle pour valider les données et l'algorithme de la somme de contrôle. Les données binaires sont automatiquement enregistrées dans le répertoire et le fichier que vous avez spécifiés dans la commande de demande.

```
{
      "DataLength": "524288",
      "Checksum": "cf0Y6/Fn0oFa4VyjQPOa/iD0zhTflPTKzxGv2OKowXc=",
      "ChecksumAlgorithm": "SHA256"
```

```
  }
```

AWS API

L'GetSnapshotBlockexemple de demande suivant renvoie les données de l'index du bloc `3072` avec le jeton de blocAAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid, sous forme d'instantané`snap-0c9EXAMPLE1b30e2f`.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232838Z
  Authorization: <Authentication parameter>
```

L'exemple de réponse suivant pour la demande précédente montre la taille des données renvoyées, la somme de contrôle pour valider les données et l'algorithme utilisé pour générer la somme de contrôle. Les données binaires sont transmises dans le corps de la réponse et sont représentées comme *`BlockData`* dans l'exemple suivant.

```
HTTP/1.1 200 OK
  x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
  x-amz-Data-Length: 524288
  x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
  x-amz-Checksum-Algorithm: SHA256
  Content-Type: application/octet-stream
  Content-Length: 524288
  Date: Wed, 17 Jun 2020 23:28:38 GMT
  Connection: keep-alive

  BlockData
```

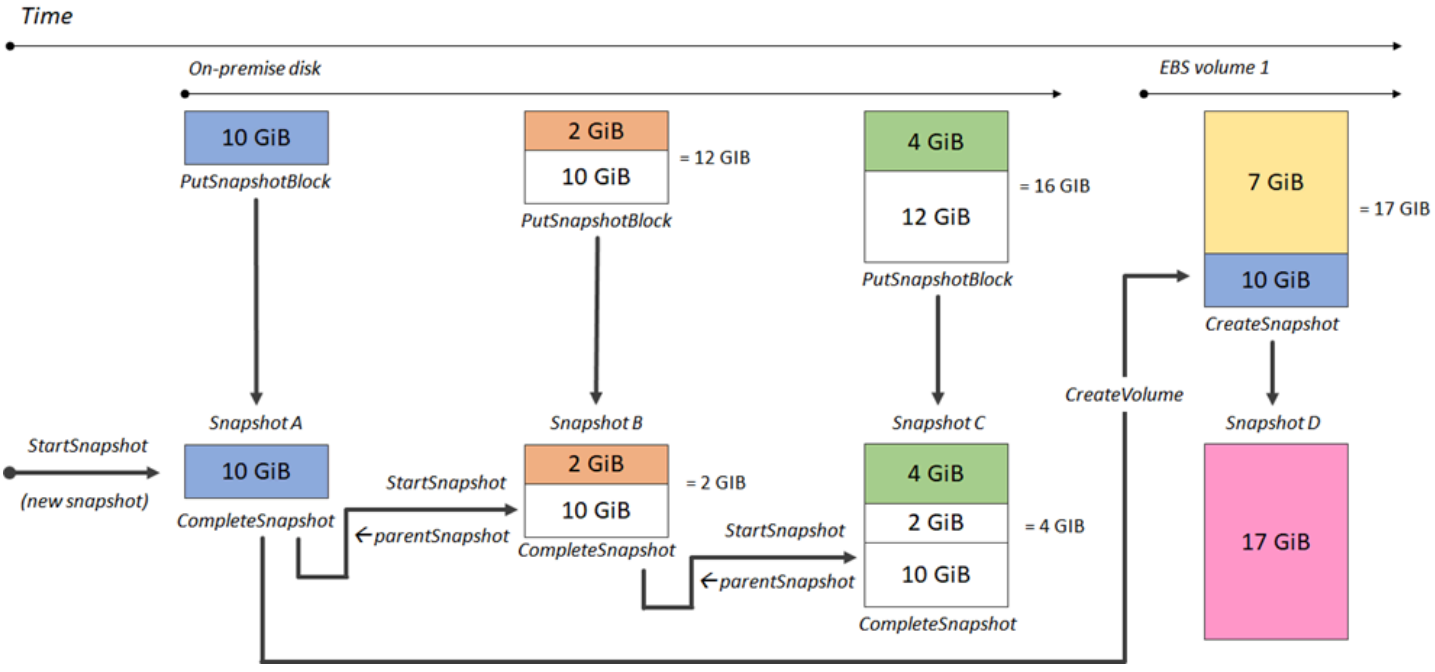
Rédigez des instantanés Amazon EBS avec EBS direct APIs

Les étapes suivantes décrivent comment utiliser l'EBS direct pour écrire des APIs instantanés incrémentiels :

1. Utilisez cette StartSnapshot action et spécifiez un ID de cliché parent pour démarrer un instantané en tant que capture incrémentielle d'un instantané existant, ou omettez l'ID de cliché parent pour démarrer un nouveau cliché. Cette action renvoie le nouvel ID d'instantané, qui est en attente.
2. Utilisez l' PutSnapshotBlock action et spécifiez l'ID de l'instantané en attente pour y ajouter des données sous forme de blocs individuels. Vous devez spécifier une SHA256 somme de contrôle codée en Base64 pour le bloc de données transmis. Le service calcule la somme de contrôle des données reçues et la valide avec la somme de contrôle que vous avez spécifiée. L'action échoue si les sommes de contrôle ne correspondent pas.
3. Lorsque vous avez terminé d'ajouter des données à l'instantané en attente, utilisez cette CompleteSnapshot action pour démarrer un flux de travail asynchrone qui scelle l'instantané et le fait passer à l'état terminé.

Répétez ces étapes pour créer un nouvel instantané incrémentiel à l'aide de l'instantané précédemment créé en tant que parent.

Par exemple, dans le diagramme suivant, l'instantané A est le premier nouvel instantané démarré. L'instantané A est utilisé comme instantané parent pour démarrer l'instantané B. L'instantané B est utilisé comme instantané parent pour démarrer et créer l'instantané C. Les instantanés A, B et C sont des instantanés incrémentiels. L'instantané A est utilisé pour créer le volume EBS 1. L'instantané D est créé à partir du volume EBS 1. L'instantané D est un instantané incrémentiel de A ; et non un instantané incrémentiel de B ou C.



Les exemples suivants montrent comment écrire des instantanés à l'aide de l'EBS direct. APIs

Rubriques

Démarrer un instantané

AWS CLI

L'exemple de commande start-snapshot suivant démarre un instantané 8 Gio en utilisant l'instantané `snap-123EXAMPLE1234567` comme instantané parent. Le nouvel instantané sera un instantané incrémentiel de l'instantané parent. L'instantané passe à un état d'erreur s'il n'y a pas de demande d'ajout ou d'exécution pour l'instantané pendant la période de `60` minutes spécifiée. Le jeton client `550e8400-e29b-41d4-a716-446655440000` garantit l'idempotence pour la demande. Si le jeton client est omis, le AWS SDK en génère un automatiquement pour vous. Pour plus d'informations sur l'idempotence, consultez Garantir l'idempuissance des demandes d'API StartSnapshot .

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

L'exemple de réponse suivant pour la commande précédente indique l'ID du snapshot, l'ID du compte AWS , l'état, la taille du volume en Gio et la taille des blocs dans l'instantané. L'instantané est démarré dans un état `pending`. Spécifiez l'ID d'instantané dans les commandes `put-snapshot-block` suivantes pour écrire des données dans l'instantané, puis utilisez la commande `complete-snapshot` pour terminer l'instantané et modifier son état sur `completed`.

```
{
    "SnapshotId": "snap-0aaEXAMPLEe306d62",
    "OwnerId": "111122223333",
    "Status": "pending",
    "VolumeSize": 8,
    "BlockSize": 524288
}
```

AWS API

L'StartSnapshotexemple de demande suivant démarre un instantané 8 GiB, en utilisant l'instantané `snap-123EXAMPLE1234567` comme instantané parent. Le nouvel instantané sera un instantané incrémentiel de l'instantané parent. L'instantané passe à un état d'erreur s'il n'y a pas de demande d'ajout ou d'exécution pour l'instantané pendant la période de `60` minutes spécifiée. Le jeton client `550e8400-e29b-41d4-a716-446655440000` garantit l'idempotence pour la demande. Si le jeton client est omis, le AWS SDK en génère un automatiquement pour vous. Pour plus d'informations sur l'idempotence, consultez Garantir l'idempuissance des demandes d'API StartSnapshot .

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

L'exemple de réponse suivant pour la demande précédente indique l'ID d'instantané, l'ID de compte AWS , l'état, la taille du volume en Gio et la taille des blocs dans l'instantané. L'instantané est démarré dans un état en attente. Spécifiez l'ID d'instantané dans une demande `PutSnapshotBlocks` ultérieure d'écriture de données dans l'instantané .

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Description": null,
    "OwnerId": "138695307491",
```

```
    "Progress": null,
    "SnapshotId": "snap-052EXAMPLEc85d8dd",
    "StartTime": null,
    "Status": "pending",
    "Tags": null,
    "VolumeSize": 8
}
```

Ajouter des données dans un instantané

AWS CLI

L'put-snapshot-blockexemple de commande suivant écrit des 524288 octets de données pour bloquer l'index 1000 sur un instantanésnap-0aaEXAMPLEe306d62. La somme de contrôle QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= codée en Base64 a été générée à l'aide de l'algorithme SHA256. Les données transmises se trouvent dans le fichier /tmp/data.

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
 --block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= --checksum-algorithm SHA256
```

L'exemple de réponse suivant pour la commande précédente confirme la longueur des données, la somme de contrôle et l'algorithme de somme de contrôle pour les données reçues par le service.

```
{
    "DataLength": "524288",
    "Checksum": "QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=",
    "ChecksumAlgorithm": "SHA256"
}
```

AWS API

L'PutSnapshotexemple de demande suivant écrit des 524288 octets de données pour bloquer l'index 1000 sur un instantanésnap-052EXAMPLEc85d8dd. La somme de contrôle QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= codée en Base64 a été générée à l'aide de l'algorithme SHA256. Les données sont transmises dans le corps de la demande et sont représentées comme *BlockData* dans l'exemple suivant.

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
```

```
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>

          BlockData
```

Voici un exemple de réponse pour la demande précédente, qui confirme la longueur des données, la somme de contrôle et l'algorithme de somme de contrôle pour les données que le service reçoit.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

{}
```

Terminer un instantané

AWS CLI

L'exemple de commande complete-snapshot suivant termine l'instantané `snap-0aaEXAMPLEe306d62`. La commande spécifie que les blocs 5 ont été écrits dans l'instantané. La somme de contrôle `6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=` représente la somme de contrôle de l'ensemble complet des données écrites dans un instantané. Pour plus d'informations sur les sommes de contrôle, consultez Utilisez les APIs sommes de contrôle directes d'EBS pour valider les données des instantanés plus haut dans ce guide.

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-
count 5 --checksum 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= --checksum-
algorithm SHA256 --checksum-aggregation-method LINEAR
```

Voici un exemple de réponse pour la commande précédente.

```
{
    "Status": "pending"
}
```

AWS API

L'CompleteSnapshotexemple de demande suivant permet de terminer le snapshotsnap-052EXAMPLEc85d8dd. La commande spécifie que les blocs 5 ont été écrits dans l'instantané. La somme de contrôle 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= représente la somme de contrôle de l'ensemble complet des données écrites dans un instantané.

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

Voici un exemple de réponse pour la demande précédente.

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

Résultats du chiffrement pour EBS Direct APIs

Lorsque vous démarrez un nouvel instantané en utilisant StartSnapshot, l'état du chiffrement dépend des valeurs que vous spécifiez pour Chiffré KmsKeyArn, et ParentSnapshotId, et du fait que votre AWS compte est activé pour le chiffrement par défaut.

> **Note**
>
> - Vous aurez peut-être besoin d'autorisations IAM supplémentaires pour utiliser l'EBS direct APIs avec le chiffrement. Pour plus d'informations, consultez Autorisations d'utilisation AWS KMS keys.
> - Si le chiffrement Amazon EBS est activé par défaut sur votre AWS compte, vous ne pouvez pas créer de snapshots non chiffrés.
> - Si le chiffrement Amazon EBS est activé par défaut sur votre AWS compte, vous ne pouvez pas créer un nouvel instantané à l'aide d'un instantané parent non chiffré. Vous devez d'abord chiffrer l'instantané parent en le copiant. Pour plus d'informations, consultez Copier un instantané Amazon EBS.

Rubriques

Résultats du chiffrement : instantané parent non chiffré

Le tableau suivant décrit le résultat du chiffrement pour chaque combinaison possible de paramètres lors de la spécification d'un instantané parent non chiffré.

ParentSnapshotId	Chiffré	KmsKeyArn	Chiffrement par défaut	Résultat
Non chiffré	Omis	Omis	Activées	Échec de la demande avec `ValidationException` .

ParentSnapshotId	Chiffré	KmsKeyArn	Chiffrement par défaut	Résultat
			Désactivées	L'instantané n'est pas chiffré.
		Spécifié	Activé	
			Désactivées	
Non chiffré	True	Omis	Activées	Échec de la demande avec `ValidationException` .
			Désactivées	
		Spécifié	Activé	
			Désactivées	
Non chiffré	False	Omis	Activées	Échec de la demande avec `ValidationException` .
			Désactivées	
		Spécifié	Activé	
			Désactivées	

Résultats du chiffrement : instantané parent chiffré

Le tableau suivant décrit le résultat du chiffrement pour chaque combinaison possible de paramètres lors de la spécification d'un instantané parent chiffré.

ParentSnapshotId	Chiffré	KmsKeyArn	Chiffrement par défaut	Résultat
Chiffré	Omis	Omis	Activées	L'instantané est chiffré à l'aide de la même clé KMS que l'instantané parent.
			Désactivées	
		Spécifié	Activé	Échec de la demande avec `ValidationException` .

ParentSnapshotId	Chiffré	KmsKeyArn	Chiffrement par défaut	Résultat
			Désactivées	
Chiffré	True	Omis	Activées	Échec de la demande avec `ValidationException` .
			Désactivées	
		Spécifié	Activé	
			Désactivées	
Chiffré	False	Omis	Activées	Échec de la demande avec `ValidationException` .
			Désactivées	
		Spécifié	Activé	
			Désactivées	

Résultats du chiffrement : aucun instantané parent

Les tableaux suivants décrivent le résultat du chiffrement pour chaque combinaison possible de paramètres en l'absence d'utilisation d'un instantané parent.

ParentSnapshotId	Chiffré	KmsKeyArn	Chiffrement par défaut	Résultat
Omis	True	Omis	Activées	L'instantané est chiffré à l'aide de la clé KMS par défaut de votre compte. *
			Désactivées	
		Spécifié	Activé	Le snapshot est chiffré à l'aide de la clé KMS spécifiée pour KmsKeyArn.
			Désactivées	
Omis	False	Omis	Activées	Échec de la demande avec `ValidationException` .

ParentSnapshotId	Chiffré	KmsKeyArn	Chiffrement par défaut	Résultat
			Désactivées	L'instantané n'est pas chiffré.
		Spécifié	Activé	Échec de la demande avec `ValidationException` .
			Désactivées	
Omis	Omis	Omis	Activées	L'instantané est chiffré à l'aide de la clé KMS par défaut de votre compte. *
			Désactivées	L'instantané n'est pas chiffré.
		Spécifié	Activé	Le snapshot est chiffré à l'aide de la clé KMS spécifiée pour KmsKeyArn.
			Désactivées	

* Cette clé KMS par défaut peut être une clé gérée par le client ou la clé KMS AWS gérée par défaut pour le chiffrement Amazon EBS.

Utilisez les APIs sommes de contrôle directes d'EBS pour valider les données des instantanés

L' GetSnapshotBlock action renvoie des données qui se trouvent dans un bloc d'un instantané, et l' PutSnapshotBlock action ajoute des données à un bloc d'un instantané. Les données de bloc transmises ne sont pas signées dans le cadre du processus de signature de la version 4. Par conséquent, les sommes de contrôle sont utilisées pour valider l'intégrité des données comme suit :

- Lorsque vous utilisez l' GetSnapshotBlock action, la réponse fournit une somme de SHA256 contrôle codée en Base64 pour les données du bloc à l'aide de l'en-tête X-AMZ-Checksum, et l'algorithme de somme de contrôle utilisant l'en-tête X-AMZ-Checksum-Algorithm. Utilisez la somme de contrôle renvoyée pour valider l'intégrité des données. Si la somme de contrôle que vous générez ne correspond pas à celle fournie par Amazon EBS, vous devez considérer les données non valides et réessayer votre demande.

- Lorsque vous utilisez l' PutSnapshotBlock action, votre demande doit fournir une somme de SHA256 contrôle codée en Base64 pour les données du bloc à l'aide de l'en-tête X-AMZ-Checksum, et l'algorithme de somme de contrôle utilisant l'en-tête X-AMZ-Checksum-Algorithm. La somme de contrôle que vous fournissez est validée par rapport à une somme de contrôle générée par Amazon EBS pour valider l'intégrité des données. Si les sommes de contrôle ne correspondent pas, la demande échoue.
- Lorsque vous utilisez l' CompleteSnapshot action, votre demande peut éventuellement fournir une SHA256 somme de contrôle agrégée codée en Base64 pour l'ensemble complet des données ajoutées à l'instantané. Fournissez la somme de contrôle à l'aide de l'en-tête x-amz-Checksum, l'algorithme de somme de contrôle à l'aide de l'en-tête x-amz-Checksum-Algorithm et la méthode d'agrégation de somme de contrôle à l'aide de l'en-tête x-amz-Checksum-Aggregation-Method. Pour générer la somme de contrôle agrégée à l'aide de la méthode d'agrégation linéaire, organisez les sommes de contrôle pour chaque bloc écrit dans l'ordre croissant de son index de bloc, concaténez-les pour former une chaîne unique, puis générez la somme de contrôle sur la chaîne entière à l'aide de l'algorithme. SHA256

Les sommes de contrôle de ces actions font partie du processus de signature de la version 4.

Garantir l'idempuissance des demandes d'API StartSnapshot

L'idempotence garantit qu'une requête API n'est exécutée qu'une seule fois. Avec une demande idempotente, si la demande d'origine se termine avec succès, les tentatives suivantes renvoient le résultat de la demande d'origine réussie et elles n'ont aucun effet supplémentaire.

L' StartSnapshotAPI prend en charge l'idempotencie à l'aide d'un jeton client. Un jeton client est une chaîne unique que vous spécifiez lorsque vous effectuez une demande d'API. Si vous réessayez une demande d'API avec le même jeton client et les mêmes paramètres de requête une fois qu'elle est terminée correctement, le résultat de la demande d'origine est renvoyé. Si vous réessayez une demande avec le même jeton client, mais que vous modifiez un ou plusieurs paramètres de requête, l'erreur `ConflictException` est renvoyée.

Si vous ne spécifiez pas votre propre jeton client, un jeton client est AWS SDKs automatiquement généré pour la demande afin de s'assurer qu'elle est idempotente.

Un jeton client peut être n'importe quelle chaîne qui comprend jusqu'à 64 caractères ASCII. Vous ne devez pas réutiliser les mêmes jetons client pour différentes demandes.

Pour effectuer une StartSnapshot demande idempotente avec votre propre jeton client à l'aide de l'API

Spécifiez le paramètre de demande `ClientToken`.

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

Pour effectuer une StartSnapshot demande idempotente avec votre propre jeton client à l'aide du AWS CLI

Spécifiez le paramètre de demande `client-token`.

```
$ C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-
snapshot snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-
a716-446655440000
```

Rétentatives d'erreur pour EBS Direct APIs

Ils AWS SDKsimplémentent une logique de nouvelle tentative automatique pour les demandes renvoyant des réponses d'erreur. Vous pouvez configurer les paramètres de nouvelle tentative pour le AWS SDKs. Pour plus d'informations, consultez la documentation de votre kit SDK.

Vous pouvez configurer AWS CLI pour réessayer automatiquement certaines demandes qui ont échoué. Pour plus d'informations sur la configuration des tentatives pour le AWS CLI, consultez la section AWS CLI Rétentatives dans le Guide de l'AWS Command Line Interface utilisateur.

L'AWS API de requête ne prend pas en charge la logique de nouvelle tentative pour les demandes ayant échoué. Si vous utilisez des requêtes HTTP ou HTTPS, vous devez implémenter une logique de nouvelle tentative dans votre application cliente.

Le tableau suivant présente les réponses possibles aux erreurs de l'API. Certaines erreurs de l'API peuvent faire l'objet d'une nouvelle tentative. Votre application client doit toujours relancer les demandes qui ont échoué et qui reçoivent une erreur récupérable.

Erreur	Code de réponse	Description	Lancé par	Récupérable ?
`InternalServerException`	500	La demande a échoué en raison d'un problème réseau ou AWS côté serveur.	Tout APIs	Oui
`ThrottlingException`	400	Le nombre de demandes d'API a dépassé la limite maximale de limitation des demandes d'API autorisée pour le compte.	Tout APIs	Oui
`RequestThrottleException`	400	Le nombre de demandes d'API a dépassé la limite maximale de limitation des demandes d'API autorisée pour l'instantané.	GetSnapshotBlock | PutSnapshotBlock	Oui
`ValidationException` avec le message « `Failed to read block data` »	400	Le bloc de données fourni n'était pas lisible.	PutSnapshotBlock	Oui

Erreur	Code de réponse	Description	Lancé par	Récupérable ?
`ValidationException` avec tout autre message	400	La syntaxe de la demande est mal formée, ou l'entrée ne satisfait pas aux contraintes spécifiées par Service AWS.	Tout APIs	Non
`ResourceNotFoundException`	404	L'ID de l'instantané spécifié n'existe pas.	Tout APIs	Non
`ConflictException`	409	Le jeton client spécifié a déjà été utilisé dans une demande similaire dont les paramètres étaient différents. Pour de plus amples informations, veuillez consulter Garantir l'idempuissance des demandes d'API StartSnapshot .	StartSnapshot	Non
`AccessDeniedException`	403	Vous n'avez pas l'autorisation d'effectuer l'opération demandée.	Tout APIs	Non

Erreur	Code de réponse	Description	Lancé par	Récupérable ?
`ServiceQuotaExceededException`	402	La demande a échoué, car son exécution dépasserait un ou plusieurs quotas de services dépendants pour votre compte.	Tout APIs	Non
`InvalidSignatureException`	403	La signature d'autorisation de la demande a expiré. Vous ne pouvez réessayer la demande qu'après avoir actualisé la signature d'autorisation.	Tout APIs	Non

Optimisez les performances pour EBS Direct APIs

Vous pouvez exécuter des demandes d'API simultanément. En supposant que la PutSnapshotBlock latence est de 100 ms, un thread peut traiter 10 requêtes en une seconde. En outre, en supposant que votre application cliente crée plusieurs threads et connexions (par exemple, 100 connexions), elle peut faire 1000 (10 * 100) demandes par seconde au total. Cela correspondra à un débit d'environ 500 Mo par seconde.

La liste suivante contient quelques éléments à rechercher dans votre application :

- Chaque thread utilise-t-il une connexion séparée ? Si les connexions sont limitées sur l'application, plusieurs threads attendront que la connexion soit disponible et vous remarquerez un débit inférieur.

- Y a-t-il un temps d'attente dans l'application entre deux demandes d'ajout ? Cela réduira le débit effectif d'un thread.
- La limite de bande passante de l'instance : si la bande passante de l'instance est partagée par d'autres applications, cela peut limiter le débit disponible pour les PutSnapshotBlock demandes.

Veillez à prendre note des autres charges de travail qui peuvent être exécutées dans le compte pour éviter les goulots d'étranglement. Vous devez également intégrer des mécanismes de nouvelle tentative dans vos APIs flux de travail directs EBS pour gérer les ralentissements, les délais d'expiration et l'indisponibilité des services.

Passez en revue les quotas de APIs service direct EBS pour déterminer le nombre maximal de demandes d'API que vous pouvez exécuter par seconde. Pour plus d'informations, consultez Points de terminaison et quotas Amazon Elastic Block Store dans AWS General Reference.

Points de terminaison de service pour EBS Direct APIs

Un point de terminaison est une URL qui sert de point d'entrée à un service AWS Web. EBS direct APIs prend en charge les types de terminaux suivants :

- IPv4 points de terminaison
- Des terminaux à double pile qui prennent en charge à la fois et IPv4 IPv6
- Points de terminaison FIPS

Lorsque vous faites une demande, vous pouvez spécifier le point de terminaison et la région à utiliser. Si vous ne spécifiez aucun point de IPv4 terminaison, celui-ci est utilisé par défaut. Pour utiliser un autre type de point de terminaison, vous devez le spécifier dans votre demande. Pour obtenir un exemple de la façon de procéder, consultez Spécification des points de terminaison.

Pour plus d'informations sur les régions, consultez Régions et zones de disponibilité dans le guide de EC2 l'utilisateur Amazon. Pour obtenir la liste des points de terminaison pour EBS direct APIs, voir Points de terminaison pour l'EBS direct dans le. APIs Référence générale d'Amazon Web Services

Rubriques

- IPv4 points de terminaison
- Points de terminaison à double pile (IPv4 et IPv6)
- Points de terminaison FIPS

- Spécification des points de terminaison

IPv4 points de terminaison

IPv4 les terminaux ne prennent en charge que IPv4 le trafic. IPv4 les points de terminaison sont disponibles pour toutes les régions.

EBS direct ne APIs prend en charge que les IPv4 points de terminaison régionaux que vous pouvez utiliser pour effectuer vos demandes. Vous devez spécifier la région dans le nom du point de terminaison. Les noms des points de terminaison utilisent la convention de dénomination suivante :

- `ebs.region.amazonaws.com`

Par exemple, pour diriger vos demandes vers le `us-east-2` IPv4 point de terminaison, vous devez le spécifier `ebs.us-east-2.amazonaws.com` comme point de terminaison. Pour obtenir la liste des points de terminaison pour EBS direct APIs, voir Points de terminaison pour l'EBS direct dans le. APIs Référence générale d'Amazon Web Services

Tarification

Les données transférées directement entre les EC2 instances EBS direct APIs et Amazon via un IPv4 point de terminaison situé dans la même région ne vous sont pas facturées. Toutefois, s'il existe des services intermédiaires, tels que des AWS PrivateLink points de terminaison, une passerelle NAT ou des passerelles Amazon VPC Transit, leurs coûts associés vous sont facturés.

Points de terminaison à double pile (IPv4 et IPv6)

Les terminaux à double pile prennent en charge à la fois le trafic IPv4 et IPv6 le trafic. Les points de terminaison à double pile sont disponibles pour toutes les régions.

Pour l'utiliser IPv6, vous devez utiliser un point de terminaison à double pile. Lorsque vous envoyez une demande à un point de terminaison à double pile, l'URL du point de terminaison correspond à une IPv4 adresse IPv6 ou à une adresse, selon le protocole utilisé par votre réseau et votre client.

EBS Direct ne APIs prend en charge que les points de terminaison régionaux à double pile, ce qui signifie que vous devez spécifier la région dans le nom du point de terminaison. Les noms des points de terminaison à double pile utilisent la convention d'affectation de noms suivante :

- `ebs.region.api.aws`

Par exemple, le nom du point de terminaison à double pile de la région `eu-west-1` est `ebs.eu-west-1.api.aws`. Pour obtenir la liste des points de terminaison pour EBS direct APIs, voir Points de terminaison pour l'EBS direct dans le. APIs Référence générale d'Amazon Web Services

Tarification

Les données transférées directement entre les EC2 instances EBS direct APIs et Amazon à l'aide d'un point de terminaison à double pile situé dans la même région ne vous sont pas facturées. Toutefois, s'il existe des services intermédiaires, tels que des AWS PrivateLink points de terminaison, une passerelle NAT ou des passerelles Amazon VPC Transit, leurs coûts associés vous sont facturés.

Points de terminaison FIPS

EBS direct APIs fournit des points de terminaison à double pile (IPv4 et IPv6) validés FIPS pour IPv4 les régions suivantes :

- `us-east-1` : USA Est (Virginie du Nord)
- `us-east-2` : USA Est (Ohio)
- `us-west-1` : USA Ouest (Californie du Nord)
- `us-west-2` : USA Ouest (Oregon)
- `ca-central-1` : Canada (Centre)

Les IPv4 points de terminaison FIPS utilisent la convention de dénomination suivante :. `ebs-fips.region.amazonaws.com` Par exemple, le point de IPv4 terminaison FIPS pour `us-east-1` est`ebs-fips.us-east-1.amazonaws.com`.

Les points de terminaison FIPS à double pile utilisent la convention d'affectation de noms suivante : `ebs-fips.region.api.aws`. Par exemple, le point de terminaison à double pile FIPS pour `us-east-1` est `ebs-fips.us-east-1.api.aws`.

Pour plus d'informations sur les points de terminaison FIPS, consultez Points de terminaison FIPS dans le Référence générale d'Amazon Web Services.

Spécification des points de terminaison

Cette section fournit quelques exemples sur la manière de spécifier un point de terminaison lors de l'envoi d'une demande.

AWS CLI

Les exemples suivants montrent comment spécifier un point de terminaison pour la région `us-east-2` à l'aide de AWS CLI.

- Double pile

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.api.aws
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.us-east-2.amazonaws.com
```

AWS SDK for Java 2.x

Les exemples suivants montrent comment spécifier un point de terminaison pour la région `us-east-2` à l'aide de AWS SDK for Java 2.x.

- Double pile

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.api.aws", "us-
east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.us-east-2.amazonaws.com",
 "us-east-2");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

AWS SDK for Go

Les exemples suivants montrent comment spécifier un point de terminaison pour la région `us-east-2` à l'aide de AWS SDK pour Go.

- Double pile

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast1RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.api.aws")
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.UsEast1RegionID),
    Endpoint: aws.String("https://ebs.us-east-2.amazonaws.com")
})
```

AWS Exemples de code SDK pour EBS direct APIs

Les exemples de code suivants montrent comment utiliser EBS direct APIs avec un kit de développement AWS logiciel (SDK).

Actions

- Utilisation StartSnapshot avec un AWS SDK ou une CLI
- Utilisation PutSnapshotBlock avec un AWS SDK ou une CLI
- Utilisation CompleteSnapshot avec un AWS SDK ou une CLI

Utilisation **`StartSnapshot`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`StartSnapshot`.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn start(client: &Client, description: &str) -> Result<String, Error> {
    let snapshot = client
        .start_snapshot()
        .description(description)
        .encrypted(false)
        .volume_size(1)
        .send()
        .await?;

    Ok(snapshot.snapshot_id.unwrap())
}
```

- Pour plus de détails sur l'API, voir StartSnapshotla section de référence de l'API AWS SDK for Rust.

Utilisation **`PutSnapshotBlock`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`PutSnapshotBlock`.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn add_block(
    client: &Client,
    id: &str,
    idx: usize,
    block: Vec<u8>,
    checksum: &str,
) -> Result<(), Error> {
    client
        .put_snapshot_block()
        .snapshot_id(id)
        .block_index(idx as i32)
        .block_data(ByteStream::from(block))
        .checksum(checksum)
        .checksum_algorithm(ChecksumAlgorithm::ChecksumAlgorithmSha256)
        .data_length(EBS_BLOCK_SIZE as i32)
        .send()
        .await?;

    Ok(())
}
```

- Pour plus de détails sur l'API, voir PutSnapshotBlockla section de référence de l'API AWS SDK for Rust.

Utilisation **`CompleteSnapshot`** avec un AWS SDK ou une CLI

L'exemple de code suivant montre comment utiliser`CompleteSnapshot`.

Rust

SDK pour Rust

> **Note**
>
> Il y en a plus à ce sujet GitHub. Trouvez l'exemple complet et découvrez comment le configurer et l'exécuter dans le référentiel d'exemples de code AWS.

```
async fn finish(client: &Client, id: &str) -> Result<(), Error> {
```

```
    client
        .complete_snapshot()
        .changed_blocks_count(2)
        .snapshot_id(id)
        .send()
        .await?;

    println!("Snapshot ID {}", id);
    println!("The state is 'completed' when all of the modified blocks have been
 transferred to Amazon S3.");
    println!("Use the get-snapshot-state code example to get the state of the
 snapshot.");

    Ok(())
}
```

- Pour plus de détails sur l'API, voir CompleteSnapshotla section de référence de l'API AWS SDK for Rust.

Création d'une connexion privée entre un VPC et EBS direct APIs

Vous pouvez établir une connexion privée entre votre VPC et EBS directement en créant un point de terminaison VPC d'interface, alimenté APIs par. AWS PrivateLink Vous pouvez accéder à EBS directement APIs comme s'il se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT, de connexion VPN ou de connexion. AWS Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer directement avec EBS. APIs

Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface.

Pour plus d'informations, consultez la section Accès Services AWS par AWS PrivateLink le biais du AWS PrivateLink guide.

Considérations relatives aux points de terminaison APIs VPC directs EBS

Avant de configurer un point de terminaison VPC d'interface pour EBS direct APIs, consultez les considérations du guide.AWS PrivateLink

Par défaut, l'accès complet à EBS direct APIs est autorisé via le point de terminaison. Vous pouvez contrôler l'accès au point de terminaison de l'interface à l'aide des politiques de point de terminaison

VPC. Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès direct à EBS. APIs La politique spécifie les informations suivantes :

- Le principal qui peut effectuer des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être effectuées.

Pour de plus amples informations, veuillez consulter Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Amazon VPC Guide de l'utilisateur.

Voici un exemple de politique de point de terminaison pour EBS direct APIs. Lorsqu'elle est attachée à un point de terminaison, cette politique donne accès à toutes les APIs actions directes d'EBS sur toutes les ressources, à l'exception des instantanés marqués d'une clé `Environment` et d'une valeur. `Test`

```
{
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Environment": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

Création d'un point de terminaison VPC d'interface pour EBS direct APIs

Vous pouvez créer un point de terminaison VPC pour EBS direct à APIs l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Créer un point de terminaison d'un VPC dans le Guide AWS PrivateLink .

Créez un point de terminaison VPC pour EBS direct APIs en utilisant le nom de service suivant :

- `com.amazonaws.region.ebs`

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à EBS directement APIs en utilisant son nom DNS par défaut pour la région, par exemple,`ebs.us-east-1.amazonaws.com`.

Enregistrez les APIs appels directs EBS à l'aide de AWS CloudTrail

EBS Direct APIs est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture les appels passés à l'EBS directement APIs sous forme d'événements. Les appels capturés incluent des appels provenant d'appels à code AWS Management Console et adressés à l'EBS direct APIs. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à EBS directement APIs, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

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 :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur d'IAM Identity Center
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable

des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous pouvez créer un journal de suivi pour une seule région ou un journal de suivi multirégion à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements journalisés pour la Région AWS de ce journal de suivi. Pour plus d'informations sur les journaux de suivi, consultez Création d'un journal de suivi dans votre Compte AWS et Création d'un journal de suivi pour une organisation dans le Guide de l'utilisateur AWS CloudTrail .

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option

de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Événements liés aux APIs données directes d'EBS dans CloudTrail

Les événements de données fournissent des informations sur les opérations de ressource effectuées sur ou dans une ressource. Ils sont également connus sous le nom opérations de plans de données. Les événements de données sont souvent des activités dont le volume est élevé. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Vous pouvez enregistrer les événements de données pour les types de APIs ressources directes EBS à l'aide de la CloudTrail console ou des AWS CLI opérations de CloudTrail l'API. Pour plus d'informations sur la façon de journaliser les événements de données, consultez Journalisation des événements de données avec la AWS Management Console et Journalisation des événements de données avec l' AWS Command Line Interface dans le Guide de l'utilisateur AWS CloudTrail .

Vous pouvez enregistrer les APIs opérations directes EBS suivantes en tant qu'événements de données.

- ListSnapshotBlocks
- ListChangedBlocks
- GetSnapshotBlock
- PutSnapshotBlock

> **Note**
>
> Si vous effectuez une action sur un instantané partagé avec vous, les événements de données ne sont pas envoyés au AWS compte propriétaire de l'instantané.

Événements de APIs gestion directe d'EBS dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Le APIs service EBS direct enregistre les opérations du plan de contrôle suivantes en CloudTrail tant qu'événements de gestion.

- StartSnapshot
- CompleteSnapshot

Exemples d' APIs événements directs EBS

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

Voici des exemples d' CloudTrail événements relatifs à l'EBS direct APIs.

StartSnapshot


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:27:26Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "StartSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "volumeSize": 8,
```

```
        "clientToken": "token",
        "encrypted": true
    },
    "responseElements": {
        "snapshotId": "snap-123456789012",
        "ownerId": "123456789012",
        "status": "pending",
        "startTime": "Jul 3, 2020 11:27:26 PM",
        "volumeSize": 8,
        "blockSize": 524288,
        "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

CompleteSnapshot

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:28:24Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "CompleteSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "snapshotId": "snap-123456789012",
        "changedBlocksCount": 5
    },
    "responseElements": {
        "status": "completed"
    },
```

```
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

ListSnapshotBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-03T00:32:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListSnapshotBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example6-0e12-4aa9-b923-1555eexample",
    "eventID": "example4-218b-4f69-a9e0-2357dexample",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
```

```
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

ListChangedBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        },
       {
```

```
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

GetSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T20:43:05Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "GetSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
```

```
    "resources": [
        {
          "accountId": "123456789012",
          "type": "AWS::EC2::Snapshot",
          "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

PutSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "PutSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "dataLength": 524288,
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
```

```
    "responseElements": {
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "requestID": "example3-d5e0-4167-8ee8-50845example",
    "eventID": "example8-4d9a-4aad-b71d-bb31fexample",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```


Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Questions fréquemment posées sur EBS direct APIs

Est-il possible d'accéder à un instantané à l'aide de l'EBS direct APIs s'il est en attente ?

Non. L'instantané n'est accessible que si son statut est terminé.

Les index des blocs sont-ils renvoyés par l'EBS directement APIs dans l'ordre numérique ?

Oui. Les index de bloc renvoyés sont uniques et classés par ordre numérique.

Puis-je soumettre une demande avec une valeur de MaxResults paramètre inférieure à 100 ?

Non. La valeur de MaxResult paramètre minimale que vous pouvez utiliser est de 100. Si vous soumettez une demande avec une valeur de MaxResult paramètre inférieure à 100 et que l'instantané contient plus de 100 blocs, l'API renverra au moins 100 résultats.

Puis-je exécuter des demandes d'API simultanément ?

Vous pouvez exécuter des demandes d'API simultanément. Veillez à prendre note des autres charges de travail qui peuvent être exécutées dans le compte pour éviter les goulots d'étranglement. Vous devez également intégrer des mécanismes de nouvelle tentative dans vos APIs flux de travail directs EBS pour gérer les ralentissements, les délais d'expiration et l'indisponibilité des services. Pour de plus amples informations, veuillez consulter Optimisez les performances pour EBS Direct APIs.

Passez en revue les quotas de APIs service direct EBS pour déterminer les demandes d'API que vous pouvez exécuter par seconde. Pour plus d'informations, consultez Points de terminaison et quotas Amazon Elastic Block Store dans AWS General Reference.

Lors de l'exécution de l' ListChangedBlocks action, est-il possible d'obtenir une réponse vide même s'il y a des blocs dans l'instantané ?

Oui. Si les blocs modifiés sont rares dans l'instantané, la réponse peut être vide, mais l'API renverra une valeur de jeton de page suivante. Utilisez la valeur de jeton de page suivante pour passer à la page suivante des résultats. Vous pouvez confirmer que vous avez atteint la dernière page de résultats lorsque l'API renvoie une valeur de jeton de page suivante nulle.

Si le NextToken paramètre est spécifié en même temps qu'un StartingBlockIndex paramètre, lequel des deux est utilisé ?

Le NextToken est utilisé et StartingBlockIndex est ignoré.

Quelle est la durée de validité des jetons de bloc et des jetons suivants ?

Les jetons de bloc sont valides pendant sept jours et les jetons suivants sont valides pendant 60 minutes.

Les instantanés chiffrés sont-ils pris en charge ?

Oui. Les instantanés chiffrés sont accessibles à l'aide de l'EBS direct. APIs

Pour accéder à un instantané chiffré, l'utilisateur doit avoir accès à la clé KMS utilisée pour chiffrer le cliché et à l'action de AWS KMS déchiffrement. Consultez la Contrôlez l'accès à EBS direct à APIs l'aide d'IAM section précédente de ce guide pour connaître la AWS KMS politique à attribuer à un utilisateur.

Les instantanés publics sont-ils pris en charge ?

Les instantanés publics ne sont pas pris en charge.

Les instantanés locaux Amazon EBS sur Outposts sont-ils pris en charge ?

Les instantanés locaux Amazon EBS sur Outposts ne sont pas pris en charge.

L'opération ListSnapshotBlocks renvoie-t-elle tous les index de bloc et tous les jetons de bloc d'un instantané, ou seulement ceux dans lesquels des données ont été écrites ?

Elle renvoie uniquement les index de bloc et les jetons de bloc dans lesquels des données ont été écrites.

Puis-je obtenir un historique des appels d'API effectués par EBS directement APIs sur mon compte à des fins d'analyse de sécurité et de résolution des problèmes opérationnels ?

Oui. Pour recevoir l'historique des appels d' APIs API directs EBS effectués sur votre compte, activez AWS CloudTrail le AWS Management Console. Pour de plus amples informations, veuillez consulter Enregistrez les APIs appels directs EBS à l'aide de AWS CloudTrail.

Récupérez des instantanés Amazon EBS supprimés et sauvegardés par EBS AMIs avec Recycle Bin

La corbeille est une fonctionnalité de récupération de données qui vous permet de restaurer des instantanés Amazon EBS supprimés accidentellement et sauvegardés par EBS. AMIs Lorsque vous utilisez la corbeille, si vos ressources sont supprimées, elles sont retenues dans la corbeille pendant une période spécifiée avant leur suppression définitive.

Vous pouvez restaurer une ressource à partir de la corbeille à tout moment avant l'expiration de sa période de rétention. Une fois que vous avez restauré une ressource à partir de la corbeille, elle est supprimée de la corbeille et vous pouvez l'utiliser de la même manière que n'importe quelle autre ressource de ce type sur votre compte. Si la période de rétention expire et que la ressource n'est pas restaurée, elle est définitivement supprimée de la corbeille et n'est plus disponible pour restauration.

L'utilisation de la corbeille aide à garantir la continuité métier en protégeant vos données métier critiques contre toute suppression accidentelle.

Rubriques

- Récupérer les fichiers AMIs supprimés de la corbeille
- Surveillez la corbeille à l'aide d'Amazon EventBridge
- Surveillez l'utilisation de la corbeille AWS CloudTrail
- Points de terminaison de service pour la corbeille
- Création d'une connexion privée entre un VPC et une corbeille

Ressources prises en charge

La corbeille prend en charge les types de ressources suivants :

- Instantanés Amazon EBS

> **Important**
>
> Les règles de conservation de la corbeille s'appliquent également aux instantanés archivés dans le niveau de stockage des archives. Si vous supprimez un instantané archivé qui correspond à une règle de conservation, cet instantané est conservé dans la corbeille pendant la période définie dans la règle de conservation. Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille.

- Amazon Machine Images soutenues par Amazon EBS () AMIs

> **Note**
>
> Les règles de conservation s'appliquent également aux personnes handicapées AMIs.

Comment fonctionne la corbeille ?

Pour activer et utiliser la corbeille, vous devez créer des règles de conservation dans les AWS régions dans lesquelles vous souhaitez protéger vos ressources. Les règles de rétention précisent :

- Type de ressource que vous souhaitez protéger (instantanés ou AMIs).
- Type de règle de conservation :
  - Règles de rétention au niveau des balises : ces règles de conservation utilisent des balises de ressources pour identifier les ressources à protéger. Pour chaque règle de rétention, vous

spécifiez une ou plusieurs paires clé-valeur d'identification. Les ressources (du type spécifié) qui possèdent au moins l'une de ces paires clé/valeur de balise sont automatiquement conservées dans la corbeille lors de leur suppression. Utilisez ce type de règle de conservation pour protéger des ressources spécifiques de votre compte en fonction de leurs balises.

  - Règles de rétention au niveau de la région : ces règles de rétention s'appliquent par défaut à toutes les ressources (du type spécifié) de la région, même si les ressources ne sont pas balisées. Vous pouvez toutefois spécifier des balises d'exclusion pour exclure les ressources dotées de balises spécifiques. Utilisez ce type de règle de rétention pour protéger toutes les ressources d'un type spécifique dans une région.
- Période de conservation des ressources après leur suppression. Une fois cette période expirée, les ressources sont définitivement supprimées de la corbeille.

Lorsqu'une ressource se trouve dans la corbeille, il est possible de la restaurer à tout moment. La ressource reste dans la corbeille jusqu'à ce que l'un des événements suivants se produise :

- Vous le restaurez manuellement pour l'utiliser. Lorsque vous restaurez une ressource à partir de la corbeille, celle-ci est supprimée de la corbeille et elle devient immédiatement disponible pour être utilisée. Vous pouvez utiliser les ressources restaurées de la même manière que n'importe quelle autre ressource de ce type dans votre compte.
- La période de rétention expire. Si la période de rétention expire et que la ressource n'a pas été restaurée à partir de la corbeille, elle est définitivement supprimée de la corbeille et ne peut plus être affichée ou restaurée.

Considérations relatives à la corbeille

Les points suivants s'appliquent lors de l'utilisation de la corbeille et des règles de rétention.

Considérations d'ordre général

- **Important**

  Lorsque vous créez votre première règle de rétention, la règle peut prendre jusqu'à 30 minutes pour s'activer et commencer à retenir les ressources. Après avoir créé la première règle de rétention, les règles de rétention suivantes deviennent actives et commencent à retenir les ressources presque immédiatement.

- Si une ressource correspond à plus d'une règle de conservation lors de la suppression, la règle de conservation ayant la période de conservation la plus longue a la priorité.
- Vous ne pouvez pas supprimer manuellement une ressource de la corbeille. La ressource sera supprimée automatiquement à l'expiration de sa période de rétention.
- Lorsqu'une ressource se trouve dans la corbeille, vous pouvez uniquement l'afficher, la restaurer ou modifier ses identifications. Pour utiliser la ressource d'une autre manière, vous devez d'abord la restaurer.
- Si une ressource Service AWS, telle que AWS Backup ou Amazon Data Lifecycle Manager, supprime une ressource correspondant à une règle de conservation, cette ressource est automatiquement conservée par Recycle Bin. Si nécessaire, vous pouvez empêcher ces ressources d'entrer dans la corbeille lors de leur suppression en les étiquetant, puis en les ajoutant en tant que balises d'exclusion à vos règles de conservation.
- Lorsqu'une ressource est envoyée à la corbeille, l'identification de génération système suivante est affectée à la ressource :
  - Clé d'identification : `aws:recycle-bin:resource-in-bin`
  - Valeur d'identification : `true`

  Vous ne pouvez pas modifier ou supprimer manuellement cette identification. Lorsque la ressource est restaurée à partir de la corbeille, l'identification est automatiquement supprimée.

Considérations relatives aux instantanés

- **Important**

  Si vous avez des règles de conservation pour AMIs et pour les instantanés associés, veillez à ce que la période de conservation des instantanés soit identique ou supérieure à celle du. AMIs Cela garantit que la corbeille ne supprime pas les instantanés associés à une AMI avant de supprimer l'AMI elle-même, car cela rendrait l'AMI irrécupérable.
- Si la restauration rapide d'instantané est activée pour un instantané lorsqu'il est supprimé, elle est automatiquement désactivée peu de temps après l'envoi de l'instantané dans la corbeille.
  - Si vous restaurez l'instantané avant que la restauration rapide d'instantané ne soit désactivée pour l'instantané, elle reste activée.

  - Si vous restaurez l'instantané, une fois que la restauration d'instantané rapide a été désactivée, elle reste désactivée. Si nécessaire, vous devez réactiver manuellement la restauration rapide d'instantané.
- Si un instantané est partagé lors de sa suppression, le partage est automatiquement annulé lorsqu'il est envoyé à la corbeille. Si vous restaurez l'instantané, toutes les autorisations de partage précédentes sont automatiquement restaurées.
- Si un instantané créé par un autre AWS service, par exemple, AWS Backup est envoyé à la corbeille et que vous restaurez ultérieurement cet instantané à partir de la corbeille, il n'est plus géré par le AWS service qui l'a créé. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Considérations relatives à AMIs

- Seuls les produits soutenus par Amazon EBS AMIs sont pris en charge.
-
  > **Important**
  >
  > Si vous avez des règles de conservation pour AMIs et pour les instantanés associés, veillez à ce que la période de conservation des instantanés soit identique ou supérieure à celle du. AMIs Cela garantit que la corbeille ne supprime pas les instantanés associés à une AMI avant de supprimer l'AMI elle-même, car cela rendrait l'AMI irrécupérable.
- Si une AMI est partagée lors de sa suppression, le partage est automatiquement annulé lorsqu'elle est envoyée à la corbeille. Si vous restaurez l'AMI, toutes les autorisations de partage précédentes sont automatiquement restaurées.
- Avant de pouvoir restaurer une AMI à partir de la corbeille, vous devez d'abord restaurer tous les instantanés associés à partir de la corbeille et vous assurer qu'ils se trouvent à l'état `available`.
- Si les instantanés associés à l'AMI sont supprimés de la corbeille, l'AMI n'est plus récupérable. L'AMI sera supprimée à l'expiration de la période de rétention.
- Si une AMI créée par un autre AWS service, tel que AWS Backup, est envoyée dans la corbeille et que vous restaurez ultérieurement cette AMI à partir de la corbeille, elle n'est plus gérée par le AWS service qui l'a créée. Vous devez supprimer manuellement l'AMI si elle n'est plus nécessaire.

Considérations relatives aux politiques d'instantanés Amazon Data Lifecycle Manager

- Si Amazon Data Lifecycle Manager supprime un instantané qui correspond à une règle de conservation, cet instantané est automatiquement conservé par la corbeille.
- Si Amazon Data Lifecycle Manager supprime un instantané et l'envoie à la corbeille lorsque le seuil de rétention de la politique est atteint, et que vous restaurez manuellement l'instantané à partir de la corbeille, vous devez supprimer manuellement cet instantané s'il n'est plus nécessaire. Amazon Data Lifecycle Manager ne gérera plus l'instantané.
- Si vous supprimez manuellement un instantané créé par une politique et que cet instantané se trouve dans la corbeille lorsque le seuil de rétention de la politique est atteint, Amazon Data Lifecycle Manager ne supprime pas l'instantané. Amazon Data Lifecycle Manager ne gère pas les instantanés lorsqu'ils sont stockés dans la corbeille.

  Si l'instantané est restauré à partir de la corbeille avant que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager supprime l'instantané lorsque le seuil de rétention de la politique est atteint.

  Si l'instantané est restauré à partir de la corbeille après que le seuil de rétention de la politique soit atteint, Amazon Data Lifecycle Manager ne supprime plus l'instantané. Vous devez supprimer manuellement l'instantané s'il n'est plus nécessaire.

Considérations relatives à la AWS sauvegarde

- Si AWS Backup supprime un instantané conforme à une règle de conservation, cet instantané est automatiquement conservé par Recycle Bin.

Considérations relatives aux instantanés archivés

- Les règles de conservation de la corbeille s'appliquent également aux instantanés archivés dans le niveau de stockage des archives. Si vous supprimez un instantané archivé qui correspond à une règle de conservation, cet instantané est conservé dans la corbeille pendant la période définie dans la règle de conservation.

  Les instantanés archivés sont facturés au tarif des instantanés archivés lorsqu'ils se trouvent dans la corbeille.

Si une règle de conservation supprime un instantané archivé de la corbeille avant la période d'archivage minimale de 90 jours, vous êtes facturé pour les jours restants. Pour plus d'informations, consultez la section Aperçu des prix et de la facturation archivés.

Pour utiliser un instantané archivé qui se trouve dans la corbeille, vous devez d'abord récupérer l'instantané depuis la corbeille, puis le restaurer du niveau d'archivage au niveau standard.

Quotas

Les quotas suivants s'appliquent à la corbeille.

Quota	Quota par défaut
Règles de rétention par région	250
Paires clé-valeur d'identification par règle de rétention	50

Services connexes

La corbeille fonctionne avec les services suivants :

- AWS CloudTrail : permet d'enregistrer les événements qui se produisent dans la corbeille. Pour de plus amples informations, veuillez consulter Surveillez l'utilisation de la corbeille AWS CloudTrail.

Tarification

Il n'y a pas de facturation supplémentaire pour l'utilisation de la corbeille et des règles de rétention. Pour plus d'informations, consultez la section Tarification d'Amazon EBS.

- Instantanés Amazon EBS : les instantanés placés dans la corbeille sont facturés au même tarif que les instantanés ordinaires de votre compte.
- Soutenu par EBS AMIs : aucun frais supplémentaire n'est facturé pour le stockage AMIs dans la corbeille.

> **Note**
>
> Certaines ressources peuvent encore apparaître dans la console de la corbeille ou dans la sortie de l'API AWS CLI et pendant une courte période après l'expiration de leur période de conservation et leur suppression définitive. Ces ressources ne vous sont pas facturées. La facturation s'arrête dès que la période de rétention expire.

Vous pouvez utiliser les balises de répartition des coûts AWS générées suivantes à des fins de suivi et de répartition des coûts lors de l'utilisation AWS Billing and Cost Management.

- Clé : `aws:recycle-bin:resource-in-bin`
- Valeur : `true`

Pour plus d'informations, veuillez consulter la section Balises de répartition des coûts générées par AWS dans le Guide de l'utilisateur AWS Billing and Cost Management .

Contrôlez l'accès à la corbeille avec IAM

Par défaut, les utilisateurs ne sont pas autorisés à utiliser la corbeille, les règles de rétention ou les ressources contenues dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Rubriques

- Autorisations pour utiliser la corbeille et les règles de rétention
- Autorisations pour utiliser des ressources dans la corbeille
- Clés de condition pour la corbeille

Autorisations pour utiliser la corbeille et les règles de rétention

Pour utiliser la corbeille et les règles de rétention, les utilisateurs ont besoin des autorisations suivantes.

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `tag:GetResources`.

Voici un exemple de politique IAM qui inclut l'autorisation `tag:GetResources` pour les utilisateurs de la console. Si certaines autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rbin:CreateRule",
            "rbin:UpdateRule",
            "rbin:GetRule",
            "rbin:ListRules",
            "rbin:DeleteRule",
            "rbin:TagResource",
            "rbin:UntagResource",
            "rbin:ListTagsForResource",
            "rbin:LockRule",
            "rbin:UnlockRule",
```

```
            "tag:GetResources"
        ],
        "Resource": "*"
    }]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Autorisations pour utiliser des ressources dans la corbeille

Pour plus d'informations sur les autorisations IAM nécessaires pour travailler avec les ressources de la corbeille, reportez-vous aux rubriques suivantes :

- Autorisations pour utiliser des instantanés dans la corbeille
- Autorisations d'utilisation AMIs dans la corbeille

Clés de condition pour la corbeille

La corbeille définit les clés de condition suivantes que vous pouvez utiliser dans l'élément `Condition` d'une politique IAM pour contrôler les conditions d'application de l'instruction de stratégie. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Rubriques

Clé de condition `rbin:Request/ResourceType`

La clé de `rbin:Request/ResourceType` condition peut être utilisée pour filtrer l'accès CreateRuleet les ListRulesdemandes en fonction de la valeur spécifiée pour le paramètre de `ResourceType` demande.

Exemple 1 - CreateRule

L'exemple de politique IAM suivant permet aux principaux IAM de faire des CreateRuledemandes uniquement si la valeur spécifiée pour le paramètre de `ResourceType` demande est ou. `EBS_SNAPSHOT` `EC2_IMAGE` Cela permet au principal de créer de nouvelles règles de conservation pour les instantanés et AMIs uniquement.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Exemple 2 - ListRules

L'exemple de politique IAM suivant permet aux principaux IAM de faire des ListRulesdemandes uniquement si la valeur spécifiée pour le paramètre de `ResourceType` demande est. `EBS_SNAPSHOT` Cela permet au principal de répertorier les règles de rétention pour les instantanés

uniquement, et cela les empêche de répertorier les règles de rétention pour tout autre type de ressource.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Clé de condition **`rbin:Attribute/ResourceType`**

La clé de `rbin:Attribute/ResourceType` condition peut être utilisée pour filtrer l'accès sur DeleteRule, GetRule, UpdateRule, LockRule, UnlockRule, TagResourceUntagResource, et les ListTagsForResourcedemandes en fonction de la valeur de l'`ResourceType`attribut de la règle de rétention.

Exemple 1 - UpdateRule

L'exemple de politique IAM suivant permet aux principaux IAM de faire des UpdateRuledemandes uniquement si l'`ResourceType`attribut de la règle de rétention demandée est ou. `EBS_SNAPSHOT` `EC2_IMAGE` Cela permet au principal de mettre à jour les règles de conservation pour les instantanés et AMIs uniquement.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
```

```
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Exemple 2 - DeleteRule

L'exemple de politique IAM suivant permet aux principaux IAM de faire des DeleteRuledemandes uniquement si l'`ResourceType`attribut de la règle de rétention demandée est. `EBS_SNAPSHOT` Cela permet au principal de supprimer des règles de rétention pour les instantanés uniquement.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:DeleteRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Création d'une règle de conservation de la corbeille

Lorsque vous créez une règle de conservation, vous devez spécifier les paramètres obligatoires suivants :

- Type de ressource à protéger (instantanés ou AMIs).

- Type de règle de rétention (au niveau du tag ou au niveau de la région). Les règles au niveau des balises protègent uniquement les ressources dotées de balises spécifiques. Les règles au niveau de la région protègent toutes les ressources de la région, mais peuvent exclure les ressources dotées de balises spécifiques.
- La durée de conservation, qui peut aller jusqu'à 1 an (365 jours).

Vous pouvez également éventuellement spécifier un nom de règle et une description de 255 caractères maximum chacun, ainsi que des balises pour vous aider à identifier et à organiser vos règles. Nous vous recommandons de ne pas inclure d'informations d'identification personnelle, confidentielles ou sensibles dans le nom, la description ou les tags.

Vous pouvez également éventuellement verrouiller les règles de rétention au niveau de la région lors de leur création. Si vous verrouillez une règle de conservation lors de sa création, vous devez également spécifier le délai de déverrouillage, qui peut aller de 7 à 30 jours. Les règles de conservation restent déverrouillées par défaut, à moins que vous ne les verrouilliez explicitement.

> **Note**
>
> Les règles de rétention fonctionnent uniquement dans les régions où elles ont été créées. Si vous avez l'intention d'utiliser la corbeille dans d'autres régions, vous devez créer des règles de rétention supplémentaires dans ces régions.

Vous pouvez créer une règle de rétention de corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour créer une règle de rétention au niveau des balises

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention), puis Create retention rule (Créer une règle de rétention).
3. (Facultatif) Pour Retention rule name (Nom de la règle de rétention), saisissez un nom descriptif pour la règle de rétention.
4. (Facultatif) Pour Retention rule description (Description de la règle de rétention), saisissez uns brève description pour la règle de rétention.

5. Pour Type de ressource, sélectionnez le type de ressource que la règle de rétention doit protéger. La règle de rétention conservera uniquement les ressources de ce type dans la corbeille.
6. Pour Sélectionner les ressources à conserver, choisissez Conserver les ressources dotées de balises spécifiques.
7. Pour les balises de ressources, entrez les paires clé-valeur de balise à utiliser pour identifier les ressources à conserver dans la corbeille. Seules les ressources du type spécifié qui possèdent au moins l'une des balises spécifiées seront conservées par la règle de rétention.
8. Pour Période de conservation, entrez le nombre de jours pendant lesquels les ressources supprimées sont conservées dans la corbeille.
9. Choisissez Create retention rule (Créer une règle de rétention).

Pour créer une règle de rétention au niveau de la région

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention), puis Create retention rule (Créer une règle de rétention).
3. (Facultatif) Pour Retention rule name (Nom de la règle de rétention), saisissez un nom descriptif pour la règle de rétention.
4. (Facultatif) Pour Retention rule description (Description de la règle de rétention), saisissez uns brève description pour la règle de rétention.
5. Pour Type de ressource, sélectionnez le type de ressource que la règle de rétention doit protéger. La règle de rétention conservera uniquement les ressources de ce type dans la corbeille.
6. Pour Sélectionner les ressources à conserver, choisissez Conserver toutes les ressources.
7. (Facultatif) Pour exclure les ressources dotées de balises spécifiques, pour les balises d'exclusion, entrez jusqu'à cinq paires clé-valeur de balise à utiliser pour identifier les ressources à exclure. Les ressources dotées de l'une de ces balises sont ignorées par la règle de rétention.
8. Pour Période de conservation, entrez le nombre de jours pendant lesquels les ressources supprimées sont conservées dans la corbeille.
9. (Facultatif) Pour verrouiller la règle de conservation, dans Rule lock settings (Paramètres de verrouillage des règles), sélectionnez Lock (Verrouiller), puis dans Unlock delay period (Délai

de déverrouillage), spécifiez le délai de déverrouillage en jours. Une règle de conservation verrouillée ne peut être ni modifiée ni supprimée. Pour modifier ou supprimer la règle, vous devez d'abord la déverrouiller, puis attendre l'expiration du délai de déverrouillage. Pour plus d'informations, consultez Verrouiller une règle de conservation de la corbeille pour empêcher sa mise à jour ou sa suppression.

Pour laisser la règle de conservation déverrouillée, dans Rule lock settings(Paramètres de verrouillage des règles), conservez l'option Unlock (Déverrouiller). Une règle de conservation déverrouillée peut être modifiée ou supprimée à tout moment.

> **Note**
>
> Vous ne pouvez pas verrouiller les règles de rétention au niveau de la région qui comportent des balises d'exclusion.

10. Choisissez Create retention rule (Créer une règle de rétention).

AWS CLI

Pour créer une règle de rétention

Utilisez la commande create-rule de la AWS CLI . Pour `--retention-period`, spécifiez le nombre de jours de rétention des instantanés supprimés dans la corbeille. Pour`--resource-type`, spécifiez `EBS_SNAPSHOT` pour les instantanés ou `EC2_IMAGE` pour AMIs. Pour créer une règle de rétention au niveau des identifications, pour `--resource-tags`, spécifiez les identifications à utiliser afin d'identifier les instantanés à retenir. Pour créer une règle de rétention au niveau de la région, omettez`--resource-tags`, et éventuellement spécifiez`--exclude-resource-tags`, pour exclure les ressources dotées de balises spécifiques. Pour verrouiller une règle de rétention au niveau de la région`--lock-configuration`, incluez et spécifiez le délai de déverrouillage en jours.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value \
--exclude-resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Exemple 1

L'exemple de commande suivant crée une règle de conservation au niveau de la région déverrouillée qui conserve tous les instantanés supprimés pendant une période de 7 jours.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

Exemple 2

L'exemple de commande suivant crée une règle de niveau identification qui retient les instantanés supprimés qui sont étiquetés `purpose=production` pendant une période de 7 jours.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Exemple 3

L'exemple de commande suivant crée une règle de conservation au niveau de la région verrouillée qui conserve tous les instantanés supprimés pendant une période de 7 jours. La règle de conservation est verrouillée avec un délai de déverrouillage de 7 jours.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Exemple 4

L'exemple de commande suivant crée une règle de rétention déverrouillée au niveau de la région qui conserve tous les instantanés supprimés, à l'exception des instantanés marqués avec`purpose:testing`, pendant plusieurs jours. 7

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
```

```
--description "Match only production snapshots" \
--exclude-resource-tags ResourceTagKey=purpose,ResourceTagValue=testing
```

Mettre à jour une règle de conservation de la corbeille existante

Vous pouvez mettre à jour la description d'une règle de conservation déverrouillée, ses balises de ressource et sa période de conservation à tout moment après sa création. Vous ne pouvez pas mettre à jour le type de ressource ou le délai de déverrouillage d'une règle de conservation, même si la règle de conservation est déverrouillée.

Vous ne pouvez en aucun cas mettre à jour une règle de conservation verrouillée. Si vous devez modifier une règle de conservation verrouillée, vous devez d'abord la déverrouiller, puis attendre l'expiration du délai de déverrouillage.

Si vous devez modifier le délai de déverrouillage d'une règle de conservation verrouillée, vous devez déverrouiller la règle de conservation, puis attendre l'expiration du délai de déverrouillage actuel. Lorsque le délai de déverrouillage est expiré, vous devez verrouiller à nouveau la règle de conservation et spécifier le nouveau délai de déverrouillage.

> **Note**
>
> Nous vous recommandons de ne pas inclure de données d'identification personnelle, confidentielles ou sensibles dans la description de la règle de rétention.

Une fois que vous avez mis à jour une règle de rétention, les modifications s'appliquent uniquement aux nouvelles ressources qu'elle retient. Les modifications n'affectent pas les ressources précédemment envoyées à la corbeille. Par exemple, si vous mettez à jour la période de rétention d'une règle de rétention, seuls les instantanés supprimés après la mise à jour sont retenus pour la nouvelle période de rétention. Les instantanés envoyés à la corbeille avant la mise à jour sont retenus pendant la période de rétention précédente (ancienne).

Vous pouvez mettre à jour une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour mettre à jour une règle de rétention

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/

2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de rétention à mettre à jour, puis choisissez Actions, Edit retention rule (Modifier une règle de rétention).
4. Dans la section Rule details (Détails de la règle), mettez à jour Retention rule name (Nom de la règle de rétention) et Retention rule description (Description de la règle de rétention), si nécessaire.
5. Dans la section Rule settings (Paramètres de la règle), mettez à jour Resource type (Type de ressource), Resource tags to match (Identifications de ressource à faire correspondre) et Retention period (Période de rétention), si nécessaire.
6. Dans la section Tags (Identifications), ajoutez ou supprimez des identifications de règles de rétention si nécessaire.
7. Choisissez Save retention rule (Enregistrer la règle de rétention).

AWS CLI

Pour mettre à jour une règle de rétention

Utilisez la commande update-site de la AWS CLI . Pour`--identifier`, spécifiez l'ID de la règle de conservation à mettre à jour pour`--resource-types`, spécifiez `EBS_SNAPSHOT` pour les instantanés ou `EC2_IMAGE` pour AMIs.

```
aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

Exemple

L'exemple de commande suivant met à jour la règle de rétention `6lsJ2Fa9nh9` pour retenir tous les instantanés pour 7 jours et met à jour sa description.

```
aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

Verrouiller une règle de conservation de la corbeille pour empêcher sa mise à jour ou sa suppression

La corbeille vous permet de verrouiller les règles de conservation au niveau de la région à tout moment.

Une règle de conservation verrouillée ne peut être ni modifiée ni supprimée, même par les utilisateurs disposant des autorisations IAM requises. Verrouillez vos règles de conservation pour les protéger contre les modifications et les suppressions accidentelles ou malveillantes.

Lorsque vous verrouillez une règle de conservation, vous devez spécifier un délai de déverrouillage. Il s'agit de la période de temps que vous devez attendre après avoir déverrouillé la règle de conservation avant de pouvoir la modifier ou la supprimer. Vous ne pouvez ni modifier ni supprimer la règle de conservation pendant le délai de déverrouillage. Vous pouvez modifier ou supprimer la règle de conservation qu'une fois le délai de déverrouillage expiré.

Vous ne pouvez pas modifier la période de déverrouillage après le verrouillage de la règle de conservation. Si les autorisations de votre compte ont été compromises, le délai de déverrouillage vous donne plus de temps pour détecter les menaces de sécurité et y répondre. La durée de cette période doit être plus longue que le temps nécessaire à pour identifier les failles de sécurité et y répondre. Pour définir la durée appropriée, vous pouvez passer en revue les incidents de sécurité précédents et le temps nécessaire pour identifier et corriger une violation de compte.

Nous vous recommandons d'utiliser EventBridge les règles Amazon pour vous informer des modifications de l'état de verrouillage des règles de rétention. Pour de plus amples informations, veuillez consulter Surveillez la corbeille à l'aide d'Amazon EventBridge.

Considérations

- Vous ne pouvez pas verrouiller les règles de rétention au niveau des balises, ni les règles de rétention au niveau de la région comportant des balises d'exclusion.
- Vous pouvez verrouiller une règle de conservation déverrouillée à tout moment.
- Le délai de déverrouillage doit être de 7 à 30 jours.
- Vous pouvez verrouiller à nouveau une règle de conservation pendant le délai de déverrouillage. Verrouiller à nouveau la règle de conservation réinitialise le délai de déverrouillage.

Vous pouvez verrouiller une règle de conservation au niveau de la région à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour verrouiller une règle de conservation

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/
2. Dans le panneau de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de conservation déverrouillée que vous souhaitez verrouiller, puis choisissez Actions, Edit retention rule lock (Modifier le verrouillage d'une règle de conservation).
4. Dans l'écran Edit retention rule lock (Modifier le verrouillage d'une règle de conservation), choisissez Lock (Verrouiller), puis pour Unlock delay period (Délai de déverrouillage), spécifiez le délai de déverrouillage en jours.
5. Cochez la case I acknowledge that locking the retention rule will prevent it from being modified or deleted (Je reconnais que le verrouillage de la règle de conservation empêchera sa modification ou sa suppression), puis choisissez Save (Enregistrer).

AWS CLI

Pour verrouiller une règle de conservation déverrouillée

Utilisez la commande AWS CLI lock-rule. Pour `--identifier`, spécifiez l'ID de la règle de conservation à verrouiller. Pour `--lock-configuration`, spécifiez le délai de déverrouillage en jours.

```
aws rbin lock-rule \
--identifier rule_ID \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Exemple

L'exemple de commande suivant verrouille la règle de conservation `6lsJ2Fa9nh9` et définit le délai de déverrouillage sur 15 jours.

```
aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
```

```
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Déverrouillez une règle de conservation de la corbeille pour permettre sa mise à jour ou sa suppression

Vous ne pouvez ni modifier ni supprimer une règle de conservation verrouillée. Si vous devez modifier une règle de conservation verrouillée, vous devez d'abord la déverrouiller. Après avoir déverrouillé la règle de rétention, vous devez attendre que le délai de déverrouillage expire avant de pouvoir la modifier ou la supprimer. Vous ne pouvez ni modifier ni supprimer une règle de conservation pendant le délai de déverrouillage.

Une règle de conservation déverrouillée peut être modifiée et supprimée à tout moment par un utilisateur disposant des autorisations IAM requises. Le fait de laisser vos règles de conservation déverrouillées peut les exposer à des modifications et à des suppressions accidentelles ou malveillantes.

Considérations

- Vous pouvez verrouiller à nouveau une règle de conservation pendant le délai de déverrouillage.
- Vous pouvez verrouiller à nouveau une règle de conservation une fois le délai de déverrouillage expiré.
- Vous ne pouvez pas contourner le délai de déverrouillage.
- Vous ne pouvez pas modifier le délai de déverrouillage après le verrouillage initial.

Nous vous recommandons d'utiliser EventBridge les règles Amazon pour vous informer des modifications de l'état de verrouillage des règles de rétention. Pour de plus amples informations, veuillez consulter Surveillez la corbeille à l'aide d'Amazon EventBridge.

Vous pouvez déverrouiller une règle de conservation au niveau de la région à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour déverrouiller une règle de conservation

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/
2. Dans le panneau de navigation, choisissez Retention rules (Règles de rétention).

3. Dans la grille, sélectionnez la règle de conservation verrouillée que vous souhaitez déverrouiller, puis choisissez Actions, Edit retention rule lock (Modifier le verrouillage d'une règle de conservation).
4. Sur l'écran Edit retention rule lock (Modifier le verrouillage d'une règle de conservation), choisissez Unlock (Déverrouiller), puis Save (Enregistrer).

AWS CLI

Pour déverrouiller une règle de conservation verrouillée

Utilisez la commande AWS CLI unlock-rule. Pour `--identifier`, spécifiez l'ID de la règle de conservation à déverrouiller.

```
aws rbin unlock-rule \
--identifier rule_ID
```

Exemple

L'exemple de commande suivant déverrouille la règle de conservation `6lsJ2Fa9nh9`

```
aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

Marquer une règle de conservation de la corbeille

Vous pouvez affecter des identifications personnalisées à vos règles de rétention pour classer celles-ci de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Cela vous permet de trouver de manière efficace une règle de rétention spécifique en fonction des identifications personnalisées que vous avez affectées.

Vous pouvez affecter une identification à une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour étiqueter une règle de rétention

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/

2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention à étiqueter, choisissez l'onglet Tags (Identifications), puis choisissez Manage tags (Gérer les identifications).
4. Choisissez Ajouter une balise. Pour Key (Clé), saisissez la clé de l'identification. Pour Value (Valeur), saisissez la valeur de l'identification.
5. Choisissez Save (Enregistrer).

AWS CLI

Pour étiqueter une règle de rétention

Utilisez la commande tag-resource AWS CLI . Pour `--resource-arn`, indiquez l'Amazon Resource Name (ARN) de la règle de rétention à étiqueter, et pour `--tags`, spécifiez la paire clé-valeur d'identification.

```
aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

Exemple

L'exemple de commande suivant étiquette la règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3` avec l'identification `purpose=production`.

```
aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \
--tags key=purpose,value=production
```

Afficher les identifications de règle de rétention

Vous pouvez afficher les identifications affectées à une règle de rétention à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour afficher les identifications d'une règle de rétention

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/

2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention pour laquelle afficher les identifications, puis choisissez l'onglet Tags (Identifications).

AWS CLI

Pour afficher les identifications affectées à une règle de rétention

Utilisez la commande list-tags-for-resource. AWS CLI Pour `--resource-arn`, spécifiez l'ARN de la règle de rétention.

```
aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

Exemple

L'exemple de commande suivant répertorie les identifications de règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3
```

Supprimer les identifications des règles de rétention

Vous pouvez supprimer les identifications d'une règle de rétention en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour supprimer une identification d'une règle de rétention

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/
2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Sélectionnez la règle de rétention dont vous souhaitez supprimer une identification et choisissez Tags (Identifications), puis Manage tags (Gérer les identifications).
4. Choisissez Remove (Supprimer) en regard de l'identification à supprimer.
5. Choisissez Save (Enregistrer).

AWS CLI

Pour supprimer une identification d'une règle de rétention

Utilisez la commande untag-resource de la AWS CLI . Pour `--resource-arn`, spécifiez l'ARN de la règle de rétention. Pour `--tagkeys`, spécifiez les clés d'identifications des identifications à supprimer.

```
aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

Exemple

Voici un exemple de commande supprimant les identifications disposant d'une clé d'identification de type `purpose` de la règle de rétention `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

Supprimer une règle de rétention de la corbeille pour l'empêcher de conserver les ressources

Vous pouvez supprimer une règle de rétention à tout moment. Lorsque vous supprimez une règle de rétention, elle ne retient plus les nouvelles ressources dans la corbeille une fois qu'elles ont été supprimées. Les ressources envoyées à la corbeille avant la suppression de la règle de rétention continuent d'être retenues dans la corbeille en fonction de la période de rétention définie dans la règle de rétention. Lorsque la période expire, l'instantané est définitivement supprimé de la corbeille.

Vous pouvez supprimer une règle de rétention en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour supprimer une règle de rétention

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/

2. Dans le volet de navigation, choisissez Retention rules (Règles de rétention).
3. Dans la grille, sélectionnez la règle de rétention à supprimer, puis choisissez Actions, Delete retention rule (Supprimer la règle de rétention).
4. Lorsque vous y êtes invité, saisissez le message de confirmation et choisissez Delete retention rule (Supprimer la règle de rétention).

AWS CLI

Pour supprimer une règle de rétention

Utilisez la commande delete-rule de la AWS CLI . Pour `--identifier`, spécifiez l'ID de la règle de rétention à supprimer.

```
aws rbin delete-rule --identifier rule_ID
```

Exemple

L'exemple de commande suivant supprime la règle de rétention `6lsJ2Fa9nh9`.

```
aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

Récupérez les instantanés supprimés de la corbeille

Rubriques

- Autorisations pour utiliser des instantanés dans la corbeille
- Afficher les instantanés dans la corbeille
- Restaurer des instantanés à partir de la corbeille

Autorisations pour utiliser des instantanés dans la corbeille

Par défaut, les utilisateurs ne sont pas autorisés à utiliser les instantanés contenus dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Pour afficher et récupérer des instantanés qui se trouvent dans la corbeille, les utilisateurs doivent disposer des autorisations suivantes :

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Pour gérer les identifications des instantanés dans la corbeille, les utilisateurs ont besoin des autorisations supplémentaires suivantes.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `ec2:DescribeTags`.

Voici un exemple de politique IAM. Elle comprend l'autorisation `ec2:DescribeTags` pour les utilisateurs de la console et les autorisations `ec2:CreateTags` et `ec2:DeleteTags` pour la gestion des identifications. Si les autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },
```

```
    ]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.
- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations nécessaires pour utiliser la corbeille, consultez Autorisations pour utiliser la corbeille et les règles de rétention.

Afficher les instantanés dans la corbeille

Lorsqu'un instantané se trouve dans la corbeille, vous pouvez afficher des informations limitées à son sujet, notamment :

- ID de l'instantané
- la description de l'instantané ;
- l'ID du volume à partir duquel l'instantané a été créé ;
- la date et l'heure de la suppression de l'instantané et de son entrée dans la corbeille ;
- la date et l'heure d'expiration de la période de rétention ; à ce moment-là, l'instantané sera définitivement supprimé de la corbeille.

Vous pouvez afficher les instantanés dans la corbeille à l'aide de l'une des méthodes suivantes.

Recycle Bin console

Pour visualiser les instantanés dans la corbeille à l'aide de la console

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les instantanés qui se trouvent actuellement dans la corbeille. Pour afficher les détails d'un instantané spécifique, sélectionnez-le dans la grille et choisissez Actions, View details (Afficher les détails).

AWS CLI

Pour afficher des instantanés dans la corbeille à l'aide du AWS CLI

Utilisez la AWS CLI commande list-snapshots-in-recycle-bin. Incluez l'option `--snapshot-id` pour afficher un instantané spécifique ou omettez l'option `--snapshot-id` pour afficher tous les instantanés dans la corbeille.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Par exemple, la commande suivante renvoie des informations sur l'instantané `snap-01234567890abcdef` dans la corbeille.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Exemple de sortie :

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Restaurer des instantanés à partir de la corbeille

Vous ne pouvez en aucun cas utiliser un instantané lorsqu'il se trouve dans la corbeille. Pour utiliser l'instantané, vous devez d'abord le restaurer. Lorsque vous restaurez un instantané à partir de la corbeille, il est immédiatement disponible pour utilisation et il est supprimé de la corbeille. Une fois qu'il est restauré, vous pouvez l'utiliser de la même manière que n'importe quel autre instantané de votre compte.

Vous pouvez restaurer un instantané à partir de la corbeille en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour restaurer un instantané à partir de la corbeille en utilisant la console

1. Ouvrez la console de la corbeille à la https://console.aws.amazon.com/rbin/maison/
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie tous les instantanés qui se trouvent actuellement dans la corbeille. Sélectionnez l'instantané à restaurer, puis choisissez Recover (Récupérer).
4. Lorsque vous y êtes invité, choisissez Recover (Récupérer).

AWS CLI

Pour restaurer un instantané supprimé de la corbeille à l'aide du AWS CLI

Utilisez la AWS CLI commande restore-snapshot-from-recycle-bin. Pour `--snapshot-id`, spécifiez l'ID de l'instantané à restaurer.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Par exemple, la commande suivante restaure l'instantané `snap-01234567890abcdef` depuis la corbeille.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Exemple de sortie :

```
{
```

```
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

Récupérer les fichiers AMIs supprimés de la corbeille

Rubriques

- Autorisations d'utilisation AMIs dans la corbeille
- Afficher AMIs dans la corbeille
- Restaurer AMIs à partir de la corbeille

Autorisations d'utilisation AMIs dans la corbeille

Par défaut, les utilisateurs ne sont pas autorisés à travailler avec ceux AMIs qui se trouvent dans la corbeille. Pour permettre aux utilisateurs de travailler avec ces ressources, vous devez créer des politiques IAM qui accordent l'autorisation d'utiliser des ressources et des actions d'API spécifiques. Une fois les politiques créées, vous devez ajouter des autorisations à vos utilisateurs, groupes ou rôles.

Pour consulter et récupérer AMIs le contenu de la corbeille, les utilisateurs doivent disposer des autorisations suivantes :

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

Pour gérer les balises AMIs dans la corbeille, les utilisateurs ont besoin des autorisations supplémentaires suivantes.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Pour utiliser la console de la corbeille, les utilisateurs ont besoin de l'autorisation `ec2:DescribeTags`.

Voici un exemple de politique IAM. Elle comprend l'autorisation `ec2:DescribeTags` pour les utilisateurs de la console et les autorisations `ec2:CreateTags` et `ec2:DeleteTags` pour la gestion des identifications. Si les autorisations ne sont pas nécessaires, vous pouvez les supprimer de la politique.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListImagesInRecycleBin",
            "ec2:RestoreImageFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region::image/*"
      }
    ]
}
```

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d'identité :

  Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d'un rôle pour un utilisateur IAM dans le Guide de l'utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique Ajout d'autorisations à un utilisateur (console) du Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations nécessaires pour utiliser la corbeille, consultez Autorisations pour utiliser la corbeille et les règles de rétention.

Afficher AMIs dans la corbeille

Lorsqu'une AMI se trouve dans la corbeille, vous pouvez afficher des informations limitées à son sujet, notamment :

- Le nom, la description et l'ID unique de l'AMI.
- La date et l'heure de la suppression de l'AMI et de son entrée dans la corbeille.
- la date et l'heure d'expiration de la période de rétention ; L'AMI sera définitivement supprimée à ce moment-là.

Vous pouvez les afficher AMIs dans la corbeille en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour afficher les fichiers supprimés AMIs dans la corbeille à l'aide de la console

1. Ouvrez la console Recycle Bin sur console.aws.amazon. com/rbin/home/.
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie toutes les ressources qui se trouvent actuellement dans la corbeille. Pour afficher les détails d'une AMI spécifique, sélectionnez-la dans la grille et choisissez Actions, View details (Afficher les détails).

AWS CLI

Pour afficher les fichiers supprimés AMIs dans la corbeille à l'aide du AWS CLI

Utilisez la AWS CLI commande list-images-in-recycle-bin. Pour une vue spécifique AMIs, incluez l'`--image-id`option et spécifiez IDs celle AMIs à afficher. Vous pouvez en spécifier jusqu'à 20 IDs dans une seule demande.

Pour afficher tout ce qui se trouve AMIs dans la corbeille, omettez l'`--image-id`option. Si vous ne spécifiez pas de valeur pour `--max-items`, la commande renvoie par défaut 1 000 éléments par page. Pour plus d'informations, consultez la section Pagination dans le manuel Amazon EC2 API Reference.

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Par exemple, la commande suivante renvoie des informations sur l'AMI `ami-01234567890abcdef` dans la corbeille.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Exemple de sortie :

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

Important

Si le message d'erreur suivant s'affiche, il se peut que vous deviez mettre à jour votre AWS CLI version. Pour plus d'informations, veuillez consulter la rubrique Erreurs liées aux commandes introuvables.

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

Restaurer AMIs à partir de la corbeille

Vous ne pouvez en aucun cas utiliser une AMI lorsqu'elle se trouve dans la corbeille. Pour utiliser l'AMI, vous devez d'abord la restaurer. Lorsque vous restaurez une AMI à partir de la corbeille, elle est immédiatement disponible pour utilisation et elle est supprimée de la corbeille. Une fois qu'elle est restaurée, vous pouvez l'utiliser de la même manière que n'importe quelle autre AMI de votre compte.

Vous pouvez restaurer une AMI à partir de la corbeille en utilisant l'une des méthodes suivantes.

Recycle Bin console

Pour restaurer une AMI depuis la corbeille en utilisant la console

1. Ouvrez la console Recycle Bin sur console.aws.amazon. com/rbin/home/.
2. Dans le volet de navigation, choisissez Recycle Bin (Corbeille).
3. La grille répertorie toutes les ressources qui se trouvent actuellement dans la corbeille. Sélectionnez l'AMI à restaurer, puis choisissez Recover (Récupérer).
4. Lorsque vous y êtes invité, choisissez Recover (Récupérer).

AWS CLI

Pour restaurer une AMI supprimée de la corbeille à l'aide du AWS CLI

Utilisez la AWS CLI commande restore-image-from-recycle-bin. Pour `--image-id`, spécifiez l'ID de l'AMI à restaurer.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Par exemple, la commande suivante restaure l'AMI `ami-01234567890abcdef` depuis la corbeille.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

La commande ne renvoie aucun résultat en cas de succès.

> **Important**
>
> Si le message d'erreur suivant s'affiche, il se peut que vous deviez mettre à jour votre AWS CLI version. Pour plus d'informations, veuillez consulter la rubrique Erreurs liées aux commandes introuvables.
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

Surveillez la corbeille à l'aide d'Amazon EventBridge

La corbeille envoie des événements à Amazon EventBridge pour les actions effectuées sur les règles de rétention. Avec EventBridge, vous pouvez établir des règles qui initient des actions programmatiques en réponse à ces événements. Par exemple, vous pouvez créer une EventBridge règle qui envoie une notification à votre adresse e-mail lorsqu'une règle de rétention est déverrouillée et qu'elle entre dans son délai de déverrouillage. Pour plus d'informations, consultez Création de EventBridge règles Amazon qui réagissent aux événements.

Les événements dans EventBridge sont représentés sous forme d'objets JSON. Les champs spécifiques à l'événement figurent dans la section `detail` de l'objet JSON. Le champ `event` contient le nom de l'événement. Le champ `result` contient l'état terminé de l'action qui lance l'événement. Pour plus d'informations, consultez les modèles EventBridge d'événements Amazon dans le guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations sur Amazon EventBridge, consultez Qu'est-ce qu'Amazon EventBridge ? dans le guide de EventBridge l'utilisateur Amazon.

Événements

- RuleLocked
- RuleChangeAttempted
- RuleUnlockScheduled
- RuleUnlockingNotice
- RuleUnlocked

RuleLocked

Voici un exemple d'événement généré par la corbeille lorsqu'une règle de conservation est correctement verrouillée. Cet événement peut être généré par CreateRuledes LockRuledemandes. L'API qui a généré l'événement est indiquée dans le champ `api-name`.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Locked",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "api-name": "CreateRule"
 }
 }
```

RuleChangeAttempted

Voici un exemple d'événement généré par la corbeille lors de tentatives infructueuses de modification ou de suppression d'une règle verrouillée. Cet événement peut être généré par DeleteRuledes UpdateRuledemandes. L'API qui a généré l'événement est indiquée dans le champ `api-name`.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Change Attempted",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
```

```
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "api-name": "DeleteRule"
 }
 }
```

RuleUnlockScheduled

Voici un exemple d'événement généré par la corbeille lorsqu'une règle de conservation est déverrouillée et qu'elle commence son délai de déverrouillage.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlock Scheduled",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "scheduled-unlock-time": "2022-09-10T16:37:50Z",
 }
 }
```

RuleUnlockingNotice

Voici un exemple d'événement généré quotidiennement par la corbeille alors qu'une règle de conservation est dans son délai de déverrouillage, jusqu'à la veille de l'expiration du délai de déverrouillage.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlocking Notice",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "scheduled-unlock-time": "2022-09-10T16:37:50Z"
 }
 }
```

RuleUnlocked

Voici un exemple d'événement généré par la corbeille lorsque le délai de déverrouillage d'une règle de conservation expire et que la règle de rétention peut être modifiée ou supprimée.

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlocked",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
```

```
"arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
],
"detail":
{
"detail-version": " 1.0.0",
"rule-id": "a12345abcde",
"rule-description": "locked account level rule",
"unlock-delay-period": "30 days",
"scheduled-unlock-time": "2022-09-10T16:37:50Z"
}
}
```

Surveillez l'utilisation de la corbeille AWS CloudTrail

Le service Recycle Bin est intégré à AWS CloudTrail. CloudTrail est un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture tous les appels d'API effectués dans la corbeille sous forme d'événements. Si vous créez un suivi, vous pouvez activer la diffusion continue des CloudTrail événements vers un bucket Amazon Simple Storage Service (Amazon S3). Si vous ne configurez pas de suivi, vous pouvez toujours consulter les derniers événements de gestion dans la CloudTrail console dans Historique des événements. Vous pouvez utiliser les informations collectées CloudTrail pour déterminer la demande qui a été faite à Recycle Bin, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des informations supplémentaires.

Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur la corbeille dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité événementielle prise en charge se produit dans la corbeille, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris les événements liés à Recycle Bin, créez un parcours. Un journal permet CloudTrail de fournir des fichiers journaux à un compartiment S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique

à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez la section Overview for creating a trail dans le Guide de l'utilisateur AWS CloudTrail .

Actions d'API prises en charge

Pour Recycle Bin, vous pouvez CloudTrail enregistrer les actions d'API suivantes en tant qu'événements de gestion.

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

Pour plus d'informations sur les événements de gestion de journalisation, consultez la section Événements de gestion de journalisation pour les sentiers dans le guide de CloudTrail l'utilisateur.

Informations relatives à l'identité

Chaque événement ou entrée du journal contient des informations sur la personne qui a généré la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- 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 CloudTrail userIdentityElement.

Comprendre les entrées du fichier journal de la corbeille

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment 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.

Voici des exemples d'entrées de CloudTrail journal.

CreateRule


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:45:22Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "CreateRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
```

```
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"retentionPeriod": {
  "retentionPeriodValue": 7,
  "retentionPeriodUnit": "DAYS"
},
"description": "Match all snapshots",
"resourceType": "EBS_SNAPSHOT"
},
"responseElements": {
"identifier": "jkrnexample"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```


GetRule


```
{
"eventVersion": "1.08",
"userIdentity": {
"type": "AssumedRole",
"principalId": "123456789012",
"arn": "arn:aws:iam::123456789012:root",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
```

```
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
}
},
"eventTime": "2021-08-02T21:45:33Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "GetRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"identifier": "jkrnexample"
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```


ListRules


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
```

```
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
}
},
"eventTime": "2021-08-02T21:44:37Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "ListRules",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"resourceTags": [
  {
    "resourceTagKey": "test",
    "resourceTagValue": "test"
  }
]
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
```

```
 }
```

UpdateRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:46:03Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "UpdateRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
 "requestParameters": {
 "identifier": "jkrnexample",
 "retentionPeriod": {
   "retentionPeriodValue": 365,
   "retentionPeriodUnit": "DAYS"
 },
 "description": "Match all snapshots",
 "resourceType": "EBS_SNAPSHOT"
 },
```

```
 "responseElements": null,
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

DeleteRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:46:25Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "DeleteRule",
```

```
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
 "requestParameters": {
 "identifier": "jkrnexample"
 },
 "responseElements": null,
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

TagResource

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
```

```
    "creationDate": "2021-10-22T21:38:34Z"
  }
 }
 },
 "eventTime": "2021-10-22T21:43:15Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "TagResource",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
 "requestParameters": {
 "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
 "tags": [
  {
    "key": "purpose",
    "value": "production"
  }
 ]
 },
 "responseElements": null,
 "requestID": "examplee-7962-49ec-8633-795efexample",
 "eventID": "example4-6826-4c0a-bdec-0bab1example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```


UntagResource


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
```

```
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-10-22T21:38:34Z"
  }
}
},
"eventTime": "2021-10-22T21:44:16Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UntagResource",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
"requestParameters": {
"resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
"tagKeys": [
  "purpose"
]
},
"responseElements": null,
"requestID": "example7-6c1e-4f09-9e46-bb957example",
"eventID": "example6-75ff-4c94-a1cd-4d5f5example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
```

```
 }
```

ListTagsForResource


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-10-22T21:38:34Z"
   }
 }
 },
 "eventTime": "2021-10-22T21:42:31Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "ListTagsForResource",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
 "requestParameters": {
 "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
 },
 "responseElements": null,
 "requestID": "example8-10c7-43d4-b147-3d9d9example",
 "eventID": "example2-24fc-4da7-a479-c9748example",
 "readOnly": true,
 "eventType": "AwsApiCall",
 "managementEvent": true,
```

```
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

LockRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "creationDate": "2022-10-25T00:45:11Z",
     "mfaAuthenticated": "false"
   }
 }
 },
 "eventTime": "2022-10-25T00:45:19Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "LockRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "python-requests/2.25.1",
 "requestParameters": {
 "identifier": "jkrnexample",
 "lockConfiguration": {
```

```
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
}
},
"responseElements": {
"identifier": "jkrnexample",
"description": "",
"resourceType": "EBS_SNAPSHOT",
"retentionPeriod": {
  "retentionPeriodValue": 7,
  "retentionPeriodUnit": "DAYS"
},
"resourceTags": [],
"status": "available",
"lockConfiguration": {
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
},
"lockState": "locked"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

UnlockRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
```

```
"type": "AssumedRole",
"principalId": "123456789012",
"arn": "arn:aws:iam::123456789012:root",
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "creationDate": "2022-10-25T00:45:11Z",
    "mfaAuthenticated": "false"
  }
}
},
"eventTime": "2022-10-25T00:46:17Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UnlockRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "python-requests/2.25.1",
"requestParameters": {
"identifier": "jkrnexample"
},
"responseElements": {
"identifier": "jkrnexample",
"description": "",
"resourceType": "EC2_IMAGE",
"retentionPeriod": {
  "retentionPeriodValue": 7,
  "retentionPeriodUnit": "DAYS"
},
"resourceTags": [],
"status": "available",
"lockConfiguration": {
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
```

```
},
"lockState": "pending_unlock",
"lockEndTime": "Nov 1, 2022, 12:46:17 AM"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```


Points de terminaison de service pour la corbeille

Un point de terminaison est une URL qui sert de point d'entrée à un service AWS Web. La corbeille prend en charge les types de terminaux suivants :

- IPv4 points de terminaison
- Des terminaux à double pile qui prennent en charge à la fois et IPv4 IPv6
- Points de terminaison FIPS

Lorsque vous faites une demande, vous pouvez spécifier le point de terminaison et la région à utiliser. Si vous ne spécifiez aucun point de terminaison, le IPv4 point de terminaison est utilisé par défaut. Pour utiliser un autre type de point de terminaison, vous devez le spécifier dans votre demande. Pour obtenir un exemple de la façon de procéder, consultez Spécification des points de terminaison.

Pour la corbeille, voir Points de terminaison de la corbeille dans le Référence générale d'Amazon Web Services.

Rubriques

- IPv4 points de terminaison

- Points de terminaison à double pile (IPv4 et IPv6)
- Points de terminaison FIPS
- Spécification des points de terminaison

IPv4 points de terminaison

IPv4 les terminaux ne prennent en charge que IPv4 le trafic. IPv4 les points de terminaison sont disponibles pour toutes les régions.

Vous devez spécifier la région dans le nom du point de terminaison. Les noms des points de terminaison utilisent la convention de dénomination suivante :

- corbeille. *region*.amazonaws.com

Par exemple, le IPv4 point de terminaison pour la région USA Est (Virginie du Nord) est`rbin.us-east-1.amazonaws.com`.

Points de terminaison à double pile (IPv4 et IPv6)

Les terminaux à double pile prennent en charge à la fois le trafic IPv4 et IPv6 le trafic. Les points de terminaison à double pile sont disponibles pour toutes les régions.

Pour l'utiliser IPv6, vous devez utiliser un point de terminaison à double pile. Lorsque vous envoyez une demande à un point de terminaison à double pile, l'URL du point de terminaison correspond à une IPv4 adresse IPv6 ou à une adresse, selon le protocole utilisé par votre réseau et votre client.

Vous devez spécifier la région dans le nom du point de terminaison. Les noms des points de terminaison à double pile utilisent la convention d'affectation de noms suivante :

- `rbin.`*region*`.api.aws`

Par exemple, le point de terminaison à double pile pour la région de l'est des États-Unis (Virginie du Nord) est`rbin.us-east-1.api.aws`.

Points de terminaison FIPS

La corbeille fournit des points de terminaison validés par la norme FIPS IPv4 et à double pile (IPv4 et IPv6) pour les régions suivantes :

- `us-east-1` : USA Est (Virginie du Nord)
- `us-east-2` : USA Est (Ohio)
- `us-west-1` : USA Ouest (Californie du Nord)
- `us-west-2` : USA Ouest (Oregon)
- `ca-central-1` : Canada (Centre)
- `ca-west-1`— Canada Ouest (Calgary)

Les IPv4 points de terminaison FIPS utilisent la convention de dénomination suivante :. `rbin-fips.region.amazonaws.com` Par exemple, le point de IPv4 terminaison FIPS pour la région de l'est des États-Unis (Virginie du Nord) est`rbin-fips.us-east-1.amazonaws.com`.

Les points de terminaison FIPS à double pile utilisent la convention d'affectation de noms suivante : `rbin-fips.region.api.aws`. Par exemple, le point de terminaison FIPS à double pile pour la région USA Est (Virginie du Nord) est. `rbin-fips.us-east-1.api.aws`

Spécification des points de terminaison

Les exemples suivants montrent comment spécifier un point de terminaison pour la région `us-east-2` à l'aide de AWS CLI.

- Double pile

```
aws rbin get-rule \
--identifier rule_id \
--endpoint-url https://rbin.us-east-2.api.aws
```

- IPv4

```
aws rbin get-rule \
--identifier rule_id \
--endpoint-url https://rbin.us-east-2.amazonaws.com
```

Création d'une connexion privée entre un VPC et une corbeille

Vous pouvez établir une connexion privée entre votre VPC et la corbeille en créant un point de terminaison VPC d'interface, alimenté par. AWS PrivateLink Vous pouvez accéder à la corbeille comme si elle se trouvait dans votre VPC, sans utiliser de passerelle Internet, de périphérique NAT,

de connexion VPN ou AWS Direct Connect de connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec Recycle Bin.

Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que vous activez pour le point de terminaison d'interface.

Pour plus d'informations, consultez la section Accès aux AWS services AWS PrivateLink dans le AWS PrivateLink Guide.

Création d'un point de terminaison VPC d'interface pour la corbeille

Vous pouvez créer un point de terminaison VPC pour Recycle Bin à l'aide de la console Amazon VPC ou du. AWS CLI Pour plus d'informations, consultez Créer un point de terminaison d'un VPC dans le Guide AWS PrivateLink .

Créez un point de terminaison VPC pour Recycle Bin en utilisant le nom de service suivant : `com.amazonaws.region.rbin`

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à Recycle Bin en utilisant son nom DNS par défaut pour la région, par exemple,`rbin.us-east-1.amazonaws.com`.

Création d'une politique de point de terminaison VPC pour Recycle Bin

Par défaut, l'accès complet à la corbeille est autorisé via le point de terminaison. Vous pouvez contrôler l'accès au point de terminaison de l'interface à l'aide des politiques de point de terminaison VPC. Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès à la corbeille. La politique spécifie les informations suivantes :

- Le principal qui peut effectuer des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être effectuées.

Pour de plus amples informations, veuillez consulter Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Amazon VPC Guide de l'utilisateur.

```
{
    "Statement": [
    {
```

```
        "Effect": "Allow",
        "Action": "rbin:*",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Effect": "Deny",
        "Action": "rbin:DeleteRule",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "StringEquals" : {
                "rbin:Attribute/ResourceType": "EBS_SNAPSHOT"
            }
        }
    }]
}
```

Sécurité sur Amazon EBS

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures 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 AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Elastic Block Store, consultez la section AWS Services concernés par programme de conformitéAWS .
- 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 lors de l'utilisation d'AmazonEBS. Les rubriques suivantes expliquent comment configurer Amazon pour EBS atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos EBS ressources Amazon.

Rubriques

Protection des données dans Amazon EBS

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Elastic Block Store. 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 Amazon EBS ou une autre entreprise à Services AWS 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.

Rubriques

Sécurité des données Amazon EBS

Les volumes Amazon EBS vous sont présentés comme des périphériques de stockage en mode bloc bruts non formatés. Ces appareils sont des périphériques logiques créés sur l'infrastructure EBS et le service Amazon EBS garantit que les appareils sont logiquement vides (c'est-à-dire que les blocs bruts sont mis à zéro ou contiennent des données pseudo-aléatoires cryptographiques) avant toute utilisation ou réutilisation par un client.

Si vous avez des procédures qui exigent que toutes les données soient effacées à l'aide d'une méthode spécifique, après ou avant utilisation (ou les deux), telles que celles détaillées dans DoD 5220.22-M (National Industrial Security Program Operating Manual) ou NIST 800-88 (Guidelines for Media Sanitization), vous avez la possibilité de le faire sur Amazon EBS. Cette activité de niveau bloc sera reflétée sur le support de stockage sous-jacent du service Amazon EBS.

Chiffrement au repos et en transit

Le chiffrement Amazon EBS est une solution de chiffrement qui vous permet de chiffrer vos volumes Amazon EBS et vos instantanés Amazon EBS à l'aide de clés cryptographiques. AWS Key Management Service Les opérations de chiffrement EBS ont lieu sur les serveurs hébergeant les EC2 instances Amazon, garantissant ainsi la sécurité data-in-transitentre une instance et le volume attaché et les instantanés ultérieurs. data-at-rest Pour de plus amples informations, veuillez consulter EBSChiffrement Amazon.

Gestion des clés KMS

Lorsque vous créez un volume ou un instantané Amazon EBS chiffré, vous spécifiez une AWS Key Management Service clé. Par défaut, Amazon EBS utilise la clé KMS AWS gérée pour Amazon EBS dans votre compte et votre région (`aws/ebs`). Vous pouvez toutefois spécifier une clé KMS gérée par le client que vous créez et gérez. L'utilisation d'une clé KMS gérée par le client vous donne plus de flexibilité, notamment la possibilité de créer, de faire pivoter et de désactiver des clés KMS.

Pour utiliser une clé KMS gérée par le client, vous devez autoriser les utilisateurs à utiliser la clé KMS. Pour de plus amples informations, veuillez consulter Autorisations pour les utilisateurs .

> **Important**
>
> Amazon EBS prend uniquement en charge les clés KMS symétriques. Vous ne pouvez pas utiliser de clés KMS asymétriques pour chiffrer un volume Amazon EBS et des instantanés. Pour savoir si une clé KMS est symétrique ou asymétrique, voir Identifier les clés KMS asymétriques.

Pour chaque volume, Amazon EBS demande de AWS KMS générer une clé de données unique chiffrée sous la clé KMS que vous spécifiez. Amazon EBS stocke la clé de données chiffrée avec le volume. Ensuite, lorsque vous attachez le volume à une EC2 instance Amazon, Amazon EBS appelle AWS KMS pour déchiffrer la clé de données. Amazon EBS utilise la clé de données en texte brut de la mémoire de l'hyperviseur pour chiffrer toutes les E/S du volume. Pour de plus amples informations, veuillez consulter Comment fonctionne EBS le chiffrement Amazon.

Gestion des identités et des accès pour Amazon EBS

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 Amazon EBS. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon EBS.

Utilisateur du service : si vous utilisez le service Amazon EBS 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 d'Amazon EBS pour effectuer votre travail, il se peut que vous ayez 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 d'Amazon EBS, consultezRésoudre les problèmes d'autorisation Amazon EBS.

Administrateur du service — Si vous êtes responsable des ressources Amazon EBS au sein de votre entreprise, vous avez probablement un accès complet à Amazon EBS. Il vous incombe de déterminer à quelles fonctionnalités et ressources Amazon EBS les utilisateurs de vos services 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 Amazon EBS, consultez. Comment Amazon EBS 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 Amazon EBS. Pour consulter des exemples de politiques basées sur l'identité Amazon EBS que vous pouvez utiliser dans IAM, consultez. Exemples de politiques IAM pour Amazon EBS

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 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 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 SCPs, voir 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, consultez la section Resource control policies (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 Amazon EBS fonctionne avec IAM

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

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Elastic Block Store

Fonctionnalité IAM	Assistance Amazon EBS
Politiques basées sur l'identité	Oui

Fonctionnalité IAM	Assistance Amazon EBS
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Non

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

Politiques basées sur l'identité pour Amazon EBS

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 Amazon EBS

Pour consulter des exemples de politiques basées sur l'identité Amazon EBS, consultez. Exemples de politiques IAM pour Amazon EBS

Politiques basées sur les ressources au sein d'Amazon EBS

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 Amazon EBS

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 Amazon EBS, consultez Actions, ressources et clés de condition pour Amazon EC2 et Actions, ressources et clés de condition pour Amazon EBS dans la référence d'autorisation de service.

Les actions politiques dans Amazon EBS utilisent soit le préfixe, `ec2` soit le `ebs` préfixe avant l'action.

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
  "ec2:action1",
  "ec2:action2"
]
```

Pour consulter des exemples de politiques basées sur l'identité Amazon EBS, consultez. Exemples de politiques IAM pour Amazon EBS

Ressources relatives aux politiques pour Amazon EBS

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": "*"
```

Certaines actions de l'API Amazon EBS prennent en charge plusieurs ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules. Par exemple, `DescribeVolumes` accède à vol-01234567890abcdef et vol-09876543210fedcba, de sorte qu'un principal doit être autorisé à accéder aux deux ressources.

```
"Resource": [
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-01234567890abcdef",
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-09876543210fedcba"
]
```

Clés de conditions de politique pour Amazon EBS

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.

Par exemple, la condition suivante permet au principal d'effectuer une action sur un volume uniquement si le type de volume est`gp2`.

```
"Condition":{
  "StringLikeIfExists":{
    "ec2:VolumeType":"gp2"
  }
}
```

Pour consulter la liste des clés de condition Amazon EBS, consultez la section Actions, ressources et clés de condition dans la référence d'autorisation de service.

ACLs dans Amazon EBS

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 Amazon EBS

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 Amazon EBS

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.

Autorisations principales interservices pour Amazon EBS

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 Amazon EBS

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 associées à un rôle de service peut perturber les fonctionnalités d'Amazon EBS. Modifiez les rôles de service uniquement lorsque Amazon EBS fournit des instructions à cet effet.

Rôles liés à un service pour Amazon EBS

Prend en charge les rôles liés à un service : non

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 IAM pour Amazon EBS

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Amazon EBS. 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 dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

- Bonnes pratiques en matière de politiques
- Autoriser les utilisateurs à utiliser la console Amazon EBS
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Permettre aux utilisateurs de travailler avec des volumes
- Permettre aux utilisateurs de travailler avec des instantanés

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Amazon EBS 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.

Autoriser les utilisateurs à utiliser la console Amazon EBS

Pour accéder à la console Amazon Elastic Block Store, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter

les informations relatives aux ressources Amazon EBS 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 Amazon EBS, associez également Amazon EBS *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": "*"
        }
    ]
}
```

Permettre aux utilisateurs de travailler avec des volumes

Exemples

- Exemple : Attacher et détacher des volumes
- Exemple : Créer un volume
- Exemple : Créer un volume avec des balises
- Exemple : utilisation de volumes à l'aide de la EC2 console Amazon

Exemple : Attacher et détacher des volumes

Quand une action d'API requiert qu'un principal spécifie plusieurs ressources, vous devez créer une déclaration de politique qui permet aux utilisateurs d'accéder à toutes les ressources requises. Si vous devez utiliser un élément `Condition` avec une ou plusieurs de ces ressources, vous devez créer plusieurs déclarations, comme dans l'exemple ci-dessous.

La politique suivante permet aux utilisateurs d'associer des volumes avec le tag « `volume_user` = iam-user-name» aux instances portant le tag `department=dev` « », et de détacher ces volumes de ces instances. Si vous attachez cette politique à un groupe IAM, la variable de politique `aws:username` accorde à chaque utilisateur du groupe l'autorisation d'attacher des volumes aux instances (ou de les en détacher) avec une balise nommée `volume_user` qui a son nom d'utilisateur comme valeur.

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

```
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/volume_user": "${aws:username}"
        }
      }
    }
  ]
}
```

Exemple : Créer un volume

La politique suivante permet aux utilisateurs d'utiliser l'action CreateVolumeAPI. L'utilisateur est autorisé à créer un volume uniquement si le volume est chiffré et seulement si la taille du volume est inférieure à 20 Gio.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
```

```
      "Condition":{
         "NumericLessThan": {
             "ec2:VolumeSize" : "20"
          },
          "Bool":{
              "ec2:Encrypted" : "true"
          }
       }
    }
  ]
}
```

Exemple : Créer un volume avec des balises

La stratégie suivante inclut la clé de condition `aws:RequestTag` qui exige aux utilisateurs d'attribuer des balises aux volumes qu'ils créent avec les balises `costcenter=115` et `stack=prod`. Si les utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

Pour les actions de création de ressources qui appliquent des balises, les utilisateurs doivent être autorisés à effectuer l'action `CreateTags`. La deuxième déclaration utilise la clé de condition `ec2:CreateAction` pour permettre aux utilisateurs de créer des balises uniquement dans le contexte de `CreateVolume`. Les utilisateurs ne peuvent pas attribuer des balises à des volumes existants ou à d'autres ressources.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Sid": "AllowCreateTaggedVolumes",
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
       }
     },
     {
       "Effect": "Allow",
```

```
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "CreateVolume"
       }
      }
    }
  ]
}
```

La politique suivante permet aux utilisateurs de créer un volume sans avoir à spécifier des balises. L'action `CreateTags` est uniquement évaluée si les balises sont spécifiées dans la demande `CreateVolume`. Si les utilisateurs spécifient une balise, elle doit être `purpose=test`. Aucune autre balise n'est autorisée dans la demande.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "CreateVolume"
          },
         "ForAllValues:StringEquals": {
             "aws:TagKeys": "purpose"
          }
       }
    }
  ]
```

```
}
```

Exemple : utilisation de volumes à l'aide de la EC2 console Amazon

La politique suivante autorise les utilisateurs à consulter et à créer des volumes, ainsi qu'à attacher et détacher des volumes à des instances spécifiques à l'aide de la EC2 console Amazon.

Les utilisateurs peuvent attacher un volume aux instances ayant la balise "`purpose=test`", ainsi que détacher des volumes de ces instances. Pour attacher un volume à l'aide de la EC2 console Amazon, il est utile que les utilisateurs soient autorisés à utiliser l'`ec2:DescribeInstances`action, car cela leur permet de sélectionner une instance dans une liste préremplie dans la boîte de dialogue Attacher un volume. Cependant, comme cela permet aussi aux utilisateurs d'afficher toutes les instances sur la page Instances de la console, vous pouvez ignorer cette action.

Dans la première déclaration, l'action `ec2:DescribeAvailabilityZones` est nécessaire pour garantir qu'un utilisateur puisse sélectionner une zone de disponibilité lors de la création d'un volume.

Les utilisateurs ne peuvent pas baliser les volumes qu'ils créent (pendant ou après la création de volume).

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateVolume",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/purpose": "test"
```

```
        }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:volume/*"
   }
   ]
}
```

Permettre aux utilisateurs de travailler avec des instantanés

Voici des exemples de politiques applicables à la fois `CreateSnapshot` (point-in-timeinstantané d'un volume EBS) et `CreateSnapshots` (instantanés multi-volumes).

Exemples

- Exemple : Créer un instantané
- Exemple : Créer des instantanés
- Exemple : Créer un instantané avec des balises
- Exemple : Créer des instantanés multi-volumes avec des identifications
- Exemple : Copier des instantanés
- Exemple : Modifier les paramètres d'autorisation d'instantanés

Exemple : Créer un instantané

La politique suivante permet aux clients d'utiliser l'action CreateSnapshotAPI. Le client peut créer des instantanés uniquement si le volume est chiffré et seulement si la taille du volume est inférieure à 20 Gio.

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

```
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "NumericLessThan":{
               "ec2:VolumeSize":"20"
            },
            "Bool":{
               "ec2:Encrypted":"true"
            }
         }
      }
   ]
}
```

Exemple : Créer des instantanés

La politique suivante permet aux clients d'utiliser l'action CreateSnapshotsAPI. Le client ne peut créer des instantanés que si tous les volumes de l'instance sont de type GP2.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*"
   ]
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:volume/*",
         "Condition":{
            "StringLikeIfExists":{
               "ec2:VolumeType":"gp2"
             }
```

```
      }

       }
   ]
}
```

Exemple : Créer un instantané avec des balises

La stratégie suivante inclut la clé de condition `aws:RequestTag`, qui nécessite que le client applique les balises `costcenter=115` et `stack=prod` à tout nouvel instantané. Si les utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

Pour les actions de création de ressources qui appliquent des balises, les clients doivent être autorisés à effectuer l'action `CreateTags`. La troisième déclaration utilise la clé de condition `ec2:CreateAction` pour permettre aux clients de créer des balises uniquement dans le contexte de `CreateSnapshot`. Les clients ne peuvent pas attribuer des balises à des volumes existants ou à d'autres ressources.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*"
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
```

```
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshot"
            }
         }
      }
   ]
}
```

Exemple : Créer des instantanés multi-volumes avec des identifications

La politique suivante comprend la clé de condition `aws:RequestTag` qui exige que le client applique les identifications `costcenter=115` et `stack=prod` lors de la création d'un jeu d'instantanés multi-volumes. Si les utilisateurs ne transmettent pas ces balises spécifiques ou s'ils ne spécifient pas du tout de balises, la demande échoue.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*",
"arn:aws:ec2:*:*:volume/*"

   ]
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
```

```
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshots"
            }
         }
      }
   ]
}
```

La politique suivante permet aux clients de créer un instantané sans avoir à spécifier des balises. L'action `CreateTags` est évaluée uniquement si des balises sont spécifiées dans la demande `CreateSnapshot` ou `CreateSnapshots`. Les identifications peuvent être omises dans la demande. Si une balise est spécifiée, elle doit être de type `purpose=test`. Aucune autre balise n'est autorisée dans la demande.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshot"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

La politique suivante permet aux clients de créer des jeux d'instantanés multi-volumes sans avoir à spécifier des identifications. L'action `CreateTags` est évaluée uniquement si des balises sont spécifiées dans la demande `CreateSnapshot` ou `CreateSnapshots`. Les identifications peuvent être omises dans la demande. Si une balise est spécifiée, elle doit être de type `purpose=test`. Aucune autre balise n'est autorisée dans la demande.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshots"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

La stratégie suivante permet de créer des instantanés uniquement si le volume source est balisé avec `User:`*`username`* pour le client et que l'instantané lui-même est balisé avec `Environment:Dev` et `User:`*`username`*. Le client peut ajouter des balises supplémentaires à l'instantané.

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
```

```
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

La stratégie suivante pour `CreateSnapshots` permet de créer des instantanés uniquement si le volume source est balisé avec `User:username` pour le client et que l'instantané lui-même est balisé avec `Environment:Dev` et `User:username`.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:instance/*",
 },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
```

```
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

La stratégie suivante permet de supprimer un instantané uniquement s'il est balisé à l'aide de User:username pour le client.

```
{
   "Version":"2012-10-17",
   "Statement": [
            {
         "Effect":"Allow",
         "Action":"ec2:DeleteSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      }
   ]
}
```

La stratégie suivante permet à un client de créer un instantané mais l'empêche d'exécuter cette action si l'instantané créé comporte une clé de balise `value=stack`.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

La stratégie suivante permet à un client de créer des instantanés mais l'empêche d'exécuter cette action si les instantanés créés comportent une clé de balise `value=stack`.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
```

```
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

La politique suivante vous permet d'associer plusieurs actions dans une même politique. Vous pouvez uniquement créer un instantané (dans le contexte de `CreateSnapshots`) lorsque l'instantané est créé dans la région `us-east-1`. Vous pouvez uniquement créer des instantanés (dans le contexte de `CreateSnapshots`) lorsque les instantanés sont créés dans la région `us-east-1` et que le type d'instance est `t2*`.

```
{
   "Version":"2012-10-17",
   "Statement": [
          {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ],
         "Condition":{
            "StringEqualsIgnoreCase": {
              "ec2:Region": "us-east-1"
            },
            "StringLikeIfExists": {
              "ec2:InstanceType": ["t2.*"]
            }
         }
      }
   ]
```

```
}
```

Exemple : Copier des instantanés

Les autorisations de niveau ressource spécifiées pour l'action CopySnapshot s'appliquent uniquement au nouvel instantané. Elles ne peuvent pas être spécifiées pour l'instantané source.

L'exemple de stratégie suivant permet aux principaux de copier des instantanés uniquement si le nouvel instantané est créé avec la clé de balise `purpose` et la valeur de balise `production` (`purpose=production`).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotWithTags",
            "Effect": "Allow",
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2:*:account-id:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "production"
                }
            }
        }
    ]
}
```

Exemple : Modifier les paramètres d'autorisation d'instantanés

La politique suivante autorise la modification d'un instantané uniquement si celui-ci est étiqueté avec`User:username`, où se `username` trouve le nom d'utilisateur du AWS compte du client. La demande échoue si cette condition n'est pas respectée.

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:ModifySnapshotAttribute",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
```

```
            "StringEquals":{
               "aws:ResourceTag/user-name":"${aws:username}"
            }
         }
      }
   ]
}
```

Résoudre les problèmes d'autorisation Amazon EBS

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon EBS et IAM.

Problèmes

- Je ne suis pas autorisé à effectuer une action dans Amazon EBS
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon EBS

Je ne suis pas autorisé à effectuer une action dans Amazon EBS

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'utilisateur `mateojackson` IAM essaie d'utiliser la console pour afficher les détails d'un volume mais ne dispose pas des `ec2:DescribeVolumes` autorisations nécessaires.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeVolumes on resource: volume-id
```

Dans ce cas, Mateo demande à son AWS administrateur de l'autoriser à décrire le volume.

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 Amazon EBS.

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 effectuer une action dans Amazon EBS. 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 autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Amazon EBS

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 Amazon EBS prend en charge ces fonctionnalités, consultezComment Amazon EBS 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 Amazon EBS

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Architecture axée sur la HIPAA sécurité et la conformité sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent AWS créer HIPAA des applications éligibles.

> **Note**
>
> Tous ne Services AWS sont pas HIPAA éligibles. Pour plus d'informations, consultez la référence des services HIPAA éligibles.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière

de sécurisation Services AWS et reprennent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité PCIDSS, par exemple en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience des données sur Amazon EBS

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

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, Amazon EBS propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

- Automatisation des EBS instantanés à l'aide d'Amazon Data Lifecycle Manager
- Copier des EBS instantanés d'une région à l'autre

Outils de surveillance pour Amazon EBS

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon Elastic Block Store et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AmazonEBS, signaler un problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrailcapture API les appels et les événements connexes effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. La gestion APIs de vos EBS volumes et de vos instantanés fait partie d'Amazon EC2API. Pour plus d'informations sur Amazon CloudTrail et sur Amazon EC2API, consultez la section Enregistrer les EC2 API appels Amazon AWS CloudTrailà l'aide du guide de EC2 l'utilisateur Amazon.
- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre CPU l'utilisation ou d'autres indicateurs de vos EC2 instances Amazon et lancer automatiquement de nouvelles instances en cas de besoin. Pour de plus amples informations, veuillez consulter the section called “Amazon CloudWatch”.
- Amazon EventBridge peut être utilisé pour automatiser vos AWS services et répondre automatiquement aux événements du système, tels que les problèmes de disponibilité des applications ou les modifications des ressources. Les événements AWS liés aux services sont diffusés EventBridge en temps quasi réel. Vous pouvez écrire des règles simples pour préciser les événements qui vous intéressent et les actions automatisées à effectuer quand un événement correspond à une règle. Pour de plus amples informations, veuillez consulter the section called “Amazon EventBridge”.
- Les statistiques de performance EBS détaillées d'Amazon fournissent des statistiques de performances d'E/S en temps réel pour les EBS volumes Amazon attachés à des instances Amazon EC2 basées sur Nitro. Pour plus d'informations, consultez Statistiques de performance EBS détaillées d'Amazon.
- Amazon GuardDuty aide à détecter les activités potentiellement malveillantes dans vos EC2 instances. GuardDuty Malware Protection for EC2 scanne les EBS volumes attachés à vos

EC2 instances. Pour de plus amples informations, veuillez consulter the section called "Amazon GuardDuty".

CloudWatch Métriques Amazon pour Amazon EBS

Les CloudWatch métriques Amazon sont des données statistiques que vous pouvez utiliser pour consulter, analyser et définir des alarmes relatives au comportement opérationnel de vos volumes.

Les données sont disponibles automatiquement toutes les minutes sans coût aucun.

Lorsque vous obtenez des données CloudWatch, vous pouvez inclure un paramètre de `Period` demande pour spécifier la granularité des données renvoyées. Cette option est différente de la période que nous utilisons quand nous collectons les données (périodes de 1 minute). Il est recommandé de spécifier une période dans votre demande qui soit égale ou supérieure à la période de collection pour garantir que les données retournées sont valides.

Vous pouvez obtenir les données à l'aide de la console Amazon CloudWatch API ou de la EC2 console Amazon. La console prend les données brutes du CloudWatch API et affiche une série de graphiques basés sur ces données. Selon vos besoins, vous préférerez peut-être utiliser les données de la console API ou les graphiques de la console.

Rubriques

- Mesures relatives aux EBS volumes Amazon
- Métriques pour les EBS instantanés Amazon
- Métriques d'instances Nitro
- Métriques de restauration d'instantané rapide
- Graphiques de EC2 la console Amazon

Mesures relatives aux EBS volumes Amazon

L'espace de `AWS/EBS` noms inclut les métriques suivantes pour les EBS volumes attachés à tous les types d'instances. Tous les types de EBS volumes Amazon envoient automatiquement des métriques d'une minute à CloudWatch, mais uniquement lorsque le volume est attaché à une instance.

Pour obtenir des informations sur l'espace disque disponible à partir du système d'exploitation sur une instance, consultez Afficher l'espace disque disponible.

> **Note**
>
> Certaines de ces métriques présentent des différences par rapport aux instances conçues sur le système Nitro. Pour obtenir la liste de ces types d'instances, consultez Instances créées sur le système Nitro.

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeAvgReadLatency`	**Note** Pris en charge pour tous les types de volumes attachés aux instances Nitro. Non publié pour les volumes attachés à Amazon ECS et AWS Fargate les tâches. Temps moyen nécessaire pour effectuer les opérations de lecture en une minute. Utilisez cette métrique pour surveiller la latence d'E/S moyenne des EBS volumes attachés à vos EC2 instances	Millisecondes	`VolumeId` | `InstanceID`	`Minimum` | `Maximum`

Métrique	Description	Unités	Dimensions	Statistiques significatives
	Amazon. La moyenne est calculée sur la base des opérations d'E/S effectuées au cours de la dernière minute. Si aucune opération n'est terminée au cours de la dernière minute, la valeur de la métrique est zéro. Pour les volumes compatibles avec l'attachement multiple, utilisez la `InstanceID` dimension pour afficher la latence moyenne pour un attachement d'instance de volume spécifique.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeAvgWriteLatency`	**Note** Pris en charge pour tous les types de volumes attachés aux instances Nitro. Non publié pour les volumes attachés à Amazon ECS et AWS Fargate les tâches. Temps moyen nécessaire pour effectuer les opérations d'écriture en une minute. Utilisez cette métrique pour surveiller la latence d'E/S moyenne des EBS volumes attachés à vos EC2 instances Amazon. La moyenne est calculée sur la base des opérations d'E/S effectuées au cours de la dernière minute. Si aucune opération n'est terminée au cours de la	Millisecondes	`VolumeId` | `InstanceID`	`Minimum` | `Maximum`

Métrique	Description	Unités	Dimensions	Statistiques significatives
	dernière minute, la valeur de la métrique est zéro. Pour les volumes compatibles avec l'attachement multiple, utilisez la `InstanceID` dimension pour afficher la latence moyenne pour un attachement d'instance de volume spécifique.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeIOPSExceededCheck`	**Note** Pris en charge pour tous les types de volumes, à l'exception des volumes magnétiques (`standard`), attachés aux instances Nitro. Non pris en charge avec les volumes activés pour l'attachement multiple. Non publié pour les volumes attachés à Amazon ECS et AWS Fargate les tâches. Indique si une application a constamment tenté d'obtenir un disque IOPS dont les performances étaient supérieures aux IOPS performances allouées	Aucun	`VolumeId` | `InstanceID`	• `Sum` • `Average` • `Minimum` | `Maximum`

Métrique	Description	Unités	Dimensions	Statistiques significatives
	au volume au cours de la dernière minute. Cette métrique peut être soit `0` (provisionnée IOPS non dépassée) soit 1 (provisionnée IOPS dépassée). Pour de plus amples informations, veuillez consulter Surveillez les caractéristiques des E/S à l'aide de CloudWatch.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeThroughputExceededCheck`	**Note** Pris en charge pour tous les types de volumes, à l'exception des volumes magnétiques (`standard`), attachés aux instances Nitro. Non pris en charge avec les volumes activés pour l'attachement multiple. Non publié pour les volumes attachés à Amazon ECS et AWS Fargate les tâches. Indique si une application a constamment tenté de générer un débit supérieur aux performances de débit allouées au volume au cours de la dernière minute. Cette	Aucun	`VolumeId` | `InstanceID`	• `Sum` • `Average` • `Minimum` | `Maximum`

Métrique	Description	Unités	Dimensions	Statistiques significatives
	métrique peut être `0` (débit provisionné non dépassé) ou 1 (débit provisionné dépassé). Pour plus d'informations, consultez. Surveillez les caractéristiques des E/S à l'aide de CloudWatch			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeReadBytes`	Fournit des informations sur les opérations de lecture au cours d'une période donnée. • Les rapports statistiques `Sum` indiquent le nombre total d'octets transférés pendant la période. • Les rapports statistiques `Average` indiquent la taille moyenne de chaque opération de lecture durant la période, sauf pour les volumes attachés à une instance Nitro, pour lesquels la moyenne représente la moyenne sur la période spécifiée. • La statistique `SampleCount` indique le nombre total d'opérations de lecture durant la période, sauf pour les volumes attachés à une instance basée sur Nitro, pour lesquels le nombre d'échantillons représent	Octets	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances basées sur Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
	e le nombre de points de données utilisés pour le calcul statistique. **Note** Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité de lecture se produit sur le volume.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeWriteBytes`	Fournit des informations sur les opérations d'écriture au cours d'une période donnée. • Les rapports statistiques `Sum` indiquent le nombre total d'octets transférés pendant la période. • Les rapports statistiques `Average` indiquent la taille moyenne de chaque opération d'écriture durant la période, sauf pour les volumes attachés à une instance basée sur Nitro, pour lesquels la moyenne représente la moyenne sur la période spécifiée. • La statistique `SampleCount` indique le nombre total d'opérations d'écriture durant la période, sauf pour les volumes attachés à une instance basée sur Nitro, pour lesquels le nombre	Octets	`VolumeId`	• `Average` • `Sum` • `SampleCount` • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances basées sur Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
	d'échantillons représente le nombre de points de données utilisés pour le calcul statistique. **Note** Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité d'écriture se produit sur le volume.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeReadOps`	Nombre total d'opérations de lecture au cours d'une période donnée. Les opérations de lecture sont comptabilisées une fois terminées. Pour calculer la moyenne des opérations de lecture par seconde (lectureIOPS) pour la période, divisez le nombre total d'opérations de lecture de la période par le nombre de secondes de cette période.	Nombre	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances basées sur Nitro
`VolumeWriteOps`	Nombre total d'opérations d'écriture au cours d'une période donnée. Les opérations d'écriture sont comptabilisées une fois terminées. Pour calculer la moyenne des opérations d'écriture par seconde (écritureIOPS) pour la période, divisez le nombre total d'opérations d'écriture pendant la période par le nombre de secondes pendant cette période.	Nombre	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances basées sur Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeTotalReadTime`	**Note** Non pris en charge avec les volumes activés pour l'attachement multiple. Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité de lecture se produit sur le volume. Nombre total de secondes passées par toutes les opérations de lecture terminées, au cours d'une période donnée. Si plusieurs demandes sont soumises en même temps, ce total peut être supérieur à la durée de la période. Par exemple, pour une période de 1 minute (60 secondes) : si	Secondes	`VolumeId`	• `Average` : non pertinent pour les volumes attachés à des instances basées sur Nitro • `Sum` • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances basées sur Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
	150 opérations ont été réalisées au cours de cette période et que chaque opération a pris une seconde, la valeur serait 150 secondes.			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeTotalWriteTime`	**Note** Non pris en charge avec les volumes activés pour l'attachement multiple. Pour les instances Xen, les données sont présentées uniquement lorsqu'une activité d'écriture se produit sur le volume. Nombre total de secondes passées par toutes les opérations d'écriture terminées, au cours d'une période donnée. Si plusieurs demandes sont soumises en même temps, ce total peut être supérieur à la durée de la période. Par exemple, pour une période de 1 minute (60 secondes) : si	Secondes	`VolumeId`	• `Average` : non pertinent pour les volumes attachés à des instances basées sur Nitro • `Sum` • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances basées sur Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
	150 opérations ont été réalisées au cours de cette période et que chaque opération a pris une seconde, la valeur serait 150 secondes.			
`VolumeIdleTime`	**Note** Non pris en charge avec les volumes activés pour l'attachement multiple. Nombre total de secondes dans une période données, alors qu'aucune opération de lecture ou écriture n'a été soumise.	Secondes	`VolumeId`	• `Average` : non pertinent pour les volumes attachés à des instances basées sur Nitro • `Sum` • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances basées sur Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeQueueLength`	Nombre de demandes d'opérations de lecture et d'écriture en attente de réalisation au cours d'une période donnée.	Nombre	`VolumeId`	• `Average` • `Sum` : non pertinent pour les volumes attachés à des instances Nitro • `Minimum` | `Maximum` : uniquement pour les volumes attachés à des instances Nitro

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeStalledIOCheck`	**Note** Pour les instances Nitro uniquement. Non publié pour les volumes attachés à Amazon ECS et AWS Fargate les tâches. Indique si un volume a réussi ou échoué à une vérification d'E/S bloquée au cours de la dernière minute. Cette métrique peut être (réussie) ou `0` 1 (échouée). Pour de plus amples informations, veuillez consulter Surveillez les caractéristiques des E/S à l'aide de CloudWatch.	Aucun	`VolumeId` | `InstanceId`	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeThroughputPercentage`	**Note** IOPSSSDVolumes provisionnés uniquement. Non pris en charge avec les volumes activés pour l'attachement multiple. Pourcentage d'opérations d'E/S par seconde (IOPS) livrées par rapport au total IOPS provisionné pour un volume AmazonEBS. IOPSSSDLes volumes provisionnés fournissent leurs performances provisionnées 99,9 % du temps. Pendant une écriture, s'il n'y a aucune autre requête d'I/O en suspens en une minute, la valeur de la métrique est 100 %. En outre, les performances d'E/S d'un volume peuvent être temporair	Pourcentage	`VolumeId`	• `Average` • `Minimum` | `Maximum`

Métrique	Description	Unités	Dimensions	Statistiques significatives
	ement dégradées en raison d'une action que vous avez entreprise (par exemple, créer un instantané d'un volume en période de pointe, exécuter le volume sur une non-EBS-optimized instance ou accéder aux données du volume pour la première fois).			

Métrique	Description	Unités	Dimensions	Statistiques significatives
`VolumeConsumedReadWriteOps`	**Note** IOPSSSDVolumes provisionnés uniquement. Nombre total d'opérations de lecture et d'écriture (normalisé selon les unités de capacité 256 K) utilisées au cours d'une période donnée. Les opérations d'E/S inférieures à 256 Ko sont chacune considérées comme une opération consommée. IOPS Les opérations d'I/O supérieures à 256 K sont comptées dans les unités de capacité de 256 K. Par exemple, 1 024 000 E/S compterait pour 4 consommées. IOPS	Nombre	`VolumeId`	• `Average` • `Sum` • `Minimum` | `Maximum`

Métrique	Description	Unités	Dimensions	Statistiques significatives
`BurstBalance`	**Note** `gp2` `st1`, et `sc1` volumes uniquement. Fournit des informations concernant le pourcentage de crédits d'I/O (pour `gp2`) ou de crédits de débit (pour `st1` et `sc1`) restant dans le compartiment en rafales. Les données ne sont signalées CloudWatch que lorsque le volume est actif. Si le volume n'est pas attaché, aucune donnée n'est présentée. Si les performances de base du volume dépassent les performances en rafale maximales, les crédits ne sont jamais dépensés. Si le volume est attaché à une instance construite sur le Système Nitro, l'équilibre en rafale n'est pas signalé. Dans d'autres	Pourcentage	`VolumeId`	• `Average` • `Sum` : non pertinent pour les volumes attachés à des instances Nitro. • `Minimum` | `Maximum`

Métrique	Description	Unités	Dimensions	Statistiques significatives
	cas, l'équilibre en rafale déclaré est de 100 %. Pour de plus amples informations, veuillez consulter Performances du volume gp2.			

Métriques pour les EBS instantanés Amazon

L'espace de `AWS/EBS` noms inclut les métriques suivantes pour les EBS instantanés Amazon.

Métrique	Description	Unités	Dimensions	Statistiques significatives
`SnapshotCopyBytesTransferred`	La quantité de données de capture d'écran copiées AWS dans une région.	Octets	`sourceRegion`	`Sum`

Métriques d'instances Nitro

L'espace de `AWS/EC2` noms inclut des EBS métriques Amazon supplémentaires pour les volumes attachés à des instances basées sur Nitro qui ne sont pas des instances bare metal.

Métrique	Description	Unité	Statistiques significatives
`EBSReadOps`	Opérations de lecture terminées à partir de tous les EBS volumes Amazon attachés à	Nombre	• Somme

Métrique	Description	Unité	Statistiques significatives
	l'instance dans un délai spécifié. Pour calculer la moyenne des opérations d'E/S de lecture par seconde (lectureIOPS) pour la période, divisez le total des opérations de la période par le nombre de secondes de cette période. Si vous utilisez une surveillance de base (5 minutes), vous pouvez diviser ce nombre par 300 pour calculer le ReadIOPS. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les opérations par seconde. Par exemple, si vous avez représenté graphique ment `EBSReadOps` CloudWatch commem1, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en opérations/seconde. Pour plus d'informa tions sur les autres fonctions mathémati ques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisa teur Amazon.		• Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`EBSWriteOps`	Opérations d'écriture terminées sur tous les EBS volumes attachés à l'instance au cours d'une période spécifiée. Pour calculer la moyenne des opérations d'E/S d'écriture par seconde (écritureIOPS) pour la période, divisez le total des opérations de la période par le nombre de secondes de cette période. Si vous utilisez une surveillance de base (5 minutes), vous pouvez diviser ce nombre par 300 pour calculer le WriteIOPS. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les opérations par seconde. Par exemple, si vous avez représenté graphique ment `EBSWriteOps` CloudWatch comm`em1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en opérations/seconde. Pour plus d'informa tions sur les autres fonctions mathémati ques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisa teur Amazon.	Nombre	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`EBSReadBytes`	Octets lus à partir de tous les EBS volumes attachés à l'instance au cours d'une période spécifiée. Le nombre mentionné correspond au nombre d'octets lus pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde en lecture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement `EBSReadBytes` CloudWatch comme `m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`EBSWriteBytes`	Octets écrits sur tous les EBS volumes attachés à l'instance au cours d'une période spécifiée. Le nombre mentionné correspond au nombre d'octets écrits pendant la période. Si vous utilisez une surveillance de base (cinq minutes), vous pouvez diviser ce nombre par 300 pour trouver le nombre d'octets/seconde en écriture. Si vous avez recours à une surveillance détaillée (une minute), divisez-le par 60. Vous pouvez également utiliser la fonction mathématique CloudWatch métrique `DIFF_TIME` pour déterminer les octets par seconde. Par exemple, si vous avez représenté graphiquement `EBSWriteBytes` CloudWatch comme`m1`, la formule mathématique de la métrique `m1/(DIFF_TIME(m1))` renvoie la métrique en octets/seconde. Pour plus d'informations sur les autres fonctions mathématiques métriques `DIFF_TIME` et sur d'autres, consultez la section Utiliser les mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.	Octets	• Somme • Moyenne • Minimum • Maximum

Métrique	Description	Unité	Statistiques significatives
`EBSIOBalance%`	Fournit des informations sur le pourcentage de crédits d'I/O restant dans le compartiment en rafales. Cette métrique est disponible uniquement pour la surveillance basique. Cette métrique n'est disponible que pour certaines tailles d'instance `*.4xlarge` et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures. Pour plus d'informations, voir EBSOptimisé par défaut. La statistique `Sum` n'est pas applicable pour cette métrique.	Pourcentage	• Minimum • Maximum
`EBSByteBalance%`	Fournit des informations sur le pourcentage de crédits de débit restant dans le compartiment en rafales. Cette métrique est disponible uniquement pour la surveillance basique. Cette métrique n'est disponible que pour certaines tailles d'instance `*.4xlarge` et plus petites qui atteignent leur performance maximale pendant 30 minutes au moins une fois par 24 heures. Pour plus d'informations, voir EBSOptimisé par défaut. La statistique `Sum` n'est pas applicable pour cette métrique.	Pourcentage	• Minimum • Maximum

Métriques de restauration d'instantané rapide

L'espace de noms `AWS/EBS` inclut les métriques suivantes pour une restauration d'instantané rapide.

Métrique	Description	Unités	Dimensions	Statistiques significatives
`FastSnapshotRestoreCreditsBucketSize`	Nombre maximum de crédits de création de volume pouvant être accumulés. Cette métrique est signalée par instantané et par zone de disponibilité.	Aucun	`SnapshotId` | `AvailabilityZone`	• `Average` • `Minimum` | `Maximum` **Note** La statistique la plus significative est `Average`. Les résultats des statistiques `Minimum` et `Maximum` sont les mêmes que ceux de `Average` et peuvent être utilisés indifféremment.
`FastSnapshotRestoreCreditsBalance`	Nombre de crédits de création de volume disponibles. Cette métrique est signalée par instantané et par zone de disponibilité.	Aucun	`SnapshotId` | `AvailabilityZone`	• `Average` • `Minimum` | `Maximum` **Note** La statistique la plus significative est `Average`. Les résultats des statistiques `Minimum` et `Maximum` sont les mêmes que ceux de `Average`

Métrique	Description	Unités	Dimensions	Statistiques significatives
				et peuvent être utilisés indifféremment.

Graphiques de EC2 la console Amazon

Après avoir créé un volume, vous pouvez consulter les graphiques de surveillance du volume dans la EC2 console Amazon. Sélectionnez un volume dans la page Volumes de la console, puis sélectionnez Surveillance. Le tableau ci-après répertorie les graphiques affichés. La colonne de droite décrit comment les métriques de données brutes du CloudWatch API sont utilisées pour produire chaque graphique. La période de tous les graphiques est de 5 minutes.

Graphique	Description de l'utilisation des métriques brutes
Débit de lecture (Kio/s)	`Sum(VolumeReadBytes) / Period / 1024`
Débit d'écriture (Kio/s)	`Sum(VolumeWriteBytes) / Period / 1024`
Opérations de lecture (Ops/s)	`Sum(VolumeReadOps) / Period`
Opérations d'écriture (Ops/s)	`Sum(VolumeWriteOps) / Period`
Longueur moyenne de la file d'attente (Opérations)	`Avg(VolumeQueueLength)`
Temps inactif (%)	`Sum(VolumeIdleTime) / Period × 100`

Taille de lecture moyenne (Kio/op)	`Avg(VolumeReadBytes) / 1024`
	
	Pour les instances basées sur Nitro, la formule suivante calcule la taille de lecture moyenne à l'aide des mathématiques CloudWatch métriques :
	
	`(Sum(VolumeReadBytes) / Sum(VolumeReadOps)) / 1024`

Graphique	Description de l'utilisation des métriques brutes
	Les `VolumeReadOps` métriques `VolumeReadBytes` et sont disponibles dans la EBS CloudWatch console.

Taille d'écriture moyenne (Kio/op)	`Avg(VolumeWriteBytes) / 1024`
	
	Pour les instances basées sur Nitro, la formule suivante calcule la taille d'écriture moyenne à l'aide des mathématiques CloudWatch métriques :
	
	`(Sum(VolumeWriteBytes) / Sum(VolumeWriteOps)) / 1024`
	
	Les `VolumeWriteOps` métriques `VolumeWriteBytes` et sont disponibles dans la EBS CloudWatch console.

Latence de lecture moyenne (ms/op)	`Avg(VolumeTotalReadTime) × 1000`
	
	Pour les instances basées sur Nitro, la formule suivante calcule la latence de lecture moyenne à l'aide de CloudWatchMetric Math :
	
	`(Sum(VolumeTotalReadTime) / Sum(VolumeReadOps)) × 1000`
	
	Les `VolumeReadOps` métriques `VolumeTotalReadTime` et sont disponibles dans la EBS CloudWatch console.

Graphique	Description de l'utilisation des métriques brutes

Latence d'écriture moyenne (ms/op)	`Avg(VolumeTotalWriteTime) × 1000`
	
	Pour les instances basées sur Nitro, la formule suivante calcule la latence d'écriture moyenne à l'aide des mathématiques CloudWatch métriques :
	
	`(Sum(VolumeTotalWriteTime) / Sum(VolumeWriteOps)) * 1000`
	
	Les `VolumeWriteOps` métriques `VolumeTotalWriteTime` et sont disponibles dans la EBS CloudWatch console.

Pour les graphiques de latence moyenne et ceux de taille moyenne, la moyenne est calculée par rapport au nombre total d'opérations (lecture ou écriture, quel que soit celui applicable au graphe) complétées durant la période.

EventBridge Événements Amazon pour Amazon EBS

Amazon EBS envoie des événements à Amazon EventBridge pour les actions effectuées sur les volumes et les instantanés. Avec EventBridge, vous pouvez établir des règles qui déclenchent des actions programmatiques en réponse à ces événements. Par exemple, vous pouvez créer une règle qui envoie une notification sur votre adresse électronique lorsqu'un instantané est activé pour une restauration rapide des instantanés.

Les événements de EventBridge sont représentés sous forme JSON d'objets. Les champs propres à l'événement sont contenus dans la section « détail » de l'JSONobjet. Le champ « événement » contient le nom de l'événement. Le champ « résultat » contient l'état terminé de l'action qui déclenche l'événement. Pour plus d'informations, consultez les modèles EventBridge d'événements Amazon dans le guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations, consultez Qu'est-ce qu'Amazon EventBridge ? dans le guide de EventBridge l'utilisateur Amazon.

Événements

- EBSévénements liés au volume

- EBSévénements de modification du volume
- EBSévénements instantanés
- EBSÉvénements d'archivage des instantanés
- EBSévénements de restauration rapide des instantanés
- Utilisation AWS Lambda pour gérer les EventBridge événements

EBSévénements liés au volume

Amazon EBS envoie des événements EventBridge lorsque les événements de volume suivants se produisent.

Événements

- Créer un volume (createVolume)
- Supprimer le volume (deleteVolume)
- Attacher ou reconnecter un volume (attachVolume,reattachVolume)
- Détacher le volume () detachVolume

Créer un volume (createVolume)

L'`createVolume`événement est envoyé à votre AWS compte lorsqu'une action de création de volume est terminée. Cependant, il n'est ni enregistré, ni enregistré, ni archivé. Cet événement peut avoir le résultat `available` ou `failed`. La création échouera si une valeur non valide AWS KMS key a été fournie, comme indiqué dans les exemples ci-dessous.

Données d'événement

La liste ci-dessous est un exemple d'JSONobjet émis par EBS pour un `createVolume` événement réussi.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
```

```
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "available",
      "cause": "",
      "event": "createVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

La liste ci-dessous est un exemple d'JSONobjet émis par EBS après un échec d'un `createVolume` événement. La cause de l'échec était une KMS clé désactivée.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

Voici un exemple d'JSONobjet émis par EBS après un échec d'un `createVolume` événement. La cause de l'échec était une KMS clé en attente d'importation.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
```

```
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

Supprimer le volume (deleteVolume)

L'`deleteVolume`événement est envoyé à votre AWS compte lorsqu'une action de suppression d'un volume est terminée. Cependant, il n'est ni enregistré, ni enregistré, ni archivé. Le résultat de cet événement est `deleted`. Si la suppression ne se termine pas, l'événement n'est pas envoyé.

Données d'événement

La liste ci-dessous est un exemple d'JSONobjet émis par EBS pour un `deleteVolume` événement réussi.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "deleted",
      "cause": "",
      "event": "deleteVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
```

```
}
```

Attacher ou reconnecter un volume (attachVolume,reattachVolume)

L'événement `attachVolume` ou `reattachVolume` est envoyé à votre compte AWS si un volume ne parvient pas à s'attacher ou à se rattacher à une instance. Cependant, il n'est ni enregistré, ni enregistré, ni archivé. Si vous utilisez une KMS clé pour chiffrer un EBS volume et que la KMS clé n'est plus valide, un événement EBS sera émis si cette KMS clé est ensuite utilisée pour attacher ou reconnecter une instance, comme indiqué dans les exemples ci-dessous.

Données d'événement

La liste ci-dessous est un exemple d'JSONobjet émis par EBS après un échec d'un `attachVolume` événement. La cause de l'échec était une KMS clé en attente de suppression.

> **Note**
>
> AWS peut tenter de se reconnecter à un volume après une maintenance de routine du serveur.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

La liste ci-dessous est un exemple d'JSONobjet émis par EBS après un échec d'un `reattachVolume` événement. La cause de l'échec était une KMS clé en attente de suppression.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

Détacher le volume () detachVolume

L'`detachVolume`événement est envoyé à votre AWS compte lorsqu'un volume est détaché d'une EC2 instance Amazon.

Données d'événement

Voici un exemple d'`detachVolume`événement réussi.

```
{
  "version":"0",
  "id":"2ec37298-1234-e436-70fc-c96b1example",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.ec2",
  "account":"123456789012",
  "time":"2024-03-18T16:35:52Z",
  "region":"us-east-1",
  "resources":[],
  "detail":
```

```
  {
    "eventVersion":"1.09",
    "userIdentity":
    {
      "type":"IAMUser",
      "principalId":"AIDAJT12345SQ2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/administrator",
      "accountId":"123456789012",
      "accessKeyId":"AKIAJ67890A6EXAMPLE",
      "userName":"administrator"
    },
    "eventTime":"2024-03-18T16:35:52Z",
    "eventSource":"ec2.amazonaws.com",
    "eventName":"DetachVolume",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"12.12.123.12",
    "userAgent":"aws-cli/2.7.12 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
ec2.detach-volume",
    "requestParameters":
    {
      "volumeId":"vol-072577c46bexample",
      "force":false
    },
    "responseElements":
    {
      "requestId":"1234513a-6292-49ea-83f8-85e95example",
      "volumeId":"vol-072577c46bexample",
      "instanceId":"i-0217f7eb3dexample",
      "device":"/dev/sdb",
      "status":"detaching",
      "attachTime":1710776815000
    },
    "requestID":"1234513a-6292-49ea-83f8-85e95example",
    "eventID":"1234551d-a15a-43eb-9e69-c983aexample",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "managementEvent":true,
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":
    {
      "tlsVersion":"TLSv1.3",
      "cipherSuite":"TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader":"ec2.us-east-1.amazonaws.com"
```

```
    }
  }
}
```

EBSévénements de modification du volume

Amazon EBS envoie `modifyVolume` des événements EventBridge lorsqu'un volume est modifié. Cependant, il n'est ni enregistré, ni enregistré, ni archivé.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

EBSévénements instantanés

Amazon EBS envoie des événements EventBridge lorsque les événements de volume suivants se produisent.

Événements

- Créer un instantané (createSnapshot)
- Créer des instantanés () createSnapshots
- Copier un instantané (copySnapshot)
- Partager un instantané (shareSnapshot)

Créer un instantané (createSnapshot)

L'`createSnapshot`événement est envoyé à votre AWS compte lorsqu'une action visant à créer un instantané est terminée. Cependant, il n'est ni enregistré, ni enregistré, ni archivé. Cet événement peut avoir le résultat `succeeded` ou `failed`.

Données d'événement

La liste ci-dessous est un exemple d'JSONobjet émis par EBS pour un `createSnapshot` événement réussi. Dans la `detail` section, le `source` champ contient ARN le volume source. Les champs `startTime` et `endTime` indiquent le moment où la création de l'instantané a commencé et est terminée.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
     "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"  }
}
```

Créer des instantanés () createSnapshots

L'`createSnapshots`événement est envoyé à votre AWS compte lorsqu'une action visant à créer un instantané en plusieurs volumes est terminée. Cet événement peut avoir le résultat `succeeded` ou `failed`.

Données d'événement

La liste ci-dessous est un exemple d'JSONobjet émis par EBS pour un `createSnapshots` événement réussi. Dans la `detail` section, le `source` champ contient les volumes sources ARNs de l'ensemble de clichés multi-volumes. Les champs `startTime` et `endTime` indiquent le moment où la création de l'instantané a commencé et est terminée.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "completed"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "completed"
      }
    ]
  }
}
```

La liste ci-dessous est un exemple d'JSONobjet émis par EBS après un échec d'un `createSnapshots` événement. La cause de l'échec correspondait à un ou plusieurs instantanés de l'ensemble d'instantanés multi-volumes qui n'ont pas pu aboutir. Les valeurs de `snapshot_id` sont

celles ARNs des instantanés ayant échoué. `startTime`et indiquent `endTime` le début et la fin de l'action de création d'instantanés.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
"detail": {
    "event": "createSnapshots",
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
   "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "error"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "error"
      }
    ]
  }
}
```

Copier un instantané (copySnapshot)

L'`copySnapshot`événement est envoyé à votre AWS compte lorsqu'une action de copie d'un instantané est terminée. Cependant, il n'est ni enregistré, ni enregistré, ni archivé. Cet événement peut avoir le résultat `succeeded` ou `failed`.

Dans la `detail` section, `source` il s'agit ARN de l'instantané source et `snapshot_id` ARN de la copie de l'instantané. `startTime`et `endTime` indiquez le début et la fin de l'opération de copie. `incremental`indique si la copie d'instantané est un instantané incrémentiel (`true`) ou un instantané complet (`false`). `transferType`indique si l'opération de copie instantanée était une opération de copie standard ou une opération de copie basée sur le temps. Pour de plus amples informations, veuillez consulter Copies temporelles pour les instantanés Amazon EBS.

Si vous copiez l'instantané d'une région à l'autre, l'événement est émis dans la région de destination.

Scénario 1 : Fin de l'opération de copie instantanée standard

Voici un exemple d'événement envoyé à votre compte lorsqu'une opération de copie instantanée standard se termine avec succès. Notez que `transferType` est `standard`.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "incremental": "true",
    "transferType": "standard"
  }
}
```

Scénario 2 : L'opération de copie instantanée basée sur le temps s'achève pendant la durée d'achèvement

Voici un exemple d'événement envoyé à votre compte lorsqu'une opération de copie instantanée basée sur le temps s'achève dans les délais impartis. Notez que cela `transferType` indique qu'il s'agissait d'une opération de copie instantanée basée sur le temps. `time-based` `completionDurationStartTime`indique à quel moment la durée d'achèvement a commencé.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime":"2024-11-16T06:27:33.816Z",
    "transferType": "time-based"
  }
}
```

Scénario 3 : L'opération de copie instantanée basée sur le temps se termine mais n'atteint pas la durée d'achèvement demandée

Lorsqu'une opération de copie instantanée basée sur le temps se termine, mais n'atteint pas la durée d'achèvement demandée, deux CloudWatch événements sont envoyés à votre compte. Voici des exemples de ces événements.

- Le premier événement est envoyé sur votre compte dès que le délai d'exécution est dépassé, même si l'opération de copie est toujours en cours. Cet événement existe et `EBS Copy`

`Snapshot Missed Completion Duration` en `missedCompletionDurationCause` fournit la raison. `detail-type`

```
{
 "version":"0",
 "id":"fd90eb95-0938-e02c-cf55-b81363b8ac12",
 "detail-type":"EBS Copy Snapshot Missed Completion Duration",
 "source":"aws.ec2",
 "account":"123456789012",
 "time":"2024-11-19T18:17:08Z",
 "region":"us-east-1",
 "resources": ["arn:aws:ec2:us-east-1:123456789012:snapshot/snap-01234567890abcedf"],
 "detail":{
   "event":"copySnapshot",
   "missedCompletionDurationCause":"Snapshot copy was not able to meet the specified
 completion duration because your snapshot copy operation throughput quota was
 exceeded.",
   "snapshot_id":"arn:aws:ec2:us-
east-1:123456789012:snapshot/snap-01234567890abcedf",
   "source":"arn:aws:ec2:us-east-1:123456789012:snapshot/snap-00987654321fedcba",
   "startTime": "Sun Nov 24 22:32:55 UTC 2024",
   "transferType": "time-based"
   }
}
```

- Le deuxième événement n'est envoyé à votre compte qu'une fois l'instantané terminé. L'événement inclut`missedCompletionDurationCause`, ce qui en fournit la raison.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
```

```
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime":"2024-11-16T06:27:33.816Z",
    "missedCompletionDurationCause":"Snapshot copy was not able to meet the specified
 completion duration because your snapshot copy operation throughput quota was
 exceeded.",
    "transferType": "time-based"
  }
}
```

Scénario 4 : échec de l'opération de copie instantanée

Voici un exemple d'événement envoyé à votre compte en cas d'échec d'une opération de copie instantanée. Notez que `result` cela `failed` indique que l'opération a échoué.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

Partager un instantané (shareSnapshot)

L'`shareSnapshot`événement est envoyé à votre AWS compte lorsqu'un autre compte partage un instantané avec celui-ci. Cependant, il n'est ni enregistré, ni enregistré, ni archivé. Le résultat est toujours `succeeded`.

Données d'événement

Voici un exemple d'JSONobjet émis par EBS après la fin d'un `shareSnapshot` événement. Dans la `detail` section, la valeur de `source` est le numéro de AWS compte de l'utilisateur qui a partagé l'instantané avec vous. `startTime`et indiquent `endTime` le début et la fin de l'action de partage d'instantanés. L'événement `shareSnapshot` est émis uniquement lorsqu'un instantané privé est partagé avec un autre utilisateur. Le partage d'un instantané public ne déclenche pas l'événement.

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": 012345678901,
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

EBSÉvénements d'archivage des instantanés

Amazon EBS émet des événements liés aux actions d'archivage des instantanés. Pour de plus amples informations, veuillez consulter Surveillez l'archivage des instantanés Amazon EBS à l'aide d'Events CloudWatch .

EBSévénements de restauration rapide des instantanés

Amazon EBS envoie des événements EventBridge lorsque l'état de restauration rapide d'un instantané change. Les événements sont générés dans la mesure du possible.

Voici un exemple de données pour cet événement.

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Fast Snapshot Restore State-change Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
   ],
   "detail": {
      "snapshot-id": "snap-1234567890abcdef0",
      "state": "optimizing",
      "zone": "us-east-1a",
      "message": "Client.UserInitiated - Lifecycle state transition",
   }
}
```

Les valeurs possibles pour `state` sont `enabling`, `optimizing`, `enabled`, `disabling` et `disabled`.

Les valeurs possibles pour `message` sont les suivantes :

`Client.InvalidSnapshot.InvalidState - The requested snapshot transitioned to an invalid state (Error)`

Une demande d'activation de la fonction de restauration d'instantané rapide a échoué et l'état est passé à `disabling` ou `disabled`. La fonction de restauration d'instantané rapide ne peut pas être activée pour cet instantané.

`Client.UserInitiated`

L'état est passé avec succès à `enabling` ou `disabling`.

`Client.UserInitiated - Lifecycle state transition`

L'état est passé avec succès à `optimizing`, `enabled` ou `disabled`.

`Server.InsufficientCapacity - There was insufficient capacity available to satisfy the request`

Une demande d'activation de la fonction de restauration d'instantané rapide a échoué en raison d'une capacité insuffisante et l'état est passé à `disabling` ou `disabled`. Attendez, puis recommencez.

`Server.InternalError - An internal error caused the operation to fail`

Une demande d'activation de la fonction de restauration d'instantané rapide a échoué en raison d'une erreur interne et l'état est passé à `disabling` ou `disabled`. Attendez, puis recommencez.

`Client.InvalidSnapshot.InvalidState - The requested snapshot was deleted or access permissions were revoked`

L'état de restauration d'instantané rapide est passé à `disabling` ou `disabled` parce que l'instantané a été supprimé ou non partagé par son propriétaire. La restauration d'instantané rapide ne peut pas être activée pour un instantané qui a été supprimé ou qui n'est plus partagé avec vous.

Utilisation AWS Lambda pour gérer les EventBridge événements

Vous pouvez utiliser Amazon EBS et Amazon EventBridge pour automatiser votre flux de sauvegarde des données. Cela vous oblige à créer une IAM politique, une AWS Lambda fonction pour gérer l'événement et une EventBridge règle qui fait correspondre les événements entrants et les achemine vers la fonction Lambda.

La procédure suivante utilise l'événement `createSnapshot` pour copier automatiquement un instantané terminé vers une autre région pour la reprise après sinistre.

Pour copier un instantané terminé vers une autre région

1. Créez une IAM politique, telle que celle illustrée dans l'exemple suivant, pour autoriser l'utilisation de l'`CopySnapshot`action et l'écriture dans le EventBridge journal. Assignez la politique à l'utilisateur qui gérera l' EventBridge événement.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

2. Définissez une fonction dans Lambda qui sera disponible depuis la EventBridge console. L'exemple de fonction Lambda ci-dessous, écrit dans le fichier Node.js, est invoqué EventBridge lorsqu'un `createSnapshot` événement correspondant est émis par Amazon EBS (ce qui signifie qu'un instantané est terminé). Lorsqu'elle est appelée, la fonction copie l'instantané de `us-east-2` vers `us-east-1`.

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
```

```
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
 initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
 ${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
        } else {
            const successMessage = `Successfully started copy of snapshot
 ${snapshotId} to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
};
```

Pour vous assurer que votre fonction Lambda est disponible depuis la EventBridge console, créez-la dans la région où l' EventBridge événement se produira. Pour plus d'informations, consultez le Guide du développeur AWS Lambda.

3. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
4. Dans le volet de navigation, sélectionnez Rules (Règles), puis Create rule (Créer une règle).
5. Pour Step 1: Define rule detail (Étape 1 : Définir les détails de la règle), procédez comme suit :

    a. Saisissez un Name (Nom) et une Description pour la règle.

b. Pour Event bus (Bus d'événements), gardez default (par défaut).

c. Vérifiez que l'option Enable the rule on the selected event bus (Activer la règle sur le bus d'événements sélectionné) est activée.

d. Pour Event type (Type d'événement), choisissez Rule with an event pattern (Règle avec un modèle d'événement).

e. Choisissez Suivant.

6. Pour Step 2: Build event pattern (Étape 2 : Créer un modèle d'événement), procédez comme suit :

   a. Dans Source de l'événement, sélectionnez AWS des événements ou des événements EventBridge partenaires.

   b. Dans la section Modèle d'événement, pour Source d'événement, assurez-vous que le AWS service est sélectionné, et pour le AWS service, sélectionnez EC2.

   c. Pour Type d'événement, sélectionnez Notification EBS instantanée, sélectionnez Événement (s) spécifique (s), puis choisissez createSnapshot.

   d. Sélectionnez Specific result(s) (Résultat(s) spécifique(s)), puis choisissez succeeded.

   e. Choisissez Suivant.

7. Pour Step 3: Select targets (Étape 3 : Sélectionner les cibles), procédez comme suit :

   a. Pour Types de cibles, choisissez service AWS .

   b. Pour Select target (Sélectionner la cible), choisissez Lambda function (Fonction Lambda), et pour Fonction, sélectionnez la fonction que vous avez créée précédemment.

   c. Choisissez Next (Suivant)

8. Pour Step 4: Configure tags (Étape 4 : Configurer les balises), spécifiez des balises pour la règle si nécessaire, puis choisissez Next (Suivant).

9. Pour Step 5: Review and create (Étape 5 : Examen et création), passez en revue la règle, puis choisissez Create rule (Créer une règle).

Votre règle doit désormais apparaître sur l'onglet Rules. Dans l'exemple illustré, l'événement que vous avez configuré devrait être émis lors de EBS la prochaine copie d'un instantané.

Statistiques de performance EBS détaillées d'Amazon

Les appareils Amazon EBS NVMe Block vendent des statistiques de performance d'E/S haute résolution en temps réel pour les EBS volumes Amazon attachés à des instances Amazon EC2 basées sur Nitro. Ces statistiques sont présentées sous forme de compteurs agrégés qui sont conservés pendant toute la durée de l'attachement du volume à l'instance. Les statistiques fournissent des détails sur le nombre cumulé d'opérations, les octets envoyés et reçus, ainsi que le temps consacré aux opérations d'E/S en lecture et en écriture. En outre, les statistiques incluent des histogrammes pour les opérations d'E/S en lecture et en écriture, ainsi que le temps total pendant lequel votre application a dépassé les limites provisionnées IOPS ou de débit du EBS volume ou de l'instance attachée.

Vous pouvez collecter ces statistiques avec une granularité allant jusqu'à 1 seconde d'intervalle.

Considérations

- Les statistiques sont prises en charge pour tous les types de EBS volumes Amazon.
- Les statistiques ne sont prises en charge que pour les volumes attachés à des instances créées sur le système AWS Nitro.
- Les statistiques sont disponibles pour les volumes compatibles avec l'option Multi-Attach. Lorsque vous consultez les statistiques d'un volume activé pour l'attachement multiple, les statistiques sont spécifiques à cette instance attachée et reflètent uniquement l'utilisation de cette instance.
- Les statistiques sont disponibles sans frais supplémentaires.
- EBSles statistiques de performances détaillées ne sont pas prises en charge pour les instances G6, G6e, Gr6, P4, P5 et P5e.

Statistiques

L'appareil Amazon EBS NVMe Block fournit les statistiques suivantes :

Nom de la statistique	Nom complet	Type	Description
total_read_ops	Nombre total d'opérations de lecture	Compteur	Nombre total d'opérations de lecture terminées.
total_write_ops	Nombre total d'opérations d'écriture	Compteur	Nombre total d'opérations d'écriture terminées.
total_read_bytes	Nombre total d'octets lus	Compteur	Nombre total d'octets lus transférés.
total_write_bytes	Nombre total d'octets d'écriture	Compteur	Nombre total d'octets d'écriture transférés.
total_read_time	Temps de lecture total	Compteur	Temps total passé, en microsecondes, par toutes les opérations de lecture terminées.
total_write_time	Temps d'écriture total	Compteur	Temps total passé, en microsecondes, par toutes les opérations d'écriture terminées.
ebs_volume_performance_exceeded_iops	Durée totale pendant laquelle la demande a dépassé le volume provisionné IOPS	Compteur	Durée totale, en microsecondes, pendant laquelle IOPS la demande a dépassé les performances provisionnées IOPS du volume.
ebs_volume_performance_exceeded_tp	Durée totale pendant laquelle la demande a dépassé le volume fourni, débit	Compteur	Durée totale, en microsecondes, pendant laquelle la demande de débit a dépassé les performances de débit provisionnées du volume.
ec2_instance_ebs_performanc	Durée totale pendant laquelle la demande a dépassé les IOPS	Compteur	Durée totale, en microsecondes, pendant laquelle le EBS volume a dépassé les IOPS performances maximales de l'EC2instance Amazon attachée.

Nom de la statistique	Nom complet	Type	Description
e_exceed d_iops	performances de l'EC2instance		
ec2_insta nce_ebs_p erformanc e_exceed d_tp	Durée totale pendant laquelle la demande a dépassé les EC2 performances de débit de l'instance	Compteur	Durée totale, en microsecondes, pendant laquelle le EBS volume a dépassé les performances de débit maximales de l'EC2instance Amazon attachée.
volume_qu eue_lengt h	Longueur de file d'attente de volumes	Point dans le temps	Nombre d'opérations de lecture et d'écriture en attente d'achèvement.
read_io_l atency_hi stogram	Lire l'histogramme d'E/S	Histogramme *	Nombre d'opérations de lecture effectuées dans chaque case de latence, en microsecondes.
write_io_ latency_h istogram	Écrire un histogramme d'E/S	Histogramme *	Nombre d'opérations d'écriture effectuées dans chaque case de latence, en microsecondes.

> **Note**
>
> * Les statistiques de l'histogramme ne représentent que les opérations d'E/S qui se sont terminées avec succès. Les opérations d'E/S bloquées ou altérées ne sont pas incluses, mais elles apparaîtront clairement dans les `volume_queue_length` statistiques, qui sont présentées sous forme de statistiques. point-in-time

Accès aux statistiques

Les statistiques doivent être accessibles directement depuis l'instance à laquelle le EBS volume Amazon est attaché. Vous pouvez accéder aux statistiques en utilisant l'une des méthodes suivantes.

ebsnvme script

Le `ebsnvme` script se trouve dans le dépôt Github amazon-ec2-utils.

Pour accéder aux statistiques

1. Connectez-vous à l'instance à laquelle le volume est attaché.
2. Téléchargez le `ebsnvme` script depuis le dépôt `amazon-ec2-utils` Github.

```
wget https://raw.githubusercontent.com/amazonlinux/amazon-ec2-utils/refs/heads/main/ebsnvme
```

3. Modifiez les autorisations du script pour le rendre exécutable.

```
sudo chmod +x ./ebsnvme
```

4. Exécutez le `ebsnvme` script et spécifiez le nom du périphérique pour le volume.

```
sudo ./ebsnvme stats /dev/nvme0n1
```

nvme-cli tool (Amazon Linux only)

Pour accéder aux statistiques

1. Connectez-vous à l'instance à laquelle le volume est attaché.
2. Amazon Linux AMIs publié après le 12 novembre 2024 inclut la dernière version de l'`nvme-cli`outil. Si vous utilisez un ancien Amazon LinuxAMI, mettez à jour l'`nvme-cli`outil.

```
sudo yum install nvme-cli
```

3. Exécutez la commande suivante et spécifiez le nom du périphérique pour le volume.

```
nvme amzn stats /dev/nvme0n1
```

Prometheus

Vous pouvez également surveiller les statistiques avec Prometheus, une application de surveillance open source, et Amazon Managed Service for Prometheus. Cela facilite la surveillance des EBS volumes Amazon dans les environnements de conteneurs et Kubernetes à grande échelle. Avec les versions v1.37.0 et ultérieures du EBS CSI pilote Amazon, les statistiques de performances détaillées sont présentées sous forme de point de terminaison compatible avec Prometheus pour être exportées vers Prometheus/`metrics`.

Pour plus d'informations, consultez la section Ingestion des métriques dans votre espace de travail Amazon Managed Service for Prometheus dans le guide de l'utilisateur d'Amazon Managed Service for Prometheus.

Amazon GuardDuty pour Amazon EBS

Amazon GuardDuty est un service de détection des menaces qui aide à protéger vos comptes, vos conteneurs, vos charges de travail et les données de votre AWS environnement. À l'aide de modèles d'apprentissage automatique (ML) et de capacités de détection des anomalies et des menaces, vous surveillez GuardDuty en permanence les différentes sources de journaux et l'activité d'exécution afin d'identifier et de hiérarchiser les risques de sécurité potentiels et les activités malveillantes dans votre environnement.

La fonctionnalité Malware Protection intégrée GuardDuty analyse les EBS volumes Amazon associés à vos EC2 instances Amazon et aux charges de travail de vos conteneurs afin de détecter les menaces potentielles. GuardDuty propose deux méthodes pour ce faire :

- Activer la protection contre les programmes malveillants : lorsqu'un résultat indiquant la présence potentielle d'un logiciel malveillant dans une EC2 instance Amazon ou une charge de travail de conteneur est GuardDuty généré, il lance automatiquement une analyse des programmes malveillants sur la ressource potentiellement compromise.
- Utilisez une analyse des programmes malveillants à la demande sans activer la protection contre les programmes malveillants : indiquez le nom de ressource Amazon (ARN) de votre EC2 instance Amazon pour lancer une analyse à la demande.

Pour plus d'informations, consultez le guide de GuardDuty l'utilisateur Amazon.

Quotas pour Amazon EBS

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas d'AmazonEBS, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez les AWS services, puis sélectionnez Amazon Elastic Block Store (AmazonEBS). Pour demander une augmentation de quota, consultez Demander une augmentation de quota dans le Guide de l'utilisateur de Service Quotas.

Vous Compte AWS disposez des quotas suivants relatifs à AmazonEBS.

Nom	Par défaut	Ajusta	Description
Instantanés archivés par volume	Chaque région prise en charge : 25	Oui	Le nombre maximum d'instantanés archivés par volume.
CompleteSnapshot demandes par compte	Chaque Région prise en charge : 10 par seconde	Non	Le nombre maximum de CompleteSnapshot demandes autorisées par compte.
Copies instantanées simultanées par région de destination	Chaque Région prise en charge : 20	Non	Nombre maximal de copies instantanées simultanées vers une seule région de destination.
Instantanés simultanés par volume Cold HDD (sc1)	Par région prise en charge : 1	Non	Le nombre maximum de snapshots simultanés par volume Cold HDD (sc1) dans cette région.
Instantanés simultanés par volume à usage général SSD (gp2)	Chaque région prise en charge : 5	Non	Nombre maximal d'instantanés simultanés par

Nom	Par défaut	Ajusta	Description
			volume à usage général SSD (gp2) dans cette région.
Instantanés simultanés par volume à usage général SSD (gp3)	Chaque région prise en charge : 5	Non	Nombre maximal d'instantanés simultanés par volume à usage général SSD (gp3) dans cette région.
Instantanés simultanés par volume magnétique (standard)	Chaque région prise en charge : 5	Non	Nombre maximal d'instantanés simultanés par volume magnétique (standard) dans cette région.
Instantanés simultanés par volume provisionné IOPS SSD (io1)	Chaque région prise en charge : 5	Non	Le nombre maximum de snapshots simultanés par volume provisionné IOPS SSD (io1) dans cette région.
Instantanés simultanés par volume provisionné IOPS SSD (io2)	Chaque région prise en charge : 5	Non	Le nombre maximum de snapshots simultanés par volume provisionné IOPS SSD (io2) dans cette région.
Instantanés simultanés par volume optimisé au débit HDD (st1)	Par région prise en charge : 1	Non	Nombre maximal d'instantanés simultanés par volume optimisé au débit HDD (st1) dans cette région.

Nom	Par défaut	Ajusta	Description
Restauration d'instantané rapide	us-east-1 : 5 us-east-2 : 5 us-west-1 : 5 us-west-2 : 5 af-south-1 : 5 ap-east-1 : 5 ap-northeast-1 : 5 ap-northeast-2 : 5 ap-northeast-3 : 5 ap-south-1 : 5 ap-southeast-1 : 5 ap-southeast-2 : 5 ap-southeast-3 : 5 ca-central-1 : 5 eu-central-1 : 5 eu-north-1 : 5 eu-south-1 : 5 eu-west-1 : 5 eu-west-2 : 5 eu-west-3 : 5 me-south-1 : 5	Oui	Nombre maximal de clichés pouvant être activés pour une restauration rapide des instantanés dans cette région.

Nom	Par défaut	Ajusta	Description
	sa-east-1 : 5 Chacune des autres régions prises en charge : 5		
GetSnapshotBlock demandes par compte	us-east-1 : 5 000 par seconde us-east-2 : 5 000 par seconde us-west-2 : 5 000 par seconde ap-southeast-1 : 5 000 par seconde eu-west-1 : 5 000 par seconde Chacune des autres régions prises en charge : 1 000 par seconde	Oui	Le nombre maximum de GetSnapshotBlock demandes autorisées par compte.
GetSnapshotBlock demandes par instantané	Chaque Région prise en charge : 1 000 par seconde	Non	Le nombre maximum de GetSnapshotBlock demandes autorisées par instantané.

Nom	Par défaut	Ajusta	Description
IOPSpour les volumes provisionnés IOPS SSD (io1)	Chaque région prise en charge : 300 000	Oui	Le nombre maximum agrégé de ces volumes peut être provisionné sur les volumes provision nés IOPS SDD (io1) dans IOPS cette région.
IOPSpour les volumes provisionnés IOPS SSD (io2)	Chaque région prise en charge : 100 000	Oui	Le nombre maximum agrégé de ces volumes peut être provisionné sur les volumes provision nés IOPS SDD (io2) dans IOPS cette région.
IOPSmodifications pour les volumes provisionnés IOPS SSD (io1)	Chaque région prise en charge : 500 000	Oui	IOPSModifications maximales sur l'ensembl e du stockage provision né IOPS SSD (io1) dans cette région (Kb/s).
IOPSmodifications pour les volumes provisionnés IOPS SSD (io2)	Chaque région prise en charge : 100 000	Oui	Le courant maximal (depuis) et le maximum demandé (vers) IOPS pour les demandes de modification de volume sur les volumes provision nés IOPS SSD (io2) de cette région.
Archives instantanées en cours par compte	Chaque région prise en charge : 25	Oui	Le nombre maximum d'archives de snapshots en cours par compte.

Nom	Par défaut	Ajusta	Description
Restaurations instantanées en cours à partir d'archives par compte	Chaque Région prise en charge : 5	Oui	Nombre maximal de restaurations de snapshots en cours à partir d'archives par compte.
ListChangedBlocks demandes par compte	Chaque région prise en charge : 50 par seconde	Non	Le nombre maximum de ListChangedBlocks demandes autorisées par compte.
ListSnapshotBlocks demandes par compte	Chaque région prise en charge : 50 par seconde	Non	Le nombre maximum de ListSnapshotBlocks demandes autorisées par compte.
Instantanés en attente par compte	Chaque Région prise en charge : 100	Non	Nombre maximal de clichés en attente par compte.

Nom	Par défaut	Ajusta	Description
PutSnapshotBlock demandes par compte	us-east-1 : 5 000 par seconde us-east-2 : 5 000 par seconde us-west-2 : 5 000 par seconde ap-southeast-1 : 5 000 par seconde eu-west-1 : 5 000 par seconde Chacune des autres régions prises en charge : 1 000 par seconde	Oui	Le nombre maximum de PutSnapshotBlock demandes autorisées par compte.
PutSnapshotBlock demandes par instantané	Chaque Région prise en charge : 1 000 par seconde	Non	Le nombre maximum de PutSnapshotBlock demandes autorisées par instantané.
Instantanés par région	Chaque région prise en charge : 100 000	Oui	Le nombre maximum d'instantanés par région
StartSnapshot demandes par compte	Chaque Région prise en charge : 10 par seconde	Non	Le nombre maximum de StartSnapshot demandes autorisées par compte.

Nom	Par défaut	Ajusta	Description
Stockage pour les volumes Cold HDD (sc1), en TiB	af-south-1 : 300 ap-east-1 : 300 eu-south-1 : 300 me-south-1 : 300 Chacune des autres régions prises en charge : 50	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être provisionnée sur les volumes Cold HDD (sc1) dans cette région.
Volume de stockage pour usage général SSD (gp2), en TiB	af-south-1 : 300 ap-east-1 : 300 eu-south-1 : 300 me-south-1 : 300 Chacune des autres régions prises en charge : 50	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être provisionnée sur des volumes à usage général SSD (gp2) dans cette région.
Volume de stockage pour usage général SSD (gp3), en TiB	af-south-1 : 300 ap-east-1 : 300 eu-south-1 : 300 me-south-1 : 300 Chacune des autres régions prises en charge : 50	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être provisionnée sur des volumes à usage général SSD (gp3) dans cette région.

Nom	Par défaut	Ajusta	Description
Stockage pour volumes magnétiques (standard), en TiB	af-south-1 : 300 ap-east-1 : 300 eu-south-1 : 300 me-south-1 : 300 Chacune des autres régions prises en charge : 50	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être provisionnée sur des volumes magnétiques (standard) dans cette région.
Stockage pour les volumes provisionnés IOPS SSD (io1), en TiB	af-south-1 : 300 ap-east-1 : 300 eu-south-1 : 300 me-south-1 : 300 Chacune des autres régions prises en charge : 50	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être provisionnée sur les volumes provisionnés IOPS SSD (io1) dans cette région.
Stockage pour les volumes provisionnés IOPS SSD (io2), en TiB	Chaque région prise en charge : 20	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être provisionnée sur les volumes provisionnés IOPS SSD (io2) dans cette région.

Nom	Par défaut	Ajusta	Description
Stockage pour les volumes à débit optimisé HDD (st1), en TiB	af-south-1 : 300 ap-east-1 : 300 eu-south-1 : 300 me-south-1 : 300 Chacune des autres régions prises en charge : 50	Oui	Quantité de stockage agrégée maximale, en TiB, qui peut être provisionnée sur des volumes optimisés pour le débit HDD (st1) dans cette région.
Modifications de stockage pour les volumes Cold HDD (sc1), en TiB	Chaque région prise en charge : 500	Oui	La quantité de stockage agrégée maximale, en TiB, qui peut être demandée pour les modifications de volume sur les volumes Cold HDD (sc1) de cette région.
Modifications de stockage pour les volumes à usage général SSD (gp2), en TiB	Chaque région prise en charge : 500	Oui	Modifications de stockage maximales pour l'ensemble du stockage à usage général SSD (gp2) de cette région (TiB).
Modifications de stockage pour les volumes à usage général SSD (gp3), en TiB	Chaque région prise en charge : 500	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être demandée pour les modifications de volume sur les volumes à usage général SSD (gp3) de cette région.

Nom	Par défaut	Ajusta	Description
Modifications de stockage pour les volumes magnétiques (standard), en TiB	Chaque région prise en charge : 500	Oui	La quantité maximale de stockage agrégée, en TiB, qui peut être demandée pour les modifications de volume sur les volumes magnétiques (standard) de cette région.
Modifications du stockage pour les volumes provisionnés IOPS SSD (io1), en TiB	Chaque région prise en charge : 500	Oui	La quantité de stockage agrégée maximale, en TiB, qui peut être demandée pour les modifications de volume sur les volumes provisionnés IOPS SSD (io1) dans cette région.
Modifications du stockage pour les volumes provisionnés IOPS SSD (io2), en TiB	Chaque région prise en charge : 20	Oui	La quantité de stockage agrégée maximale, en TiB, qui peut être demandée pour les modifications de volume sur les volumes provisionnés IOPS SSD (io2) dans cette région.

Nom	Par défaut	Ajusta	Description
Modifications de stockage pour les volumes optimisés pour le débit HDD (st1), en TiB	Chaque région prise en charge : 500	Oui	Quantité de stockage agrégée maximale, en TiB, qui peut être demandée lors de modifications de volume sur des volumes optimisés pour le débit HDD (st1) dans cette région.
Débit de copie des instantanés basé sur le temps par région de destination	Chaque Région prise en charge : 2 000	Oui	Débit maximal au niveau du compte, en Mi/sec, pour les opérations de copie instantanée basées sur le temps par région de destination.

Considérations

- Vos quotas peuvent changer au fil du temps. Amazon surveille EBS en permanence votre stockage provisionné et votre IOPS utilisation dans chaque région et peut augmenter automatiquement vos quotas, région par région, en fonction de votre utilisation. Même si Amazon EBS peut augmenter automatiquement vos quotas en fonction de votre utilisation, vous pouvez demander une augmentation de quota si nécessaire. Par exemple, si vous prévoyez d'utiliser plus de gp3 stockage dans l'est des États-Unis (Virginie du Nord) que votre quota actuel, vous pouvez demander une augmentation du quota pour ce type de volume dans cette région avant l'utilisation prévue.
- Le quota de copies instantanées simultanées par région de destination n'est pas ajustable à l'aide des Quotas de Service. Vous pouvez toutefois demander une augmentation de ce quota en contactant le AWS Support.
- Les IOPSmodifications et les quotas de modifications du stockage s'appliquent à la valeur actuelle agrégée (pour la taille ou IOPS, selon le quota) des volumes qui peuvent subir des modifications simultanément. Vous pouvez effectuer des demandes de modification simultanées pour les volumes dont la valeur actuelle combinée (en termes de taille ou IOPS) est égale au quota. Par

exemple, si votre quota de IOPSmodifications pour les volumes provisionnés IOPS SSD (io1) est égal à`50,000`, vous pouvez effectuer des demandes de IOPS modification simultanées pour un nombre quelconque de `io1` volumes, à condition que leur courant combiné IOPS soit égal ou inférieur à. `50,000` Si trois `io1` volumes sont approvisionnés avec `20,000` IOPS chacun d'eux, vous pouvez demander IOPS des modifications pour deux volumes simultanément ()`20,000 * 2 < 50,000`. Si vous soumettez une demande de IOPS modification simultanée pour le troisième volume, vous dépassez votre quota et cette demande échoue (`20,000 * 3 > 50,000`).

- Amazon EBS applique les limites non ajustables suivantes pour le nombre de EBS volumes par demande de lancement d'instance.
  - `2500`— `us-east-1`us-west-2,`eu-west-1`, et `ap-northeast-1`
  - `500`— toutes les autres régions

  Cette limite s'applique aux demandes de lancement d'instance que vous effectuez, ainsi qu'aux demandes de lancement d'instance effectuées par AWS des services, tels qu'AmazonEMR, en votre nom. Si votre demande de lancement d'instance échoue en raison du dépassement de cette limite, nous vous recommandons d'ajuster la configuration des EBS volumes dans la demande de lancement afin de vous assurer que le nombre de volumes est inférieur à la limite, ou de travailler avec votre responsable de compte technique (TAM) pour explorer d'autres options de lancement de votre cluster sans dépasser la limite.

Historique du document pour le guide de l'utilisateur Amazon EBS

Le tableau suivant décrit les versions de documentation pour Amazon EBS.

Modification	Description	Date
IPv6 Support pour corbeilles	Recycle Bin fournit désormais des points de terminaison à double pile qui prennent en charge à la fois le trafic IPv4 et IPv6 le trafic.	19 décembre 2024
Instantanés locaux dans des zones locales dédiées	Vous pouvez désormais créer des instantanés locaux dans des zones locales dédiées.	16 décembre 2024
AWSDataLifecycleManagerServiceRole AWS politique gérée mise à jour	La politique AWSData LifecycleManagerServiceRole AWS gérée a été mise à jour pour inclure l'autorisation pour l'`ec2:DescribeAvailabilityZones` action.	16 décembre 2024
Copies instantanées basées sur le temps	Vous pouvez désormais demander une durée d'exécution pour les opérations de copie instantanée afin de vous assurer que les copies instantanées sont réalisées dans un délai spécifique.	26 novembre 2024
Balises d'exclusion pour la corbeille	Vous pouvez désormais ajouter des balises d'exclusion aux règles de rétention au niveau des régions afin	19 novembre 2024

	d'exclure les ressources dotées de balises spécifiques.	
AWS CloudFormation support pour Recycle Bin	Vous pouvez désormais créer et gérer des règles de conservation de la corbeille à l'aide de AWS CloudFormation.	18 novembre 2024
Statistiques de performances détaillées d'Amazon EBS	Les appareils en mode NVMe bloc Amazon EBS vendent des statistiques de performance d'E/S haute résolution en temps réel pour les volumes Amazon EBS attachés à des instances Amazon basées sur Nitro. EC2	12 novembre 2024
Nouvelles CloudWatch mesures pour les volumes Amazon EBS	Vous pouvez désormais utiliser les CloudWatch métriques `VolumeAvgReadLatency` `VolumeAvgWriteLatency` ,`VolumeIOPSExceededCheck` , et `VolumeThroughputExceededCheck` Amazon pour surveiller les performances des volumes.	3 octobre 2024
Activez les politiques par défaut d'Amazon Data Lifecycle Manager sur tous les comptes	Vous pouvez les utiliser AWS CloudFormation StackSets pour activer les politiques par défaut d'Amazon Data Lifecycle Manager au AWS sein d'une organisation ou de AWS comptes spécifiques.	26 avril 2024

AWSDataLifecycleManagerSSMFullPolitique de AWS gestion des accès	Mise à jour de la politique afin de prendre en charge les instantanés cohérents par rapport à l'application pour SAP HANA à l'aide du document SSM `AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA` .	17 novembre 2023
VolumeStalledIOCheck métrique	Vous pouvez utiliser la métrique `VolumeStalledIOCheck` pour vérifier si un volume a réussi ou échoué à une vérification d'E/S bloquée au cours de la dernière minute.	16 novembre 2023
Politiques par défaut Amazon Data Lifecycle Manager	Vous pouvez désormais créer des politiques par défaut Amazon Data Lifecycle Manager pour les instantanés EBS et les sauvegardes EBS AMIs afin de sauvegarder tous les volumes et instances d'une région.	16 novembre 2023
Verrouillage d'instantanés Amazon EBS	Vous pouvez verrouiller vos instantanés Amazon EBS pour les protéger contre les suppressions accidentelles ou malveillantes, ou pour les stocker au format WORM pendant une durée déterminée.	15 novembre 2023

Blocage de l'accès public pour les instantanés	Vous pouvez désormais activer le blocage de l'accès public pour les instantanés pour empêcher le partage public de vos instantanés.	9 novembre 2023
Pré-scripts et post-scripts Amazon Data Lifecycle Manager	Vous pouvez désormais utiliser les pré-scripts et les post-scripts dans vos politiques d'instantanés Amazon Data Lifecycle Manager pour automatiser le cycle de vie des instantanés cohérents par rapport à l'application.	7 novembre 2023
NVMe réservations	`io2`Les volumes compatibles avec Multi-Attach prennent en charge les NVMe réservations, qui sont un ensemble de protocoles de clôture de stockage conformes aux normes du secteur.	18 septembre 2023
Tests de défaillance sur Amazon EBS	AWS FIS À utiliser pour arrêter temporairement les E/S entre un volume EBS et les instances auxquelles il est attaché afin de tester la manière dont vos charges de travail gèrent les interruptions d'E/S.	27 janvier 2023

Verrouillage d'une règle de conservation de la corbeille	Vous pouvez verrouiller vos règles de conservation pour les protéger contre les modifications et les suppressions accidentelles ou malveillantes.	23 novembre 2022
Clés de condition pour la corbeille	Vous pouvez utiliser les clés de condition `rbin:Request/ResourceType` et `rbin:Attribute/ResourceType` pour filtrer l'accès sur les demandes de corbeille.	14 juin 2022
Volumes `io2` Block Express	Vous pouvez modifier la taille et les IOPS provisionnés des volumes `io2` Block Express et vous pouvez les activer pour une restauration rapide des instantanés.	31 mai 2022
Corbeille pour AMIs	La corbeille vous permet de restaurer les fichiers supprimés accidentellement AMIs.	3 février 2022
Corbeille pour instantanés Amazon EBS	La corbeille des instantanés Amazon EBS est une fonction de récupération d'instantanés qui vous permet de restaurer des instantanés supprimés accidentellement.	29 novembre 2021

Amazon EBS Snapshots Archive	Amazon EBS Snapshots Archive est un nouveau niveau de stockage que vous pouvez utiliser pour le stockage à long terme et à faible coût de vos instantanés rarement consultés.	29 novembre 2021
Prise en charge de l'obsolescence des AMI pour Amazon Data Lifecycle Manager	Les politiques d'AMI basées sur EBS d'Amazon Data Lifecycle Manager peuvent être déconseillées. AMIs La politique AWSData Lifecycle ManagerServiceRoleFor AMIManagement AWS gérée a été mise à jour pour prendre en charge cette fonctionnalité.	23 août 2021
CloudWatch métriques pour Amazon Data Lifecycle Manager	Vous pouvez surveiller vos politiques Amazon Data Lifecycle Manager à l'aide d'Amazon CloudWatch.	28 juillet 2021
CloudTrail événements liés aux données pour EBS direct APIs	Les événements de données ListSnapshotBlocks ListChangedBlocks GetSnapshotBlock,, et PutSnapshotBlock APIs peuvent être enregistrés CloudTrail.	27 Juillet 2021
Volumes `io2` Block Express	`io2`Les volumes Block Express sont désormais généralement disponibles.	19 juillet 2021

Instantanés locaux Amazon EBS sur Outposts	Vous pouvez désormais utiliser Instantanés locaux Amazon EBS sur Outposts pour stocker des instantanés de volumes sur un Outpost localement dans Amazon S3 sur l'Outpost lui-même.	4 février 2021
Prise en charge de l'attachement multiple pour les volumes io2	Vous pouvez désormais activer les volumes SSD IOPS provisionnés (`io2`) pour Amazon EBS Multi-Attach.	18 décembre 2020
Amazon Data Lifecycle Manager	Utilisez Amazon Data Lifecycle Manager pour automatiser le processus de partage des instantanés et leur copie entre AWS comptes.	17 décembre 2020
Volumes gp3	Un nouveau type de volume Amazon EBS SSD à usage général. Vous pouvez spécifier le débit et les IOPS provisionnés lorsque vous créez ou modifiez le volume.	1er décembre 2020
Tailles de volume HDD à débit optimisé et HDD à froid	Les volumes HDD à débit optimisé (`st1`) et HDD à froid (`sc1`) peuvent varier de 125 GiO à 16 TiO.	30 novembre 2020
Amazon Data Lifecycle Manager	Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création, la conservation et la suppression des fichiers sauvegardés par EBS AMIs.	9 novembre 2020

Amazon Data Lifecycle Manager	Les politiques Amazon Data Lifecycle Manager peuvent être configurées avec quatre planifications au maximum.	17 septembre 2020
Volumes IOPS SSD (io2) provisionnés pour Amazon EBS	Les volumes (`io2`) SSD d'IOPS provisionnés sont conçus pour offrir une durabilité de volume de 99,999 % avec un AFR ne dépassant pas 0,001 %.	24 août 2020
Restauration d'instantané rapide	Vous pouvez activer la restauration rapide des instantanés partagés avec vous.	21 juillet 2020
Amazon EBS Multi-Attach	Vous pouvez désormais attacher un volume SSD d'IOPS provisionnés (io1) à un maximum de 16 instances basées sur Nitro se trouvant dans la même zone de disponibilité.	14 février 2020
Restaurations d'instantanés rapides Amazon EBS	Vous pouvez activer les restaurations d'instantané rapides sur un instantané EBS pour vous assurer que les volumes EBS créés à partir de l'instantané sont entièrement initialisés à la création et fournissent instantanément la totalité des performances allouées.	20 novembre 2019

Instantanés multi-volumes Amazon EBS	Vous pouvez prendre des instantanés exacts point-in-time, coordonnés avec les données et cohérents en cas de crash sur plusieurs volumes EBS attachés à une instance. EC2	29 mai 2019
Chiffrement Amazon EBS par défaut	Une fois que vous avez activé le chiffrement par défaut dans une région, tous les nouveaux volumes EBS que vous créez dans cette région sont chiffrés à l'aide de la clé KMS par défaut pour le chiffrement EBS.	23 mai 2019
Automatisez le cycle de vie	Vous pouvez utiliser Amazon Data Lifecycle Manager pour automatiser la création et la suppression d'instantanés pour vos volumes EBS.	12 juillet 2018
Effectuer des modifications sur les volumes EBS attachés	La plupart des volumes EBS étant attachés à la plupart des EC2 instances, vous pouvez modifier la taille, le type et les IOPS du volume sans détacher le volume ni arrêter l'instance.	13 février 2017
Copiez des instantanés Amazon EBS chiffrés entre Comptes AWS	Vous pouvez désormais copier des instantanés EBS chiffrés entre deux. Comptes AWS	21 juin 2016

Types de volumes HDD et Cold HDD à débit optimisé	Vous pouvez désormais créer des volumes HDD à débit optimisé (st1) et des volumes HDD à froid (sc1).	19 avril 2016
Type de volume SSD à usage général	Les volumes SSD à usage général offrent un stockage économique idéal pour un large éventail de charges de travail. Ces volumes offrent des latences inférieur es à 10 millisecondes, la capacité d'augmenter jusqu'à 3 000 IOPS pour une durée étendue et une performance de base de 3 IOPS/Gio. La taille des volumes polyvalents peut aller de 1 Gio à 1 Tio.	16 juin 2014

Chiffrement Amazon EBS	Chiffrement Amazon EBS offre un chiffrement transparent des instantanés et des volumes de données EBS sans que vous ayez à développer et à maintenir une infrastructure de gestion de clés sécurisée . Le chiffrement EBS assure la sécurité des données au repos en chiffrant vos données à l'aide de clés Clés gérées par AWS. Le chiffrement est effectué sur les serveurs hébergeant les EC2 instances , ce qui permet de chiffrer les données lors de leur transfert entre les EC2 instances et le stockage EBS.	21 mai 2014
Copies instantanées incrémentielles	Vous pouvez désormais effectuer des copies d'instantané incrémentielles.	11 juin 2013
Copie instantanée EBS	Vous pouvez utiliser des copies instantanées pour créer des sauvegardes de données, pour créer de nouveaux volumes Amazon EBS ou pour créer des Amazon Machine Images (AMIs).	17 décembre 2012

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.