aws

Guide du développeur

AWS Backup

AWS Backup: Guide du développeur

Table of Contents

Qu'est-ce que c'est AWS Backup ?

AWS Backup est un service entièrement géré qui facilite la centralisation et l'automatisation de la protection des données dans l'ensemble AWS des services, dans le cloud et sur site. Ce service vous permet de configurer des politiques de sauvegarde et de surveiller l'activité de vos AWS ressources en un seul endroit. Il vous permet d'automatiser et de consolider les tâches de sauvegarde précédemment effectuées service-by-service, et élimine le besoin de créer des scripts personnalisés et des processus manuels. En quelques clics dans la console AWS Backup , vous pouvez automatiser vos politiques et planifications de protection des données.

AWS Backup ne régit pas les sauvegardes que vous effectuez dans votre AWS environnement en dehors de celles-ci AWS Backup. Par conséquent, si vous recherchez une end-to-end solution centralisée répondant aux exigences commerciales et réglementaires, commencez à l'utiliser AWS Backup dès aujourd'hui.

Présentation des fonctionnalités

AWS Backup fournit de nombreuses fonctionnalités et capacités, notamment les suivantes.

Gestion de sauvegarde centralisée

AWS Backup fournit une console de sauvegarde centralisée, un ensemble d'API de sauvegarde et le AWS Command Line Interface (AWS CLI) pour gérer les sauvegardes sur l'ensemble AWS des services utilisés par vos applications. Vous pouvez AWS Backup ainsi gérer de manière centralisée les politiques de sauvegarde qui répondent à vos exigences en matière de sauvegarde. Vous pouvez ensuite les appliquer à vos AWS ressources dans l'ensemble AWS des services, ce qui vous permet de sauvegarder les données de vos applications de manière cohérente et conforme. La console de sauvegarde AWS Backup centralisée offre une vue consolidée de vos sauvegardes et des journaux d'activité des sauvegardes, ce qui facilite l'audit de vos sauvegardes et garantit leur conformité.

Sauvegarde basée sur une politique

Avec AWS Backup, vous pouvez créer des politiques de sauvegarde appelées plans de sauvegarde. Utilisez ces plans de sauvegarde pour définir vos exigences en matière de sauvegarde, puis appliquez-les aux AWS ressources que vous souhaitez protéger dans l'ensemble AWS des services que vous utilisez. Vous pouvez créer différents plans de sauvegarde afin de répondre à des

exigences de conformité réglementaires et commerciales spécifiques. Cela permet de garantir que chaque AWS ressource est sauvegardée conformément à vos besoins. Les plans de sauvegarde facilitent l'application de votre stratégie de sauvegarde dans l'ensemble de votre organisation et de vos applications de manière scalable.

Pour connaître toutes les options de configuration des plans de sauvegarde, consultez Options et configuration d'un plan de sauvegarde.

Politiques de sauvegarde basées sur les balises

Vous pouvez AWS Backup appliquer des plans de sauvegarde à vos AWS ressources de différentes manières, notamment en les étiquetant. Le balisage facilite la mise en œuvre de votre stratégie de sauvegarde dans toutes vos applications et garantit que toutes vos AWS ressources sont sauvegardées et protégées. AWS les balises constituent un excellent moyen d'organiser et de classer vos AWS ressources. L'intégration avec les AWS balises vous permet d'appliquer rapidement un plan de sauvegarde à un groupe de AWS ressources, afin qu'elles soient sauvegardées de manière cohérente et conforme.

Pour connaître toutes les manières dont vous pouvez attribuer vos ressources aux plans de sauvegarde, consultez Affectation de ressources à un plan de sauvegarde.

Politiques de gestion du cycle de vie

AWS Backup vous permet de répondre aux exigences de conformité tout en minimisant les coûts de stockage des sauvegardes en stockant les sauvegardes dans un niveau de stockage à froid à faible coût. Vous pouvez configurer des stratégies de cycle de vie qui transfèrent automatiquement les sauvegardes du stockage chaud au stockage froid en fonction de la planification que vous aurez définie.

Pour une liste des ressources qui peuvent être transférées vers le stockage à froid, consultez Disponibilité des fonctionnalités par ressource. Pour savoir comment activer le stockage à froid dans votre plan de sauvegarde, consultez la section Cycle de vie et niveaux de stockage.

Sauvegarde entre régions

En utilisant AWS Backup, vous pouvez copier des sauvegardes Régions AWS sur plusieurs sites différents à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié. La sauvegarde entre régions est particulièrement utile en cas d’exigences de continuité d'activité ou de

conformité pour stocker les sauvegardes à une distance minimale de vos données de production. Pour plus d'informations, consultez Création de copies de sauvegardes entre Régions AWS.

Gestion et sauvegarde entre comptes

Vous pouvez l'utiliser AWS Backup pour gérer vos sauvegardes dans Comptes AWS l'ensemble de votre AWS Organizationsstructure. Avec la gestion entre comptes, vous pouvez utiliser automatiquement des politiques de sauvegarde pour appliquer des plans de sauvegarde sur l'ensemble des Comptes AWS au sein de votre organisation. Ceci garantit une conformité et une protection des données efficaces à grande échelle et réduit les frais d'exploitation. Cela permet également d'éliminer la duplication manuelle des plans de sauvegarde sur les comptes individuels. Pour plus d'informations, consultez Gestion des ressources AWS Backup sur plusieurs Comptes AWS.

Vous pouvez également copier des sauvegardes sur plusieurs sites différents au Comptes AWS sein de votre structure AWS Organizations de gestion. Ainsi, vous pouvez « ventiler » les sauvegardes vers un seul compte de référentiel, puis « ventiler » les sauvegardes pour une meilleure résilience. Création de copies de sauvegarde entre Comptes AWS.

Avant de pouvoir utiliser les fonctionnalités de gestion et de sauvegarde entre comptes, vous devez disposer d'une structure d'organisation existante configurée dans AWS Organizations. Une unité organisationnelle (UO) est un groupe de comptes qui peut être géré comme une seule entité. AWS Organizations est une liste de comptes qui peuvent être regroupés en unités organisationnelles et gérés comme une seule entité.

Audit et création de rapports avec AWS Backup Audit Manager

AWS Backup Audit Manager vous aide à simplifier la gouvernance des données et la gestion de la conformité de l'ensemble de vos sauvegardes AWS. AWS Backup Audit Manager fournit des contrôles intégrés et personnalisables que vous pouvez adapter aux exigences de votre organisation. Vous pouvez également utiliser ces contrôles pour suivre automatiquement vos activités et ressources de sauvegarde.

AWS Backup Audit Manager peut vous aider à localiser des activités et des ressources spécifiques qui ne sont pas encore conformes aux contrôles que vous avez définis. Il génère également des rapports quotidiens que vous pouvez utiliser pour prouver la conformité de vos contrôles au fil du temps.

Pour intégrer la conformité de vos sauvegardes à votre posture de conformité globale, vous pouvez importer automatiquement les résultats AWS Backup d'Audit Manager dans AWS Audit Manager.

Sauvegardes incrémentielles

AWS Backup stocke efficacement vos sauvegardes périodiques de manière incrémentielle. La première sauvegarde d'une ressource AWS sauvegarde une copie complète de vos données. Pour chaque sauvegarde incrémentielle successive, seules les modifications apportées à vos AWS ressources sont sauvegardées. Les sauvegardes incrémentielles vous permettent de bénéficier de la protection des données grâce aux sauvegardes fréquentes tout en minimisant les coûts de stockage.

Pour une liste des ressources qui prennent en charge les sauvegardes incrémentielles, consultez Disponibilité des fonctionnalités par ressource.

AWS Backup Gestion complète

Certains types de ressources prennent en charge AWS Backup la gestion complète. Les avantages de la AWS Backup gestion complète incluent :

- Chiffrement indépendant. AWS Backup chiffre automatiquement vos sauvegardes avec la clé KMS de votre AWS Backup coffre-fort, au lieu d'utiliser la même clé de chiffrement que votre ressource source. Cela augmente vos niveaux de défense. Pour plus d'informations, consultez Chiffrement pour les sauvegardes dans AWS Backup.
- Amazon Resource Names (ARN) **`awsbackup`**. Les ARN de sauvegarde commencent par `arn:aws:backup` au lieu de `arn:aws:`*`source-resource`*. Cela vous permet de créer des stratégies d'accès qui s'appliquent spécifiquement aux sauvegardes et non aux ressources sources. Pour plus d'informations, consultez Contrôle d'accès.
- Facturation de la sauvegarde centralisée et balises de répartition des coûts Cost Explorer. Les frais AWS Backup (y compris le stockage, les transferts de données, les restaurations et la suppression anticipée) apparaissent sous la rubrique « Sauvegarde » de votre Amazon Web Services facture, au lieu d'apparaître sous chaque ressource prise en charge. Vous pouvez également utiliser les balises de répartition des coûts de Cost Explorer pour suivre et optimiser vos coûts de sauvegarde. Pour plus d'informations, consultez Mesure, coûts et facturation.

Pour savoir quels types de ressources sont éligibles à AWS Backup la gestion complète, consultezDisponibilité des fonctionnalités par ressource.

Surveillance des activités de sauvegarde

AWS Backup fournit un tableau de bord qui facilite l'audit des activités de sauvegarde et de restauration dans l'ensemble AWS des services. En quelques clics sur la AWS Backup console,

vous pouvez consulter l'état des dernières tâches de sauvegarde. Vous pouvez également restaurer des emplois dans l'ensemble AWS des services afin de garantir que vos AWS ressources sont correctement protégées.

AWS Backup s'intègre à Amazon CloudWatch et Amazon EventBridge. CloudWatch vous permet de suivre les métriques et de créer des alarmes. EventBridge vous permet de visualiser et de surveiller les AWS Backup événements. Pour plus d'informations, consultez les sections Surveillance AWS Backup des événements à l'aide EventBridge et Surveillance AWS Backup des métriques avec CloudWatch.

AWS Backup s'intègre à AWS CloudTrail. CloudTrail vous offre une vue consolidée des journaux d'activité de sauvegarde qui permet d'auditer rapidement et facilement la manière dont vos ressources sont sauvegardées. AWS Backup s'intègre également à Amazon Simple Notification Service (Amazon SNS), vous fournissant des notifications d'activité de sauvegarde, par exemple en cas de réussite d'une sauvegarde ou de lancement d'une restauration. Pour plus d'informations, consultez Journalisation des appels AWS Backup d'API avec Amazon SNS CloudTrail et utilisation d'Amazon SNS pour suivre AWS Backup les événements.

Sécurisation de vos données dans des coffres-forts de sauvegarde

Le contenu de chaque AWS Backup sauvegarde est immuable, ce qui signifie que personne ne peut le modifier. AWS Backup sécurise davantage vos sauvegardes dans des coffres-forts de sauvegarde, ce qui les sépare en toute sécurité de leurs instances sources. Par exemple, votre coffre-fort conserve vos sauvegardes Amazon EC2 et Amazon EBS conformément à la politique de cycle de vie que vous choisissez, même si vous supprimez l'instance Amazon EC2 source et les volumes Amazon EBS.

Les coffres-forts de sauvegarde proposent le chiffrement et des stratégies d'accès basées sur les ressources afin de définir qui a accès à vos sauvegardes. Vous pouvez définir des stratégies d'accès pour un coffre-fort de sauvegarde. Elles définissent les personnes autorisées à accéder aux sauvegardes de ce coffre-fort et les actions qu'elles peuvent effectuer. Il s'agit d'un moyen simple et sécurisé de contrôler l'accès à vos sauvegardes sur l'ensemble AWS des services. Pour consulter AWS les politiques gérées par le client pour AWS Backup, consultez la section Politiques gérées pour AWS Backup.

Vous pouvez utiliser AWS Backup Vault Lock pour empêcher quiconque (y compris vous) de supprimer des sauvegardes ou de modifier leur période de conservation. AWS Backup Vault Lock vous aide à appliquer un modèle write-once-read-many(WORM) et à ajouter une couche de défense supplémentaire à votre défense en profondeur. Pour commencer, consultez AWS Backup Vault Lock.

Prise en charge des obligations de conformité

AWS Backup vous aide à respecter vos obligations de conformité internationales. AWS Backup est concerné par les programmes de AWS conformité suivants :

- FedRAMP High
- RGPD
- SOC1, 2 et 3
- PCI
- HIPAA
- et bien d'autres

Premiers pas

Pour en savoir plus AWS Backup, nous vous recommandons de commencer parCommencer avec AWS Backup.

AWS Ressources et applications prises en charge

Vous trouverez ci-dessous des AWS ressources et des applications tierces que vous pouvez sauvegarder et restaurer à l'aide de ces ressources AWS Backup. Pour plus d’informations, consultez the section called “Disponibilité des fonctions”.

Service	Types de ressources pris en charge
Amazon Elastic Compute Cloud (Amazon EC2)	Instances Amazon EC2 (à l’exception des AMI basées sur le stockage d’instances)
Amazon Simple Storage Service (Amazon S3)	Données Amazon S3
Amazon Elastic Block Store (Amazon EBS)	Volumes Amazon EBS
Amazon DynamoDB	Tables Amazon DynamoDB

Service	Types de ressources pris en charge
Amazon Relational Database Service (Amazon RDS)	Instances de base de données Amazon RDS (y compris tous les moteurs de base de données) ; clusters à plusieurs zones de disponibilité
Amazon Aurora	Clusters Aurora
Amazon Elastic File System (Amazon EFS)	Système de fichiers Amazon EFS
FSx pour Lustre	Systèmes de fichiers FSx pour Lustre
FSx for Windows File Server	Système de fichiers FSx for Windows File Server
Amazon FSx pour ONTAP NetApp	Systèmes de fichiers FSx pour ONTAP
Amazon FSx pour OpenZFS	Systèmes de fichiers FSx pour OpenZFS
AWS Storage Gateway (Passerelle de volumes)	AWS Storage Gateway volumes
Amazon DocumentDB	Clusters basés sur des instances Amazon DocumentDB
Amazon Neptune	Clusters Amazon Neptune
Amazon Redshift	Cluster Amazon Redshift
Amazon Timestream	Tableaux Amazon Timestream
VMware Cloud™ sur AWS	Machines virtuelles VMware Cloud™ sur AWS
VMware Cloud™ sur AWS Outposts	Machines virtuelles VMware Cloud™ sur AWS Outposts
AWS CloudFormation	AWS CloudFormation piles

Service	Types de ressources pris en charge
Bases de données SAP HANA	Bases de données SAP HANA sur des instances Amazon EC2

Tarification

Avec AWS Backup, vous payez pour le stockage des sauvegardes, la restauration des données, les tests de restauration, le transfert de données entre régions et AWS Backup Audit Manager. Pour plus d'informations, consultez Tarification d'AWS Backup.

AWS Backup disponibilité des fonctionnalités

AWS Backup les fonctionnalités sont proposées en fonction des ressources et Région AWS. Les sections et tableaux suivants peuvent vous aider à déterminer la disponibilité des fonctionnalités.

Table des matières

Fonctionnalités disponibles pour toutes les ressources prises en charge

AWS Backup propose les fonctionnalités suivantes pour ses AWS services pris en charge, ainsi que pour les applications tierces prises en charge. La prise en charge d'une fonctionnalité ou d'un service ne doit pas être supposée, sauf mention explicite.

- Planifications de sauvegarde automatiques et gestion de la rétention
- Surveillance centralisée des sauvegardes
- Sauvegardes cryptées
- Sauvegardes incrémentielles
- Gestion multi-comptes avec AWS Organizations
- Audits et rapports de sauvegarde automatisés avec AWS Backup Audit Manager

- Écriture unique, lecture multiple (WORM) avec Vault Lock AWS Backup

Disponibilité des fonctionnalités par ressource

Pour être utilisé AWS Backup avec un AWS service pris en charge dans une région donnée, le service doit être disponible dans la région. Pour déterminer la disponibilité du service dans une région, consultez les points de terminaison du service dans le Références générales AWS.

AWS Backup soutient	Sauvegarde entre régions	Sauvegarde entre comptes	AWS Backup Audit Manager	Sauvegarde incrémentielle	Sauvegarde et point-in-time restauration continues	Gestion complète	Cycle de vie jusqu'au stockage à froid	Restauration au niveau de l'élément 1	Tests de restauration
Amazon	✓	✓	✓	✓					✓
Amazon	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
Instance unique Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Cluster Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓					✓
Amazon	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓
Amazon	✓	✓	✓	✓		✓	✓	✓	✓

AWS Backup soutient	Sauvegarde entre régions	Sauvegarde entre comptes	AWS Backup Audit Manager	Sauvegarde incrémentielle	Sauvegarde et point-in-time restauration continue	Gestion complète	Cycle de vie jusqu'au stockage à froid	Restauration au niveau de l'élément [1]	Tests de restauration
FSx pour Lustre	✓	✓	✓	✓					✓
FSx for Windows File Server	✓	✓	✓	✓					✓
FSx pour ONTAP			✓ [2]	✓					✓
FSx pour OpenZFS	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon DocumentDB	✓ [3]	✓ [3]	✓						✓
Amazon Neptune	✓ [3]	✓ [3]	✓						✓
Amazon								✓	

AWS Backup soutient	Sauvegarde entre régions	Sauvegarde entre comptes	AWS Backup Audit Manager	Sauvegarde incrémentielle	Sauvegarde et point-in-time restauration continue	Gestion complète	Cycle de vie jusqu'au stockage à froid	Restauration au niveau de l'élément [1]	Tests de restauration
Timestream	✓	✓	✓	✓		✓	✓	✓	
Windows VSS	✓	✓	✓	✓					
Machines virtuelles	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFormation modèles	✓	✓		✓ [5]		✓	✓ [5]		
Amazon DynamoDB			✓						✓
DynamoDB avec les fonctionnalités avancées AWS Backup	✓	✓	✓			✓	✓		✓

AWS Backup soutient	Sauvegarde entre régions	Sauvegarde entre comptes	AWS Backup Audit Manager	Sauvegarde incrémentielle	Sauvegarde et point-in-time restauration continues	Gestion complète	Cycle de vie jusqu'au stockage à froid	Restauration au niveau de l'élément [1]	Tests de restauration
Bases de données SAP HANA sur des instances Amazon				✓	✓	✓	✓		

Certains types de ressources disposent à la fois d'une fonction de sauvegarde continue et de la copie entre régions et entre comptes. Lorsqu'une copie entre régions ou entre comptes d'une sauvegarde continue est réalisée, le point de récupération copié (sauvegarde) devient une sauvegarde instantanée (périodique). Amazon RDS et Amazon S3 prennent en charge les copies instantanées incrémentielles ; Amazon Aurora ne prend en charge que les copies instantanées complètes. La restauration à un instant dans le passé (PITR) n'est pas disponible pour ces copies.

[1] L' « élément » d'une restauration au niveau de l'élément varie en fonction de la ressource prise en charge. Par exemple, un élément du système de fichiers est un fichier ou un répertoire, tandis qu'un élément S3 est un objet S3. Un élément VMware est un disque. Pour plus d'informations, consultez la section Restauration d'une sauvegarde sur la ressource prise en charge.

[2] AWS Backup Audit Manager prend en charge cette ressource pour tous les contrôles, à l'exception de la copie entre comptes et de la copie entre régions.

[3] RDS, Aurora, DocumentDB et Neptune ne prennent pas en charge une seule action de copie qui effectue à la fois une sauvegarde entre régions ET entre comptes. Vous devez choisir l'une ou l'autre. Vous pouvez également utiliser un AWS Lambda script pour écouter la fin de votre première copie, effectuer votre deuxième copie, puis supprimer la première copie. Les instances de base de données

RDS à plusieurs zones de disponibilité (multi-AZ) peuvent être copiées, mais les clusters multi-AZ ne prennent actuellement pas en charge la copie entre régions ou entre comptes. Voir Considérations relatives à la copie entre régions avec des ressources spécifiques pour plus d'informations.

[4] Consultez la section Sauvegardes de zones de multidisponibilité RDS pour les régions où le support de Backup Audit Manager est disponible.

[5] Dans les sauvegardes par CloudFormation pile, les ressources imbriquées conservent les fonctionnalités de leurs ressources sources. Cependant, les ressources de la pile ne conservent pas les fonctionnalités de restauration ponctuelle (PITR) (telles qu'Amazon S3 et Amazon RDS). Les propriétés de la matrice ci-dessus s'appliquent uniquement aux CloudFormation modèles et non aux ressources de la pile.

[6] Pour Aurora, les instantanés sont complets et une sauvegarde incrémentielle est proposée via PITR.

Disponibilité des fonctionnalités par Région AWS

AWS Backup est disponible dans toutes les versions suivantes Régions AWS. AWS Backup les fonctionnalités sont disponibles dans toutes ces régions, sauf indication contraire dans le tableau suivant.

AWS Backup soutient	Sauvegarde entre régions	Gestion entre comptes	Sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration
USA Est (Virginie du Nord)	✓	✓	✓	✓	✓
USA Est (Ohio)	✓	✓	✓	✓	✓
USA Ouest (Californie du Nord)	✓	✓	✓	✓	✓

AWS Backup soutient	Sauvegarde entre régions	Gestion entre comptes	Sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration
USA Ouest (Oregon)	✓	✓	✓	✓	✓
Afrique (Le Cap)	✓		✓	✓	✓
Asie-Pacifique (Hong Kong)	✓		✓	✓	✓
Asie-Pacifique (Hyderabad)	✓		✓		✓
Asie-Pacifique (Jakarta)	✓		✓		✓
Asie-Pacifique (Melbourne)	✓		✓		✓
Asie-Pacifique (Mumbai)	✓	✓	✓	✓	✓
Asie-Pacifique (Osaka)	✓	✓	✓		✓
Asia Pacific (Seoul)	✓	✓	✓	✓	✓

AWS Backup soutient	Sauvegarde entre régions	Gestion entre comptes	Sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration
Asie-Pacifique (Singapour)	✓	✓	✓	✓	✓
Asie-Pacifique (Sydney)	✓	✓	✓	✓	✓
Asie-Pacifique (Tokyo)	✓	✓	✓	✓	✓
Canada (Centre)	✓	✓	✓	✓	✓
Canada Ouest (Calgary)	✓ (sauf Amazon S3)		✓		
Chine (Beijing)	✓				
China (Ningxia)	✓				
Europe (Francfort)	✓	✓	✓	✓	✓
Europe (Irlande)	✓	✓	✓	✓	✓
Europe (Londres)	✓	✓	✓	✓	✓

AWS Backup soutient	Sauvegarde entre régions	Gestion entre comptes	Sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration
Europe (Milan)	✓		✓	✓	✓
Europe (Paris)	✓	✓	✓	✓	✓
Europe (Espagne)	✓		✓		✓
Europe (Stockholm)	✓	✓	✓	✓	✓
Europe (Zurich)	✓		✓		✓
Israël (Tel Aviv)	✓		✓		
Moyen-Orient (Bahreïn)	✓		✓	✓	✓
Moyen-Orient (EAU)	✓		✓		✓
Amérique du Sud (São Paulo)	✓	✓	✓	✓	✓
AWS GovCloud (USA Est)	✓	✓	✓	✓	

AWS Backup soutient	Sauvegarde entre régions	Gestion entre comptes	Sauvegarde entre comptes	AWS Backup Audit Manager et tableau de bord des jobs	Tests de restauration
AWS GovCloud (US-Ouest)	✓	✓	✓	✓	

Les régions Chine (Beijing) et Chine (Ningxia) prennent en charge la copie entre ces deux régions. La copie entre régions n'est pas prise en charge depuis ces régions vers d'autres régions ou inversement. La copie entre comptes n'est pas prise en charge pour ces régions.

Le tableau de bord des offres d'emploi n'est pas disponible dans AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). L'agrégation du tableau de bord des offres d'emploi n'est disponible que dans les régions qui prennent en charge la gestion entre AWS Backup comptes et Audit Manager.

Amazon FSx for Windows File Server et Amazon Neptune ne prennent pas en charge les copies de sauvegarde interrégionales dans les régions à adhésion volontaire.

Services pris en charge par Région AWS

AWS Backup prend en charge les éléments suivants dans toutes les régions prises en charge :

- Aurora
- DynamoDB
- DynamoDB avec fonctionnalités avancées AWS Backup
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

Le tableau suivant indique le AWS Backup soutien apporté aux autres Services AWS par région.

Région et service	Amazon FSx	SAP HANA sur des instances EC	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup
USA Est (Virginie du Nord)	✓	✓	✓	✓	✓	✓
USA Est (Ohio)	✓	✓	✓	✓	✓	✓
USA Ouest (Californie du Nord)	Windows ; Lustre ; ONTAP	✓	✓	✓		✓
USA Ouest (Oregon)	Windows ; Lustre ; ONTAP	✓	✓	✓	✓	✓
Afrique (Le Cap)	Windows ; Lustre ; ONTAP	✓	✓[1]	✓		✓
Asie-Pacifique (Hong Kong)	✓	✓	✓[1]	✓		✓
Asie-Pacifique (Hyderabad)	Windows ; Lustre ; ONTAP		✓[1]	✓		
Asie-Pacifique (Jakarta)	Windows ; Lustre ; ONTAP		✓	✓		

Région et service	Amazon FSx	SAP HANA sur des instances EC	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup
Asie-Pacifique (Melbourne)	Windows ; Lustre ; ONTAP		✓[1]	✓		
Asie-Pacifique (Mumbai)	✓	✓	✓	✓		✓
Asie-Pacifique (Osaka)	Windows ; Lustre	✓	✓[1]	✓		✓
Asie-Pacifique (Séoul)	✓	✓	✓	✓		✓
Asie-Pacifique (Singapour)	✓	✓	✓	✓		✓
Asie-Pacifique (Sydney)	✓	✓	✓	✓	✓	✓
Asie-Pacifique (Tokyo)	✓	✓	✓	✓	✓	✓
Canada (Centre)	✓	✓	✓	✓		✓

Région et service	Amazon FSx	SAP HANA sur des instances EC	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup
Canada Ouest (Calgary)						
Chine (Beijing)	Windows ; Lustre		✓[1]	✓	✓	
Chine (Ningxia)	Windows ; Lustre		✓[1]	✓	✓	
Europe (Francfort)	✓	✓	✓	✓	✓	✓
Europe (Irlande)	✓	✓	✓	✓	✓	✓
Europe (Londres)	✓	✓	✓	✓		✓
Europe (Milan)	Windows ; Lustre ; ONTAP	✓	✓[1]	✓		✓
Europe (Paris)	Windows ; Lustre ; ONTAP	✓	✓	✓		✓
Europe (Espagne)	Windows ; Lustre ; ONTAP		✓[1]	✓		
Europe (Stockholm)	✓	✓	✓	✓		✓

Région et service	Amazon FSx	SAP HANA sur des instances EC	Amazon S3	Storage Gateway	Amazon Timestream	VMware et passerelle Backup
Europe (Zurich)	Windows ; Lustre ; ONTAP		✓[1]	✓		
Israël (Tel Aviv)	Windows ; Lustre ; ONTAP		✓[1]	✓		
Moyen-Orient (Bahreïn)	Windows ; Lustre ; ONTAP	✓	✓[1]	✓		✓
Moyen-Orient (EAU)			✓[1]	✓		
Amérique du Sud (São Paulo)		✓	✓	✓		✓
AWS GovCloud (US-Ouest)	Windows ; Lustre ; ONTAP		✓[1]	✓		✓
AWS GovCloud (USA Est)	Windows ; Lustre ; ONTAP		✓[1]	✓		✓

Une vérification sous Amazon FSx indique que FSx for Windows File Server, FSx for Lustre, FSx for ONTAP et FSx pour OpenZFS sont tous pris en charge dans cette région par ; sinon, les configurations prises en AWS Backup charge seront répertoriées.

[1] Les copies entre régions et entre comptes ne sont pas prises en charge.

AWS Backup : comment ça marche

AWS Backup est un service de sauvegarde entièrement géré qui facilite la centralisation et l'automatisation de la sauvegarde des données entre les AWS services. Avec AWS Backup, vous pouvez créer des politiques de sauvegarde appelées plans de sauvegarde. Vous pouvez utiliser ces plans pour définir vos besoins en matière de sauvegarde, notamment la fréquence de sauvegarde de vos données et la durée de conservation de ces sauvegardes.

AWS Backup vous permet d'appliquer des plans de sauvegarde à vos AWS ressources en les étiquetant simplement. AWS Backup sauvegarde ensuite automatiquement vos AWS ressources conformément au plan de sauvegarde que vous avez défini.

Les sections suivantes décrivent son AWS Backup fonctionnement, les détails de sa mise en œuvre et les considérations relatives à la sécurité.

Rubriques

Comment AWS Backup fonctionne avec les AWS services pris en charge

Certains AWS services AWS Backup pris en charge proposent leurs propres fonctionnalités de sauvegarde autonomes. Ces fonctionnalités sont à votre disposition, que vous utilisiez ou non AWS Backup. Cependant, les sauvegardes créées par AWS les autres services ne sont pas disponibles pour une gouvernance centralisée AWS Backup.

AWS Backup Pour configurer la gestion centralisée de la protection des données pour tous les services pris en charge, vous devez choisir de gérer ce service avec AWS Backup, créer une sauvegarde à la demande ou planifier des sauvegardes à l'aide d'un plan de sauvegarde, puis stocker vos sauvegardes dans des coffres-forts de sauvegarde.

Rubriques

- Utilisation avec les données Amazon S3
- Utilisation avec les machines virtuelles VMware
- Utilisation d'Amazon DynamoDB
- Utilisation avec les systèmes de fichiers Amazon FSx
- Utilisation avec Amazon EC2
- Utilisation avec Amazon EFS
- Utilisation avec Amazon EBS
- Utilisation avec Amazon RDS et Aurora
- Travailler avec AWS BackInt
- Travailler avec AWS Storage Gateway
- Utilisation avec Amazon DocumentDB
- Utilisation avec Amazon Neptune
- Utilisation avec Amazon Timestream
- Travailler avec AWS Organizations
- Travailler avec AWS CloudFormation
- Travailler avec AWS BackInt, AWS Systems Manager pour SAP et SAP HANA
- Comment AWS les services sauvegardent leurs propres ressources

Optez pour la gestion des services avec AWS Backup

Lorsque de nouveaux AWS services sont disponibles, vous AWS Backup devez autoriser leur utilisation. Si vous essayez de créer un plan de sauvegarde ou la sauvegarde à la demande à l'aide de ressources provenant d'un service qui n'est pas activé, un message d'erreur s'affiche et le processus ne peut pas être achevé.

La AWS Backup console dispose de deux méthodes pour inclure des types de ressources dans un plan de sauvegarde : attribuer explicitement le type de ressource dans un plan de sauvegarde ou inclure toutes les ressources. Consultez les points ci-dessous pour comprendre comment ces sélections fonctionnent avec les activations de service.

- Si les attributions de ressources sont uniquement basées sur des balises, les paramètres d'acceptation du service sont appliqués.

- Si un type de ressource est explicitement attribué à un plan de sauvegarde, il sera inclus dans la sauvegarde même si l'opt-in n'est pas activé pour ce service en particulier. Cela ne s'applique pas à Aurora, Neptune et Amazon DocumentDB. Pour que ces services soient inclus, l'opt-in doit être activé.
- Si le type de ressource et les balises sont spécifiés dans une attribution de ressource, les types de ressources spécifiés sont d'abord filtrés, puis les balises filtrent davantage ces ressources.

  Les paramètres d'abonnement au service sont ignorés pour la plupart des types de ressources. Aurora, Neptune et Amazon DocumentDB nécessitent toutefois un abonnement au service.
- Pour Amazon FSx for NetApp ONTAP, lorsque vous utilisez la sélection de ressources basée sur des balises, appliquez des balises à des volumes individuels plutôt qu'à l'ensemble du système de fichiers.

Les paramètres d'abonnement au service sont spécifiques à une région. Lorsqu'un compte utilise AWS Backup (crée un coffre de sauvegarde ou un plan de sauvegarde) dans une région, il est automatiquement activé pour tous les types de ressources pris AWS Backup en charge par la région à ce moment-là. Les services pris en charge ajoutés ultérieurement à cette région ne seront pas automatiquement inclus dans un plan de sauvegarde. Vous pouvez choisir d'opter pour ces types de ressources une fois qu'ils seront pris en charge.

Pour configurer les services utilisés avec AWS Backup

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Activation du service, choisissez Configurer les ressources.
4. Utilisez les commutateurs à bascule pour activer ou désactiver les services utilisés avec AWS Backup.

   > **Important**
   >
   > RDS, Aurora, Neptune et DocumentDB partagent le même Amazon Resource Name (ARN). Choisir de gérer l'un de ces types de ressources en AWS Backup optant pour chacun d'entre eux lors de son affectation à un plan de sauvegarde. Quoi qu'il en soit, nous vous recommandons de tous les activer afin de représenter avec précision votre statut d'activation.

5. Choisissez Confirmer.

Utilisation avec les données Amazon S3

AWS Backup propose une sauvegarde et une restauration entièrement gérées pour les sauvegardes Amazon S3. Pour en savoir plus, veuillez consulter la section Sauvegardes Amazon S3.

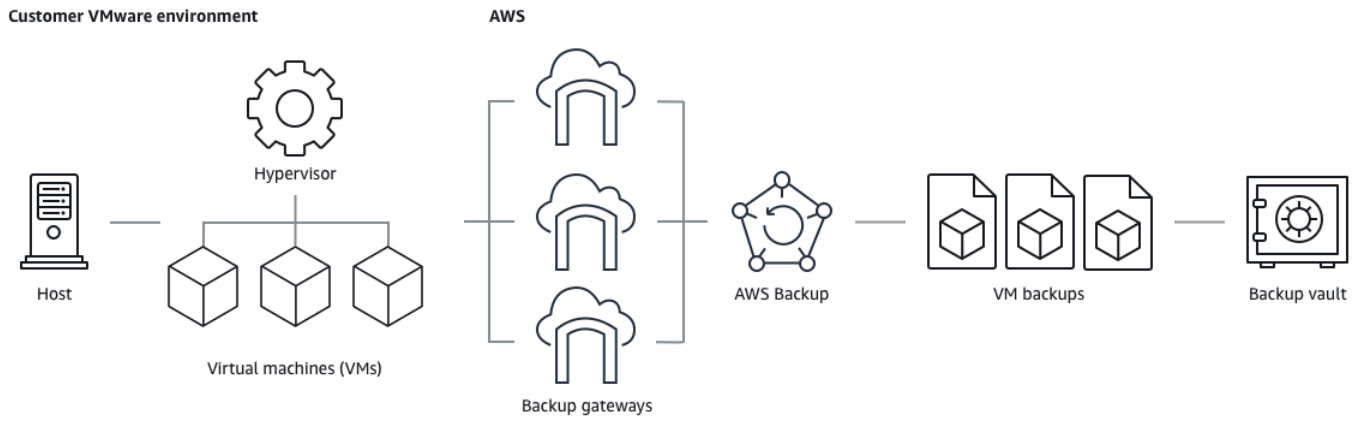
- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer les données Amazon S3 à l'aide de AWS Backup : Restauration des données S3

Pour obtenir des informations détaillées sur les données S3, consultez la documentation Amazon S3.

Utilisation avec les machines virtuelles VMware

AWS Backup prend en charge la protection des données centralisée et automatisée pour les machines virtuelles (VM) VMware sur site ainsi que pour les machines virtuelles du VMware Cloud™ (VMC) sur. AWS Vous pouvez effectuer des sauvegardes depuis vos machines virtuelles sur site et VMC vers AWS Backup. Vous pouvez ensuite effectuer une restauration sur site ou sur VMC. AWS Backup

Backup Gateway est AWS Backup un logiciel téléchargeable que vous déployez sur vos machines virtuelles VMware pour les connecter AWS Backup. La passerelle se connecte à votre serveur de gestion de machines virtuelles pour découvrir les machines virtuelles, découvrir vos machines virtuelles, chiffrer les données et les transférer efficacement vers AWS Backup. Le schéma suivant illustre la connexion de Backup Gateway à vos machines virtuelles :



- Comment sauvegarder des ressources : Sauvegardes de machines virtuelles

- Comment restaurer des ressources d'une machine virtuelle : Restauration d'une machine virtuelle à l'aide de AWS Backup

Utilisation d'Amazon DynamoDB

AWS Backup prend en charge la sauvegarde et la restauration des tables Amazon DynamoDB. DynamoDB est un service de base de données NoSQL entièrement géré qui offre des performances rapides et prévisibles avec une capacité de mise à l'échelle simple.

Depuis son lancement, DynamoDB AWS Backup a toujours été compatible. À partir de novembre 2021, des fonctionnalités avancées ont AWS Backup également été introduites pour les sauvegardes DynamoDB. Ces fonctionnalités avancées incluent la copie de vos sauvegardes entre comptes Régions AWS et comptes, la hiérarchisation des sauvegardes vers un stockage à froid et l'utilisation de balises pour les autorisations et la gestion des coûts.

Les fonctionnalités avancées de sauvegarde DynamoDB seront activées par défaut pour les nouveaux AWS Backup clients qui s'installeront après novembre 2021.

Nous recommandons à tous les AWS Backup clients existants d'activer les fonctionnalités avancées de DynamoDB. Il n'y a aucune différence de tarification du stockage de sauvegarde à chaud après l'activation des fonctionnalités avancées, et vous pouvez économiser de l'argent en hiérarchisant les sauvegardes vers le stockage à froid et optimiser vos coûts en utilisant des balises de répartition des coûts.

Pour obtenir une liste complète des fonctionnalités avancées et savoir comment les activer, consultez Sauvegarde DynamoDB avancée.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des ressources DynamoDB : Restauration d'une table Amazon DynamoDB

Pour obtenir des informations détaillées sur DynamoDB, consultez Qu'est-ce qu'Amazon DynamoDB ? dans le Guide du développeur Amazon DynamoDB.

Utilisation avec les systèmes de fichiers Amazon FSx

AWS Backup prend en charge la sauvegarde et la restauration des systèmes de fichiers Amazon FSx. Amazon FSx fournit des systèmes de fichiers tiers entièrement gérés avec la compatibilité native et les ensembles de fonctionnalités pour les charges de travail. AWS Backup utilise la fonctionnalité de sauvegarde intégrée d'Amazon FSx. Les sauvegardes effectuées depuis la console

AWS Backup présentent donc le même niveau de cohérence et de performance du système de fichiers, ainsi que les mêmes options de restauration que les sauvegardes effectuées via la console Amazon FSx.

Si vous gérez AWS Backup ces sauvegardes, vous bénéficiez de fonctionnalités supplémentaires, telles que des options de rétention illimitées et la possibilité de créer des sauvegardes planifiées toutes les heures. En outre, AWS Backup conserve vos sauvegardes même après la suppression du système de fichiers source. Cela permet d'éviter les suppressions accidentelles ou malveillantes.

Utilisez-le AWS Backup pour protéger les systèmes de fichiers Amazon FSx si vous souhaitez configurer des politiques de sauvegarde et surveiller les tâches de sauvegarde à partir d'une console de sauvegarde centrale qui étend également la prise en charge d'autres AWS services.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des ressources Amazon FSx : Restauration d'un système de fichiers FSX

Pour obtenir des informations détaillées sur les systèmes de fichiers Amazon FSx, consultez la documentation Amazon FSx.

Utilisation avec Amazon EC2

AWS Backup prend en charge les instances Amazon EC2.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des ressources Amazon EC2 : Restauration d'une instance Amazon EC2

Vous pouvez planifier ou exécuter des tâches de sauvegarde à la demande qui incluent des instances EC2 complètes, y compris ses volumes Amazon EBS. Par conséquent, vous pouvez restaurer une instance Amazon EC2 complète à partir d'un point de récupération unique, y compris le volume racine, les volumes de données et certains paramètres de configuration de l'instance, tels que le type d'instance et la paire de clés.

Vous pouvez également sauvegarder et restaurer vos applications Microsoft Windows compatibles avec VSS. Vous pouvez planifier des sauvegardes cohérentes avec les applications, définir des politiques de cycle de vie et effectuer des restaurations cohérentes dans le cadre d'une sauvegarde à la demande ou d'un plan de sauvegarde planifié. Pour plus d’informations, consultez Création de sauvegardes Windows VSS.

AWS Backup ne redémarre à aucun moment vos instances EC2.

Images et instantanés

Lors de la sauvegarde d'une instance Amazon EC2, AWS Backup prend un instantané du volume de stockage Amazon EBS racine, des configurations de lancement et de tous les volumes EBS associés. AWS Backup stocke certains paramètres de configuration de l'instance EC2, notamment le type d'instance, les groupes de sécurité, Amazon VPC, la configuration de surveillance et les balises. Les données de sauvegarde sont stockées sous la forme d'une Amazon Machine Image (AMI) basée sur le volume Amazon EBS.

Si vous supprimez un instantané Amazon Machine Image (AMI) ou Amazon EBS géré à l' AWS Backup aide de la corbeille Amazon EC2 AWS Backup et que vous avez configuré la corbeille, l'image ou l'instantané peut entraîner des frais conformément à la politique relative aux corbeilles Amazon EC2. Les instantanés et les images de la corbeille Amazon EC2 ne sont plus gérés et ne seront plus gérés AWS Backup par des politiques si vous les restaurez depuis la corbeille. AWS Backup

AWS Backup les instantanés Amazon EBS gérés et les instantanés associés à une AMI AWS Backup Amazon EC2 gérée sur laquelle Amazon EBS Snapshot Lock est appliqué ne peuvent pas être supprimés dans le cadre du cycle de vie du point de restauration si la durée du verrouillage des instantanés dépasse le cycle de vie de sauvegarde. Ces points de récupération auront plutôt le statut `EXPIRED`. Ces points de récupération peuvent être supprimés manuellement si vous choisissez de supprimer d’abord le verrouillage d’instantané Amazon EBS.

AWS Backup peut chiffrer les instantanés EBS associés à une sauvegarde Amazon EC2. Cela est similaire à la façon dont il chiffre les instantanés EBS. AWS Backup utilise le même chiffrement que celui appliqué aux volumes EBS sous-jacents lors de la création d'un instantané de l'AMI Amazon EC2, et les paramètres de configuration de l'instance d'origine sont conservés dans les métadonnées de restauration.

Un instantané tire son chiffrement du volume, et le même chiffrement est appliqué aux instantanés correspondants. Les instantanés EBS d'une AMI copiée sont toujours chiffrés. Si vous spécifiez une clé KMS lors de la copie, la clé spécifiée est appliquée. Si vous ne spécifiez pas de clé KMS, une clé KMS par défaut est appliquée.

Pour plus d'informations, consultez les instances Amazon EC2 dans le guide de l'utilisateur Amazon EC2 et le chiffrement Amazon EBS dans le guide de l'utilisateur Amazon EBS.

Utilisation avec Amazon EFS

AWS Backup prend en charge Amazon Elastic File System (Amazon EFS).

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des ressources Amazon EFS : Restauration d'un système de fichiers Amazon EFS

Pour obtenir des informations détaillées sur les systèmes de fichiers Amazon EFS, consultez Qu'est-ce qu'Amazon Elastic File System ? dans le Guide de l'utilisateur Amazon Elastic File System.

Utilisation avec Amazon EBS

AWS Backup prend en charge les volumes Amazon Elastic Block Store (Amazon EBS).

AWS Backup les instantanés Amazon EBS gérés et les instantanés associés à une AMI AWS Backup Amazon EC2 gérée sur laquelle Amazon EBS Snapshot Lock est appliqué ne peuvent pas être supprimés dans le cadre du cycle de vie du point de restauration si la durée du verrouillage des instantanés dépasse le cycle de vie de sauvegarde. Ces points de récupération auront plutôt le statut `EXPIRED`. Ces points de récupération peuvent être supprimés manuellement si vous choisissez de supprimer d'abord le verrouillage d'instantané Amazon EBS.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des volumes Amazon EBS : Restauration d'un volume Amazon EBS

Pour plus d'informations, consultez les volumes Amazon EBS dans le guide de l'utilisateur Amazon EBS.

Utilisation avec Amazon RDS et Aurora

AWS Backup prend en charge les moteurs de base de données Amazon RDS et les clusters Aurora.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des ressources Amazon RDS : Restauration d'une base de données RDS
- Comment restaurer des clusters Aurora : Restauration d'un cluster Amazon Aurora

Pour plus d'informations sur Amazon RDS, consultez Qu'est-ce que Amazon Relational Database Service (Amazon RDS) ? dans le Guide de l'utilisateur Amazon RDS.

Pour obtenir des informations détaillées sur Aurora, consultez Qu'est-ce qu'Amazon Aurora ? dans le Guide de l'utilisateur Amazon Aurora..

> **Note**
>
> Si vous lancez une tâche de sauvegarde depuis la console Amazon RDS, cela peut entrer en conflit avec une tâche de sauvegarde des clusters Aurora, provoquant le message d'erreur La tâche de sauvegarde a expiré avant d'être terminée. Dans ce cas, configurez une fenêtre de sauvegarde plus longue dans AWS Backup.

> **Note**
>
> RDS Custom for SQL Server et RDS Custom for Oracle ne sont actuellement pas pris en charge par AWS Backup.

> **Note**
>
> AWS ne facture pas les instantanés Aurora stockés dans un coffre-fort de sauvegarde tant qu'Aurora a activé les sauvegardes automatisées et que la période de conservation des sauvegardes automatisées Aurora est supérieure à la période de conservation des instantanés Aurora. Tous les instantanés contenus dans le coffre-fort de sauvegarde seront facturés si la base de données des instantanés est supprimée (les suppressions peuvent se produire accidentellement ou lors d'un déploiement bleu/vert).
> Les instantanés volumineux et les sauvegardes fréquentes à partir d'une base de données supprimée peuvent entraîner des frais de stockage importants. Consultez le Calculateur AWS Backup pour estimer les frais AWS Backup potentiels.

Travailler avec AWS BackInt

AWS Backup fonctionne avec AWS Backint pour prendre en charge la sauvegarde et la restauration des bases de données SAP HANA sur les instances Amazon EC2.

- Instructions pour sauvegarder et restaurer les ressources SAP HANA : sauvegarde et restauration des instances SAP HANA Amazon EC2
- Configurer le AWS Backint Agent AWS : Backint Agent pour SAP HANA

Travailler avec AWS Storage Gateway

AWS Backup prend en charge Storage Gateway Volume Gateway. Vous pouvez également restaurer des instantanés Amazon EBS sous forme de volumes Storage Gateway.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des ressources Storage Gateway : Restauration d'un volume Storage Gateway.

Utilisation avec Amazon DocumentDB

AWS Backup prend en charge les clusters Amazon DocumentDB.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer les ressources Amazon DocumentDB :. Restauration d'un cluster DocumentDB

Utilisation avec Amazon Neptune

AWS Backup prend en charge les clusters Amazon Neptune.

- Comment sauvegarder des ressources : Commencer avec AWS Backup
- Comment restaurer des clusters Amazon Neptune : Restauration d'un cluster Neptune.

Utilisation avec Amazon Timestream

AWS Backup prend en charge les tables Amazon Timestream.

- Comment sauvegarder des tables Timestream.
- Comment restaurer des tables Timestream.

Travailler avec AWS Organizations

AWS Backup fonctionne avec AWS Organizations pour simplifier le suivi et la gestion entre comptes

- Création d'un compte de gestion dans Organizations.
- Activation de la gestion entre comptes.

- Désignation des comptes d'administrateur délégué et des politiques de délégation.

Travailler avec AWS CloudFormation

AWS Backup AWS CloudFormation modèles de support et piles d'applications

- AWS CloudFormation empiler des sauvegardes

Travailler avec AWS BackInt, AWS Systems Manager pour SAP et SAP HANA

AWS Backup fonctionne avec AWS BackInt et avec SSM pour SAP afin de prendre en charge les fonctions de sauvegarde et de restauration de SAP HANA.

- Sauvegarde de bases de données SAP HANA sur des instances Amazon EC2
- Commencez avec AWS Systems Manager pour SAP
- AWS Backint Agent pour SAP HANA

Comment AWS les services sauvegardent leurs propres ressources

Vous pouvez consulter la documentation technique concernant le processus de sauvegarde et de restauration d'un AWS service spécifique, en particulier lorsque, lors d'une restauration, vous devez configurer une nouvelle instance de ce AWS service. Voici une liste de la documentation :

- Services connexes Amazon EC2
- Utilisation AWS Backup avec Amazon EFS
- Sauvegarde et restauration à la demande pour DynamoDB
- Instantanés Amazon EBS
- Sauvegarde et restauration d'une instance de base de données Amazon RDS
  - Présentation de la sauvegarde et de la restauration d'un cluster de bases de données Aurora
- Utilisation AWS Backup avec FSx for Windows File Server
- Utilisation AWS Backup avec FSx for Lustre
- Sauvegarde de vos volumes dans AWS Storage Gateway
- Sauvegarde et restauration dans Amazon DocumentDB

- Sauvegarde et restauration d'un cluster Amazon Neptune

Mesure, coûts et facturation

AWS Backup tarification

AWS Backup Les prix actuels sont disponibles au AWS Backup tarif indiqué.

> **Important**
>
> Pour éviter des frais supplémentaires, configurez votre politique de rétention avec une durée de stockage à chaud d'au moins une semaine.
> Supposons, par exemple, que vous effectuiez des sauvegardes quotidiennes et que vous les conserviez pendant une journée. En outre, supposons que vos ressources protégées soient si importantes qu'il vous faudra une journée entière pour terminer votre sauvegarde. AWS Backup met en œuvre votre période de conservation d'un jour et retire votre sauvegarde du stockage à chaud une fois votre travail de sauvegarde terminé. Le lendemain, AWS Backup impossible de créer une sauvegarde incrémentielle car vous n'avez aucune sauvegarde dans un espace de stockage chaud. Cette période de rétention n'étant pas conforme aux bonnes pratiques, vous encourez les risques et les dépenses liés à la création quotidienne d'une sauvegarde complète.
> Contactez-nous AWS Support pour obtenir de l'aide supplémentaire.

AWS Backup facturation

Lorsqu'un type de ressource prend en charge AWS Backup la gestion complète, les frais d'AWS Backup activité (y compris le stockage, les transferts de données, les restaurations et les suppressions anticipées) apparaissent dans la section « Backup » de votre Amazon Web Services facture. Pour obtenir la liste des services qui prennent en charge la AWS Backup gestion complète, consultez la section AWS Backup Gestion complète du Disponibilité des fonctionnalités par ressource tableau.

Lorsqu'un type de ressource ne prend pas en charge AWS Backup la gestion complète, certaines de vos AWS Backup activités, telles que les coûts de stockage pour vos sauvegardes, sont facturées par le AWS service concerné.

Échecs des tâches de copie

Vous ne serez débité qu'une fois qu'un point de récupération aura été créé dans le coffre-fort de destination. Aucun frais n'est facturé en cas d'échec d'une tâche de copie et si aucun point de récupération n'est créé.

Balises d'allocation des coûts

Vous pouvez utiliser des balises de répartition des coûts pour suivre et optimiser AWS Backup les coûts de manière détaillée, ainsi que pour afficher et filtrer ces balises à l'aide de AWS Cost Explorer.

Pour utiliser des balises de répartition des coûts, consultez Automating backups and optimizing backup costs for Amazon EFS using AWS Backup et Utilisation des balises de répartition des coûts.

AWS Backup Tarification d'Audit Manager

AWS Backup Audit Manager facture l'utilisation en fonction du nombre d'évaluations de contrôle. Une évaluation de contrôle est l'évaluation d'une ressource par rapport à un contrôle. Les frais d'évaluation du contrôle apparaissent sur votre AWS Backup facture. Pour connaître les tarifs actuels des évaluations de contrôle, consultez Tarification d'AWS Backup.

Pour utiliser les contrôles AWS Backup d'Audit Manager, vous devez activer AWS Config l'enregistrement afin de suivre votre activité de sauvegarde. AWS Config des frais pour chaque élément de configuration enregistré, et ces frais apparaissent sur votre AWS Config facture. Pour connaître la tarification actuelle des éléments de configuration enregistrés, consultez Tarification d'AWS Config.

Tarification d'Amazon Aurora

Pendant la période de rétention configurée pour les sauvegardes continues Aurora (jusqu'à 35 jours), les instantanés ne sont pas soumis à des frais de stockage. Les instantanés conservés après cette période sont facturés en tant que sauvegardes complètes.

AWS Backup blogs, vidéos, didacticiels et autres ressources

Pour plus d'informations sur AWS Backup, consultez les rubriques suivantes :

- Backup et restaurez des machines virtuelles VMware sur site à l'aide AWS Backup de. Avec Olumuyiwa Koya et Ezekiel Oyerinde (juin 2022).
- À utiliser AWS Backup pour protéger les bases de données Amazon Aurora. Avec Chris Hendon, Brandon Rubadou et Thomas Liddle (mai 2022).

- Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups. Avec Evan Peck et Sabith Venkitachalapathy (mai 2022).
- Automatisez et améliorez votre posture de sécurité à l'aide AWS Backup de et AWS PrivateLink. Avec Bilal Alam (avril 2022).
- Obtenez des rapports quotidiens agrégés entre comptes et multirégions. AWS Backup Avec Wali Akbari et Sabith Venkitachalapathy (février 2022).
- Automatisez la visibilité des résultats de sauvegarde à l'aide AWS Backup de et AWS Security Hub. Avec Kanishk Mahajan (janvier 2022).
- Les 10 meilleures pratiques de sécurité pour sécuriser les sauvegardes dans AWS. Avec Ibukun Oyewumi (janvier 2022).
- Optimisation de SAS Grid AWS avec FSx for Lustre (et optimisation de la reprise après sinistre AWS Backup grâce à FSx for Lustre). Avec Matt Saeger et Shea Lutton (janvier 2022).
- Centralisation de la protection des données et de la conformité dans Amazon Neptune AWS Backup avec. Avec Brian O'Keefe (novembre 2021).
- Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup. Avec Karthik Vijayraghavan (novembre 2021).
- Simplifiez l'audit de vos politiques de protection des données avec AWS Backup Audit Manager. Avec Jordan Bjorkman et Harshitha Putta (novembre 2021).
- Améliorez le niveau de sécurité de vos sauvegardes avec AWS Backup Vault Lock. Avec Rolland Miller (octobre 2021).
- Comment conserver les balises de ressources dans les tâches de AWS Backup restauration. Avec Ibukun Oyewumi, Amee Shah et Sabith Venkitachalapathy (septembre 2021).
- Gestion de l'accès aux sauvegardes à l'aide de politiques de contrôle des services avec AWS Backup. Avec Sabith Venkitachalapathy et Ibukun Oyewumi (août 2021).
- Automatisez la sauvegarde centralisée à grande échelle sur l'ensemble AWS des services à l'aide de AWS Backup. Avec Ibukun Oyewumi et Sabith Venkitachalapathy (juillet 2021).
- Blog : Comment simplifier la sauvegarde de Microsoft SQL Server à l'aide AWS Backup de VSS. Avec Siavash Irani et Sepehr Samiei (juillet 2021).
- Automatisez la validation de la récupération des données avec AWS Backup. Avec Mahanth Jayadeva (juin 2021).
- Configuration des notifications pour surveiller les AWS Backup tâches. Avec Virgil Ennes (juin 2021).

- Automating backups and optimizing backup costs for Amazon EFS using AWS Backup. Avec Prachi Gupta et Rohit Verma (juin 2021).
- Gestion des coûts de sauvegarde Amazon EFS : AWS Backup prise en charge des balises de répartition des coûts. Avec Aditya Maruvada (mai 2021).
- Créez et partagez des sauvegardes chiffrées entre les comptes et les régions à l'aide de AWS Backup. Avec Prachi Gupta (mai 2021).
- AWS Backup est désormais approuvé par FedRAMP High pour vos besoins en matière de conformité et de protection des données. Avec Andy Grimes (mai 2021).
- ZS Associates améliore l'efficacité des sauvegardes grâce à AWS Backup. Avec Mitesh Naik, Hiranand Mulchandani et Sushant Jadhav (mai 2021).
- Tutoriel : utilisation AWS Backup d'Amazon EBS Backup and Restore. Avec Fathima Kamal (avril 2021).
- Didacticiel vidéo : Managing cross-Region copies of backups. Avec David DeLuca (avril 2021).
- Supprimez plusieurs points AWS Backup de récupération à l'aide AWS des outils pour PowerShell. Avec Sherif Talaat (avril 2021).
- Sauvegardes entre régions et entre comptes pour Amazon FSx utilisant. AWS Backup Avec Adam Hunter et Fathima Kamal (avril 2021).
- Amazon CloudWatch Events and Metrics pour AWS Backup. Avec Rolland Miller (mars 2021).
- Tutoriel : Sauvegarde et restauration d'Amazon Relational Database Service (RDS) à l'aide de. AWS Backup Avec Fathima Kamal (mars 2021).
- oint-in-time Restauration IP et sauvegarde continue pour Amazon RDS avec AWS Backup. Avec Kelly Griffin (mars 2021).
- Automatisez AWS Backup avec AWS Service Catalog. avec John Husemoller (janvier 2021).
- Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup. Avec Cher Simon (janvier 2021).
- AWS Récapitulatif de re:Invent : Protection des données et conformité avec. AWS Backup Avec Nancy Wang (décembre 2020).
- AWS Backup fournit une protection centralisée des données pour l'ensemble de vos AWS ressources. Avec Nancy Wang (novembre 2020).
- Tech Talk: Data protection at scale with AWS Backup. Avec Kareem Behairy (septembre 2020).
- Gestion centralisée entre comptes avec utilisation de copies interrégionales. AWS Backup Avec Cher Simon (septembre 2020).

- Tutoriel vidéo : Gérer les sauvegardes à grande échelle AWS Organizations selon votre utilisation AWS Backup. Avec Ildar Sharafeev (juillet 2020).
- Gérez les sauvegardes à grande échelle AWS Organizations selon votre utilisation AWS Backup. Avec Nancy Wang, Avi Drabkin, Ganesh Sundaresan et Vikas Shah (juin 2020).
- Récupérez les fichiers et dossiers Amazon EFS avec AWS Backup. Avec Abrar Hussain et Gurudath Pai (mai 2020).
- Scheduling automated backups using Amazon EFS and AWS Backup. Avec Rob Barnes (décembre 2019).
- Re:Invent Recording : AWS re:Invent 2019 : Une plongée profonde sur pieds AWS Backup Rackspace. Avec Nancy Wang et Jason Pavao (décembre 2019).
- Protégez vos données avec AWS Backup. Avec Anthony Fiore (juillet 2019).
- Vidéo marketing : Introducing AWS Backup. Janvier 2019.
- Vidéo : Introduction to AWS Backup. Avec AWS formation et certification.

Configuration AWS pour la première fois

Avant de l'utiliser AWS Backup pour la première fois, effectuez les tâches suivantes :

1. Inscrivez-vous pour AWS
2. Créer un utilisateur IAM
3. Créer un rôle IAM

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez à Amazon Web Services (AWS), vous êtes automatiquement Compte AWS inscrit à tous les services AWS, y compris AWS Backup. Seuls les services que vous utilisez vous sont facturés.

Pour plus d'informations sur les taux AWS Backup d'utilisation, consultez la page AWS Backup Tarification.

Si vous en avez Compte AWS déjà un, passez à la tâche suivante. Si vous n'avez pas de compte AWS , observez la procédure suivante pour en créer un.

Pour créer un Compte AWS

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

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

   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 en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

Notez votre Compte AWS numéro, car vous en aurez besoin pour la prochaine tâche.

Créer un utilisateur IAM

Les services AWS, tels que AWS Backup, nécessitent que vous fournissiez des informations d'identification lorsque vous y accédez, afin que le service puisse déterminer si vous êtes autorisé à accéder à ses ressources. AWS recommande de ne pas utiliser l'utilisateur Compte AWS root pour effectuer des demandes. Il est préférable de créer un utilisateur IAM, puis de lui accorder un accès total. Nous appelons de tels utilisateurs des administrateurs. Vous pouvez utiliser les informations d'identification de l'utilisateur administrateur, au lieu des informations d'identification de l'utilisateur Compte AWS root, pour interagir avec AWS et effectuer des tâches, telles que créer un bucket, créer des utilisateurs et leur accorder des autorisations. Pour plus d'informations, consultez Informations d'identification de l'utilisateur root du Compte AWS par rapport aux informations d'identification de l'utilisateur IAM dans la Référence générale AWS et Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Si vous vous êtes inscrit AWS mais que vous n'avez pas créé d'utilisateur IAM pour vous-même, vous pouvez en créer un à l'aide de la console IAM.

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

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des identifiants à court terme pour accéder à AWS. Telles sont les meilleures pratiques en matière de sécurité. Pour plus d'informations sur les bonnes pratiques, veuillez	Suivre les instructions de la section Mise en route dans le AWS IAM Identity Center Guide de l'utilisateur.	Configurez l'accès par programmation en configurant le AWS CLI à utiliser AWS IAM Identity Center dans le guide de l'AWS Command Line Interface utilisateur.

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
	consulter Security best practices in IAM (français non garanti) dans le Guide de l'utilisateur IAM.		
Dans IAM (Non recommandé)	Utiliser des identifiants à long terme pour accéder à AWS.	Suivre les instructions relatives à la Création de votre premier groupe utilisateur administrateur et utilisateur IAM dans le Guide de l'utilisateur IAM.	Configuration de l'accès par programmation via la Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Pour vous connecter en tant que nouvel utilisateur IAM, déconnectez-vous du AWS Management Console. Utilisez ensuite l'URL suivante, où your_aws_account_id est votre Compte AWS numéro sans les tirets (par exemple, si votre numéro est le cas, votre Compte AWS identifiant est) : `1234-5678-9012` Compte AWS `123456789012`

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Saisissez le nom utilisateur et le mot de passe IAM que vous venez de créer. Lorsque vous êtes connecté, la barre de navigation affiche votre_nom_utilisateur@votre_id_compte_aws.

Si vous ne souhaitez pas que l'URL de votre page de connexion contienne votre Compte AWS identifiant, vous pouvez créer un alias de compte. Dans le tableau de bord IAM, cliquez sur Créer un alias de compte et entrez un alias, tel que le nom de votre société. Pour vous connecter après avoir créé un alias de compte, utilisez l'URL suivante :

```
https://your_account_alias.signin.aws.amazon.com/console/
```

Pour vérifier le lien de connexion des utilisateurs IAM de votre compte, ouvrez la console IAM et vérifiez le contenu du champ Alias de Compte AWS sur le tableau de bord.

Créer un rôle IAM

Vous pouvez utiliser la console IAM pour créer un rôle IAM qui accorde des AWS Backup autorisations d'accès aux ressources prises en charge. Une fois que vous avez créé le rôle IAM, vous devez y attacher des politiques.

Pour créer un rôle IAM avec la console

1. Connectez-vous à la console AWS de gestion et ouvrez la console IAM.
2. Dans la console IAM, choisissez Rôles dans le volet de navigation, puis Créer un rôle.
3. Choisissez Fonctions du service AWS , puis Sélectionner pour AWS Backup. Sélectionnez Next: Permissions (Étape suivante : autorisations).
4. Sur la page Attacher des stratégies d'autorisations, cochez `AWSBackupServiceRolePolicyForBackup` et `AWSBackupServiceRolePolicyForRestores`. Ces politiques AWS gérées AWS Backup autorisent la sauvegarde et la restauration de toutes les AWS ressources prises en charge. Pour en savoir plus sur les politiques gérées et afficher des exemples, consultez Politiques gérées.

   Puis, choisissez Next : Tags (Suivant : balises).
5. Choisissez Suivant : vérification.
6. Pour Nom du rôle, saisissez un nom qui décrit l'objectif de ce rôle. Les noms de rôles doivent être uniques au sein de votre Compte AWS. Différentes entités peuvent référencer le rôle et il n'est donc pas possible d'en modifier le nom après sa création.

   Choisissez Create Role (Créer un rôle).
7. Dans la page Rôles, choisissez le rôle que vous avez créé et ouvrez sa page de détails.

Commencer avec AWS Backup

Ce didacticiel décrit les étapes génériques d'utilisation des AWS Backup fonctionnalités. Comme pour toute partie de cette documentation technique, vous devez suivre la console AWS de gestion dans l'autre fenêtre.

Vous pouvez également apprendre à utiliser AWS Backup un service spécifique en lisant ces didacticiels :

- Backup et restauration Amazon Relational Database Service (Amazon RDS) à l'aide de AWS Backup
- Tutoriel : Amazon EBS Backup and Restore à l'aide d'Amazon EBS AWS Backup

Rubriques

Prérequis

Avant de commencer, vérifiez que vous disposez des éléments suivants :

- Un Compte AWS. Pour plus d’informations, consultez Configuration AWS pour la première fois.
- Au moins une ressource prise en charge par AWS Backup.
- Vous devez connaître les AWS services et les ressources que vous sauvegardez. Consultez la liste des ressources et des applications tierces prises en charge par AWS.

Lorsque de nouveaux AWS services sont disponibles, activez AWS Backup l'option d'utilisation de ces services.

Pour configurer les AWS services à utiliser avec AWS Backup

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
3. Sur la page Activation du service, choisissez Configurer les ressources.
4. Sur la page Configurer les ressources, utilisez les commutateurs pour activer ou désactiver les services utilisés avec AWS Backup. Choisissez Confirmer lorsque vos services sont configurés. Assurez-vous que le AWS service que vous choisissez est disponible dans votre Région AWS.

Voir Affectation de ressources à un plan de sauvegarde pour plus d'informations. La AWS Backup console permet à un utilisateur d'attribuer un type de ressource à un plan de sauvegarde ; celui-ci sera inclus même si l'opt-in n'est pas activé pour ce service en particulier.

- Assurez-vous que les ressources que vous sauvegardez sont dans la même Région AWS.

Pour terminer ce didacticiel, vous pouvez utiliser votre utilisateur Compte AWS root pour vous connecter au AWS Management Console. AWS Identity and Access Management (IAM) recommande toutefois de ne pas utiliser l'utilisateur Compte AWS root. Au lieu de cela, créez un administrateur dans votre compte et utilisez ces informations d'identification pour gérer les ressources de votre compte. Pour plus d’informations, consultez Configuration AWS pour la première fois.

La AWS Backup console propose différentes options pour sauvegarder vos ressources. Vous pouvez créer une sauvegarde à la demande, planifier et configurer la manière dont vous souhaitez que la ressource soit sauvegardée ou configurer les ressources pour qu'elles soient sauvegardées automatiquement lors de leur création.

Mise en route 1 : activation du service

La AWS Backup console dispose de deux méthodes pour inclure des types de ressources dans un plan de sauvegarde : attribuer explicitement le type de ressource dans un plan de sauvegarde

ou inclure toutes les ressources. Consultez les points ci-dessous pour comprendre comment ces sélections fonctionnent avec les activations de service.

- Si les attributions de ressources sont uniquement basées sur des balises, les paramètres d'acceptation du service sont appliqués.
- Si un type de ressource est explicitement attribué à un plan de sauvegarde, il sera inclus dans la sauvegarde même si l'opt-in n'est pas activé pour ce service en particulier. Cela ne s'applique pas à Aurora, Neptune et Amazon DocumentDB. Pour que ces services soient inclus, l'opt-in doit être activé.
- Si le type de ressource et les balises sont spécifiés dans une attribution de ressource, les types de ressources spécifiés sont d'abord filtrés, puis les balises filtrent davantage ces ressources.

  Les paramètres d'abonnement au service sont ignorés pour la plupart des types de ressources. Aurora, Neptune et Amazon DocumentDB nécessitent toutefois un abonnement au service.
- Pour Amazon FSx for NetApp ONTAP, lorsque vous utilisez la sélection de ressources basée sur des balises, appliquez des balises à des volumes individuels plutôt qu'à l'ensemble du système de fichiers.

Les choix d'opt-in s'appliquent au compte spécifique et Région AWS. Lorsqu'un compte utilise AWS Backup (crée un coffre de sauvegarde ou un plan de sauvegarde) dans une région, il est automatiquement activé pour tous les types de ressources pris AWS Backup en charge par la région à ce moment-là. Les services pris en charge ajoutés ultérieurement à cette région ne seront pas automatiquement inclus dans un plan de sauvegarde. Vous pouvez choisir d'opter pour ces types de ressources une fois qu'ils seront pris en charge.

Comme il AWS Backup prend en charge de plus en plus de AWS services et d'applications tierces, vous devrez peut-être revoir cette étape pour accéder à ces ressources nouvellement prises en charge.

AWS Backup ne régit ni ne gère les sauvegardes effectuées dans AWS des environnements autres que AWS Backup.

À activer pour protéger tous les types AWS Backup de ressources pris en charge

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation de gauche, choisissez Paramètres.

3. Sous Activation du service, choisissez Configurer les ressources.
4. Accédez à toutes les ressources AWS Backup prises en charge en déplaçant tous les boutons vers la droite.
5. Choisissez Confirm (Confirmer).

Étapes suivantes

Pour créer une sauvegarde à la demande à l'aide de AWS Backup, passez àMise en route 2 : création d'une sauvegarde à la demande.

Mise en route 2 : création d'une sauvegarde à la demande

Sur la AWS Backup console, la page Ressources protégées répertorie les ressources qui ont été sauvegardées au AWS Backup moins une fois. Si vous l'utilisez AWS Backup pour la première fois, aucune ressource, telle que les volumes Amazon EBS ou les bases de données Amazon RDS, n'est répertoriée sur cette page. C'est le cas même si une ressource a été affectée à un plan de sauvegarde, si ce plan de sauvegarde n'a pas exécuté de tâche de sauvegarde planifiée au moins une fois.

Au cours de cette première étape, vous allez créer une sauvegarde à la demande de l'une de vos ressources. Cette ressource sera ensuite répertoriée sur la page Protected resources (Ressources protégées).

Pour créer une sauvegarde à la demande

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. À l'aide du volet de navigation, choisissez Ressources protégées, puis Créer une sauvegarde à la demande.
3. Sur la page Créer une sauvegarde à la demande, choisissez le type de ressource que vous souhaitez sauvegarder. Par exemple, choisissez DynamoDB pour les tables Amazon DynamoDB.
4. Choisissez le nom ou l'ID de la ressource que vous voulez protéger. Assurez-vous que la ressource que vous avez choisie est celle que vous souhaitez.

> **Note**
>
> Pour Amazon FSx pour Lustre, les types de déploiement Persistent et Persistent_2 sont pris en charge.

5. Assurez-vous que Create backup now (Créer une sauvegarde maintenant) est sélectionné. Une sauvegarde est immédiatement lancée et vos ressources enregistrées s'affichent plus tôt sur la page Protected resources (Ressources protégées).
6. Spécifiez une valeur de transition vers le stockage à froid (le cas échéant) et une valeur d'expiration.

> **Note**
>
> - Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau Disponibilité des fonctionnalités par ressource. Tous les autres types de ressources sont enregistrés dans le stockage à chaud et ignorent l'expression de transition vers le stockage à froid. La valeur Expiration est valide pour tous les types de ressources.
> - Lorsque les sauvegardes expirent et sont marquées pour suppression dans le cadre de votre politique de cycle de vie, AWS Backup supprime les sauvegardes à un moment choisi au hasard au cours des 8 heures suivantes. Cette fenêtre permet de garantir des performances constantes.

7. Choisissez un coffre-fort de sauvegarde existant. Si vous choisissez Créer un coffre de sauvegarde, une nouvelle page s'ouvre afin que vous puissiez créer un coffre. Une fois que vous avez terminé, vous revenez à la page Créer une sauvegarde à la demande.
8. Sous IAM role (Rôle IAM), choisissez Default role (Rôle par défaut).

> **Note**
>
> Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle est créé pour vous avec les autorisations appropriées.

9. Si vous souhaitez affecter une ou plusieurs balises à votre sauvegarde à la demande, entrez une clé et une valeur facultative, puis choisissez Add tag (Ajouter une balise).

> **Note**
>
> - Pour les ressources Amazon EC2, copie AWS Backup automatiquement les balises de ressources individuelles et de groupe existantes, en plus de toutes les balises que vous ajoutez à cette sauvegarde. Pour plus d'informations, consultez Copie de balises sur des sauvegardes.
> - Lorsque vous créez un plan de sauvegarde basé sur des balises, si vous choisissez un rôle autre que le rôle par défaut, assurez-vous qu'il dispose des autorisations nécessaires pour sauvegarder toutes les ressources balisées. AWS Backup essaie de traiter toutes les ressources avec les balises sélectionnées. S'il trouve une ressource à laquelle il n'est pas autorisé à accéder, le plan de sauvegarde échoue.

10. Choisissez Create on-demand backup (Créer une sauvegarde à la demande). Vous accédez ainsi à la page Jobs (Tâches), où vous pouvez consulter une liste des tâches.
11. Si votre type de ressource est EC2, la section Paramètres de sauvegarde avancés s'affiche. Choisissez Windows VSS si votre instance EC2 exécute Microsoft Windows. Cela vous permet d'effectuer des sauvegardes Windows VSS cohérentes avec les applications.

> **Note**
>
> AWS Backup prend actuellement en charge les sauvegardes cohérentes avec les applications des ressources exécutées uniquement sur Amazon EC2. Les types d'instances ou applications ne sont pas tous pris en charge pour les sauvegardes VSS Windows. Pour plus d'informations, consultez Création de sauvegardes Windows VSS.

12. Choisissez l'ID de tâche de sauvegarde de la ressource que vous avez choisi de sauvegarder pour afficher les détails de cette tâche.

Étapes suivantes

Pour automatiser votre activité de sauvegarde, passez à Mise en route 3 : création d'une sauvegarde planifiée.

Mise en route 3 : création d'une sauvegarde planifiée

Dans cette étape du AWS Backup didacticiel, vous allez créer un plan de sauvegarde, y affecter des ressources, puis créer un coffre-fort de sauvegarde.

Avant de commencer, vérifiez que vous respectez les prérequis. Pour plus d'informations, consultez Commencer avec AWS Backup.

Rubriques

Étape 1 : Créer un plan de sauvegarde basé sur un plan existant

Un plan de sauvegarde est une expression de politique qui définit quand et comment sauvegarder vos ressources AWS , telles que des tables Amazon DynamoDB ou des systèmes de fichiers Amazon Elastic File System (Amazon EFS). Vous attribuez des ressources aux plans de sauvegarde, AWS Backup puis vous sauvegardez et conservez automatiquement les sauvegardes de ces ressources conformément au plan de sauvegarde. Pour plus d'informations, consultez Gestion des sauvegardes à l'aide de plans de sauvegarde.

Il existe deux façons de créer un plan de sauvegarde : à partir de zéro ou à partir d'un plan de sauvegarde existant. Cet exemple utilise la AWS Backup console pour créer un plan de sauvegarde en modifiant un plan de sauvegarde existant.

Pour créer un plan de sauvegarde à partir d'un plan existant

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le tableau de bord, choisissez Gérer les plans de sauvegarde. Ou, dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Choisissez Démarrer avec un modèle, choisissez un plan dans la liste (par exemple, `Daily-Monthly-1yr-Retention`) et entrez un nom dans la zone Nom du plan de sauvegarde.

> **Note**
>
> Si vous essayez de créer un plan de sauvegarde identique à un plan existant, vous obtenez une erreur `AlreadyExistsException`.

4. Sur la page Récapitulatif du plan, choisissez la règle de sauvegarde que vous voulez, puis Modifier.
5. Vérifiez et choisissez les valeurs souhaitées pour votre règle (consultez Options et configuration d'un plan de sauvegarde pour des options de règle).
6. Pour le coffre-fort de sauvegarde, choisissez Par défaut ou Créer un coffre de backup pour créer un nouveau coffre-fort.
7. (Facultatif) - Région AWS choisissez-en un dans la liste de la région de destination pour copier la sauvegarde dans une autre région. Pour ajouter d'autres régions, choisissez Ajouter une copie.
8. Lorsque vous avez terminé de modifier la règle, choisissez Enregistrer la règle de backup.

Sur la page Résumé, choisissez Affecter des ressources pour préparer la section suivante.

Étape 2 : Affecter des ressources à un plan de sauvegarde

Après avoir créé un plan de sauvegarde, vous devez affecter vos AWS ressources à ce plan de sauvegarde. Pour plus d'informations sur l'attribution des ressources, consultez Affectation de ressources à un plan de sauvegarde.

Si vous ne possédez pas encore de AWS ressources à affecter à un plan de sauvegarde, créez de nouvelles ressources à utiliser pour cet exercice. Créez une ou deux ressources à l'aide de ressources prises en charge par AWS et d'applications tierces.

Pour affecter des ressources à un plan de sauvegarde

1. Les étapes précédentes auraient dû vous mener à la page Attribuer des ressources.
2. Saisissez un Nom d'attribution de ressource.
3. Pour le rôle IAM, choisissez Rôle par défaut. Si vous choisissez un autre rôle, il doit disposer des autorisations nécessaires pour sauvegarder toutes les ressources que vous attribuez.
4. Dans la section Attribuer des ressources, choisissez Inclure tous les types de ressources. Un type de ressource est un AWS service AWS Backup pris en charge ou une application tierce. Ce

plan de sauvegarde protège désormais tous les types de ressources que vous avez choisi de protéger à l'aide de AWS Backup

5. Choisissez Attribuer des ressources.

Vous revenez à la page Résumé du plan de sauvegarde. Choisissez Créer un plan de sauvegarde pour déployer votre premier plan de sauvegarde !

Étape 3 : Créer un coffre-fort de sauvegarde

Au lieu d'utiliser le coffre-fort de sauvegarde par défaut qui est créé automatiquement pour vous sur la console AWS Backup , vous pouvez créer des coffres-forts de sauvegarde spécifiques pour enregistrer et organiser les groupes de sauvegardes dans le même coffre-fort.

Pour plus d'informations sur les coffres-forts de sauvegarde, consultez Coffres-forts de sauvegarde.

Pour créer un coffre-fort de sauvegarde

1. Sur la AWS Backup console, dans le volet de navigation, sélectionnez Backup vaults.

> **Note**
>
> Si le volet de navigation n'est pas visible sur le côté gauche, vous pouvez l'ouvrir en choisissant l'icône du menu dans le coin supérieur gauche de la AWS Backup console.

2. Choisissez Create backup vault (Créer un coffre-fort de sauvegarde).
3. Saisissez un nom pour votre coffre-fort de sauvegarde. Le nom de votre coffre-fort peut refléter ce que vous allez y stocker, ou faciliter la recherche des sauvegardes dont vous avez besoin. Vous pouvez par exemple nommer le coffre-fort **`FinancialBackups`**.
4. Sélectionnez une touche AWS Key Management Service (AWS KMS). Vous pouvez utiliser une clé que vous avez déjà créée ou sélectionner la clé AWS Backup KMS par défaut.

> **Note**
>
> La AWS KMS clé spécifiée ici s'applique uniquement aux sauvegardes de services prenant en charge le chiffrement AWS Backup indépendant. Pour consulter la liste des types de ressources qui prennent en charge le chiffrement AWS Backup

indépendant, consultez la section « AWS Backup Gestion complète » du Disponibilité des fonctionnalités par ressource tableau.

5. Vous pouvez également ajouter des balises qui vous aideront à rechercher et identifier vos coffres-forts de sauvegarde. Par exemple, vous pouvez ajouter une balise **`BackupType:Financial`**.
6. Choisissez Créer un coffre-fort de sauvegarde.
7. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde) et vérifiez que votre coffre-fort a été ajouté.

> **Note**
>
> Vous pouvez maintenant modifier une règle de sauvegarde dans l'un de vos plans de sauvegarde, afin de stocker les sauvegardes créées par cette règle dans le coffre-fort de sauvegarde que vous venez de créer.

Étapes suivantes

Pour sauvegarder spécifiquement les systèmes de fichiers Amazon EFS, passez à Mise en route 4 : création de sauvegardes automatiques Amazon EFS.

Mise en route 4 : création de sauvegardes automatiques Amazon EFS

Lorsque vous créez un système de fichiers Amazon Elastic File System (Amazon EFS) avec la console Amazon EFS, les sauvegardes automatiques sont activées par défaut. Si vous souhaitez sauvegarder automatiquement un système de fichiers Amazon EFS existant, vous pouvez le faire à l'aide de la console Amazon EFS, de l'API ou de l'interface de ligne de commande.

Pour sauvegarder automatiquement un système de fichiers Amazon EFS existant à l'aide de la console

1. Ouvrez la console Amazon EFS ici : https://console.aws.amazon.com/efs.
2. Sur la page Systèmes de fichiers, choisissez un système de fichiers pour activer les sauvegardes automatiques.

3. Choisissez Modifier dans le panneau des paramètres Général.
4. Pour activer les sauvegardes automatiques, choisissez Activer les sauvegardes automatiques.

Le paramètre du plan de sauvegarde par défaut est `daily backups, 35-day retention`. La fenêtre de sauvegarde par défaut (la période pendant laquelle la sauvegarde s'exécutera) est définie pour démarrer à 5 heures UTC (temps universel coordonné) et dure 8 heures.

> **Note**
>
> Le coffre-fort de sauvegarde automatique Amazon EFS `aws/efs/automatic-backup-vault` est réservé à ces sauvegardes automatiques uniquement.
> Ce coffre-fort ne doit pas être utilisé pour créer des copies entre comptes ou comme destination pour les sauvegardes créées par d'autres plans de sauvegarde non automatisés. Si vous l'utilisez comme destination pour d'autres plans de sauvegarde, vous recevrez un message d'erreur « privilèges insuffisants ».

AWS Backup crée un rôle lié à un service en votre nom dans votre compte. Ce rôle a les autorisations requises pour réaliser des sauvegardes Amazon EFS. Pour obtenir des informations détaillées sur les rôles liés à un service, consultez Utilisation des rôles liés aux services pour AWS Backup.

Pour savoir step-by-step comment activer ou désactiver les sauvegardes automatiques à l'aide de la console, de l'API ou de la CLI Amazon EFS, consultez la section Sauvegardes automatiques dans le guide de l'utilisateur Amazon Elastic File System.

Étapes suivantes

Pour afficher les sauvegardes que vous avez créées, passez à Mise en route 5 : affichage de vos tâches de sauvegarde et vos points de récupération.

Mise en route 5 : affichage de vos tâches de sauvegarde et vos points de récupération

Avec AWS Backup, vous pouvez consulter l'état et d'autres détails de l'activité de sauvegarde et de restauration dans les AWS services que vous utilisez.

Sur le AWS Backup tableau de bord, vous pouvez gérer les plans de sauvegarde, créer des sauvegardes à la demande, restaurer des sauvegardes et consulter l'état des tâches de sauvegarde et de restauration.

Rubriques

Affichage du statut des tâches de sauvegarde

Utilisez le AWS Backup tableau de bord pour consulter rapidement l'état de vos activités de sauvegarde et de restauration.

Pour afficher le statut de la tâche de sauvegarde

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, sélectionnez Dashboard (Tableau de bord).
3. Pour afficher l'état de vos tâches de sauvegarde, choisissez Backup jobs details (Détails des tâches de sauvegarde). Vous accédez alors à la page Tâches de sauvegarde, sur laquelle vous pouvez consulter des tables contenant des tâches de sauvegarde et de restauration.
4. Vous pouvez filtrer les tâches affichées en fonction de leur date de création. Par exemple, les tâches créées au cours des dernières 24 heures, de la dernière semaine ou des 30 derniers jours. Vous pouvez également définir le nombre de tâches à afficher par page en choisissant l'icône d'engrenage.

Affichage de toutes les sauvegardes d'un coffre

Suivez les étapes ci-dessous pour afficher les sauvegardes qui ont été créées dans un coffre-fort spécifié dans AWS Backup.

Afficher toutes les sauvegardes d'un coffre-fort

1. Sur la AWS Backup console, dans le volet de navigation, sélectionnez Backup vaults.

2. Choisissez le coffre-fort que vous avez utilisé lors de la création d'une sauvegarde à la demande ou d'une sauvegarde planifiée, et consultez toutes les sauvegardes qui ont été créées dans ce coffre-fort.

> **Note**
>
> Chaque sauvegarde possède un Statut, qui est généralement Terminé. Si, pour une raison ou une autre, il ne AWS Backup parvient pas à supprimer une sauvegarde conformément à la configuration de son cycle de vie, elle marque cette sauvegarde comme expirée. Le stockage consommé par les sauvegardes Expirées vous est facturé et vous devriez les supprimer.

Affichage des détails des ressources protégées

Sur la page Protected resources (Ressources protégées), vous pouvez explorer les détails des ressources qui sont sauvegardées dans AWS Backup.

Pour afficher les ressources protégées

1. Sur la AWS Backup console, dans le volet de navigation, sélectionnez Ressources protégées.
2. Affichez les AWS ressources qui sont sauvegardées. Choisissez une ressource dans la liste afin de consulter vos sauvegardes pour cette ressource.

Étapes suivantes

Pour restaurer un point de récupération que vous avez affiché, passez à Mise en route 6 : restauration d'une sauvegarde.

Mise en route 6 : restauration d'une sauvegarde

Une fois qu'une ressource a été sauvegardée au moins une fois, elle est considérée comme protégée et peut être restaurée à l'aide de AWS Backup. Suivez ces étapes pour restaurer une ressource à l'aide de la console AWS Backup .

Pour plus d'informations sur les paramètres de restauration pour des services spécifiques ou sur la restauration d'une sauvegarde à l'aide de l'API AWS CLI ou de l' AWS Backup API, consultez Restoring a Backup.

Pour restaurer une ressource

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Ressources protégées et l'ID de ressource à restaurer.
3. Une liste de vos points de récupération, indiquant également le type de ressource, est triée par valeur ID de ressource. Choisissez une ressource pour ouvrir la page Détails de la ressource.
4. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
5. Spécifiez les paramètres de restauration. Les paramètres de restauration indiqués sont spécifiques au type de ressource sélectionné.

   > **Note**
   >
   > Si vous ne conservez qu'une seule sauvegarde, vous pouvez uniquement restaurer vers le statut du système de fichiers au moment où vous avez effectué cette sauvegarde. Vous ne pouvez pas restaurer vers des sauvegardes incrémentielles antérieures.

   Pour obtenir des instructions sur la restauration de ressources spécifiques, consultez Restauration d'une sauvegarde.
6. Pour Restaurer le rôle, choisissez Rôle par défaut.

   > **Note**
   >
   > Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle est créé pour vous avec les autorisations appropriées.
7. Choisissez Restore backup.

   Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

> **Note**
>
> Lorsque vous effectuez une restauration pour restaurer des éléments spécifiques au sein d'une instance Amazon EFS, vous pouvez les restaurer dans un système de fichiers nouveau ou existant. Si vous restaurez les éléments dans un système de fichiers existant, AWS Backup crée un nouveau répertoire Amazon EFS à partir du répertoire racine pour contenir les éléments. La hiérarchie complète des éléments spécifiés est conservée dans le répertoire de récupération. Par exemple, si le répertoire A contient les sous-répertoires B, C et D, il AWS Backup conserve la structure hiérarchique lorsque A, B, C et D sont restaurés.
> Vous pouvez effectuer une restauration Amazon EFS partielle dans un système de fichiers existant ou sur un nouveau système de fichiers, mais chaque tentative de restauration crée un nouveau répertoire de récupération hors du répertoire racine pour contenir les fichiers restaurés. Si vous tentez plusieurs restaurations pour le même chemin d'accès, plusieurs répertoires contenant les éléments restaurés peuvent exister.

Pour restaurer une instance Amazon EFS

Si vous restaurez une instance Amazon EFS, vous pouvez effectuer une Restauration complète, qui restaure l'ensemble du système de fichiers. Vous pouvez également restaurer des fichiers et des répertoires spécifiques à l'aide de la Restauration au niveau de l'élément (les restaurations au niveau des éléments ont des limites). Consultez Restauration d'un système de fichiers EFS pour plus d'informations). Pour plus d'informations sur la restauration d'autres types de ressources, consultez Restauration d'une sauvegarde.

> **Note**
>
> Pour restaurer une instance Amazon EFS, vous devez « Autoriser » `backup:startrestorejob`.

Pour obtenir des informations détaillées sur la restauration d'une récupération, consultez Restauration d'une sauvegarde.

Étapes suivantes

Avec AWS Backup Audit Manager, vous pouvez auditer votre activité et vos ressources de sauvegarde. Vous pouvez également créer des rapports que vous pouvez utiliser comme preuve

de vos tâches de sauvegarde, de restauration et de copie. Pour créer un rapport, consultez Mise en route 7 : création d'un rapport d'audit.

Mise en route 7 : création d'un rapport d'audit

DansMise en route 5 : affichage de vos tâches de sauvegarde et vos points de récupération, vous avez observé votre activité de sauvegarde dans les vues AWS Backup Dashboard, Backup Vault et Protected Resources. Toutefois, ces vues sont dynamiques et seront mises à jour en fonction de la date à laquelle vous les consulterez. Ces vues ne constituent pas nécessairement la meilleure preuve de la conformité continue aux exigences et aux contrôles de protection des données de votre organisation au fil du temps.

Au cours de cette étape, vous allez créer un rapport de tâche de sauvegarde à la demande à l'aide AWS Backup d'Audit Manager.

AWS Backup Audit Manager fournit une variété de rapports d'audit au format CSV, JSON ou aux deux formats quotidiennement et à la demande à votre compartiment Amazon S3. Vous pouvez vérifier la conformité de votre activité et de vos ressources de sauvegarde par rapport à un certain nombre de contrôles personnalisables. Vous pouvez recevoir des rapports sur vos tâches de sauvegarde, de copie et de restauration. Le rapport des tâches de sauvegarde prouve que vos tâches de sauvegarde ont bien eu lieu.

Voici un exemple de plan de sauvegarde.


```
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC00000",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee77800000",
      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-
b489-4301-83ac-4b7dd7200000",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e6abcde",
      "creationDate": "2021-07-14T23:53:47.229Z",
      "completionDate": "2021-07-15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5aabcde",
```

```
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 8589934592,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/
AWSBackupDefaultServiceRole"
    }
  ]
}
```

Pour créer un rapport de sauvegarde (y compris un rapport de sauvegarde à la demande), vous devez d'abord créer un plan de rapport pour automatiser vos rapports et les envoyer dans un compartiment Amazon S3.

Un plan de rapport nécessite que vous disposiez d'un compartiment Amazon S3 pour recevoir vos rapports. Pour obtenir des instructions sur la configuration d'un nouveau compartiment S3, consultez Étape 1 : Créer votre premier compartiment S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour créer un plan de rapport

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Choisissez Créer un plan de rapport.
4. Sélectionnez Sauvegarder le rapport de la tâche dans la liste déroulante.
5. Pour Nom du plan de rapport, entrez **`TestBackupJobReport`**.
6. Pour Format de fichier, choisissez CSV et JSON.
7. Pour Nom du compartiment S3, sélectionnez la destination de vos rapports dans la liste déroulante.
8. Choisissez Créer un plan de rapport.

Ensuite, vous devez autoriser votre compartiment S3 à recevoir un rapport de AWS Backup. AWS Backup Audit Manager génère automatiquement une politique d'accès S3 pour vous.

Pour afficher et appliquer cette stratégie d'accès

1. Dans le volet de navigation de gauche, choisissez Rapports.

2. Sous Nom du plan de rapport, choisissez le nom de votre plan de rapport (`TestBackupJobReport`).
3. Choisissez Modifier.
4. Choisissez Afficher la stratégie d'accès pour le compartiment S3.
5. Choisissez Copier les autorisations.
6. Choisissez Modifier la politique du compartiment pour modifier la politique de votre compartiment S3 de destination afin de lui permettre de recevoir vos rapports de tâches de sauvegarde.
7. Copiez ou ajoutez les autorisations à la politique du compartiment S3 de destination.

Créez ensuite votre premier rapport de tâche de sauvegarde.

Pour créer un rapport de sauvegarde à la demande

1. Dans le volet de navigation de gauche, choisissez Rapports.
2. Sous Nom du plan de rapport, choisissez le nom de votre plan de rapport (`TestBackupJobReport`).
3. Choisissez Créer un rapport à la demande.

Enfin, consultez votre rapport.

Pour afficher votre rapport

1. Dans le volet de navigation de gauche, choisissez Rapports.
2. Sous Nom du plan de rapport, choisissez le nom de votre plan de rapport (`TestBackupJobReport`).
3. Dans la section Tâches du rapport, choisissez le Lien S3. Cette étape vous emmène vers votre compartiment S3 de destination.
4. Choisissez Téléchargement.
5. Ouvrez le rapport à l'aide du programme que vous utilisez pour travailler avec des fichiers CSV ou JSON.

Étapes suivantes

Pour nettoyer vos ressources de démarrage et éviter des frais indésirables, passez à Mise en route 8 : nettoyage des ressources.

Mise en route 8 : nettoyage des ressources

Après avoir effectué toutes les tâches dans Commencer avec AWS Backup, vous pouvez nettoyer ce que vous avez créé afin d'éviter la facturation de frais inutiles.

Rubriques

Étape 1 : Supprimer les AWS ressources restaurées

Pour supprimer les AWS ressources que vous avez restaurées depuis un point de récupération, telles que les volumes Amazon Elastic Block Store (Amazon EBS) ou les tables Amazon DynamoDB, vous utilisez la console de ce service. Par exemple, pour supprimer un système de fichiers Amazon Elastic File System (Amazon EFS), utilisez la console Amazon EFS.

> **Note**
>
> Ces informations se rapportent aux ressources restaurées et pas aux points de récupération stockés dans un coffre-fort de sauvegarde.

Étape 2 : Supprimer le plan de sauvegarde

Si vous ne souhaitez pas créer de sauvegardes planifiées, vous devez supprimer vos plans de sauvegarde. Avant de pouvoir supprimer un plan de sauvegarde, vous devez supprimer toutes les attributions de ressources de ce plan de sauvegarde.

Suivez les étapes suivantes pour supprimer un plan de sauvegarde :

Pour supprimer un plan de sauvegarde

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup plans (Plans de sauvegarde).
3. Sur la page Backup plans (Plans de sauvegarde), choisissez le plan de sauvegarde que vous souhaitez supprimer. Vous accédez alors à la page des détails de cette sauvegarde.
4. Pour supprimer les affectations de ressources pour votre plan, cochez la case d'option en regard du nom de l'affectation, puis choisissez Delete (Supprimer).
5. Pour supprimer le plan de sauvegarde, sélectionnez Delete (Supprimer) dans le coin supérieur droit de la page.
6. Sur la page de confirmation, saisissez le nom du plan, puis choisissez Delete plan (Supprimer le plan).

Étape 3 : Supprimer les points de récupération

Ensuite, vous pouvez supprimer les points de récupération de sauvegarde qui se trouvent dans votre coffre-fort de sauvegarde.

Supprimer les points de récupération

1. Sur la AWS Backup console, dans le volet de navigation, sélectionnez Backup vaults.
2. Sur la page Backup vaults (Coffres-forts de sauvegarde), choisissez le coffre-fort de sauvegarde dans lequel vous avez stocké les sauvegardes.
3. Vérifiez le point de récupération et choisissez Supprimer.
4. Si vous supprimez plusieurs points de récupération, procédez comme suit :

    a. Si votre liste contient une sauvegarde continue, choisissez de conserver ou de supprimer vos données de sauvegarde continue.

    b. Pour supprimer tous les points de récupération répertoriés, tapez **`delete`**, puis choisissez Supprimer le point de restauration.

    Gardez l'onglet du navigateur ouvert jusqu'à ce qu'une bannière verte s'affiche en haut de la page. La fermeture prématurée de cet onglet mettra fin au processus de suppression et

risque de laisser certains des points de récupération que vous souhaitiez supprimer. Pour plus d'informations, consultez Suppression des sauvegardes.

Étape 4 : Supprimer le coffre-fort de sauvegarde

Le coffre-fort de sauvegarde par défaut ne peut généralement pas être supprimé. Toutefois, si un ou plusieurs autres coffres-forts sont présents dans une région, le coffre-fort de sauvegarde par défaut de cette région peut être supprimé à l'aide de l' AWS CLI.

Vous pouvez supprimer des coffres-forts autres que ceux par défaut une fois que toutes les sauvegardes (points de récupération) qu'ils contiennent ont été supprimées. Pour ce faire, sélectionnez Supprimer dans le coffre-fort vide.

Étape 5 : Supprimer le plan de rapport

Votre plan de rapport envoie automatiquement un nouveau rapport tous les jours. Pour l'en empêcher, supprimez le plan de rapport.

Pour supprimer le plan de rapport

1. Sur la AWS Backup console, dans le volet de navigation, choisissez Reports.
2. Sous Nom du plan de rapport, choisissez le nom de votre plan de rapport.
3. Sélectionnez Delete (Supprimer).
4. Entrez le nom de votre plan de rapport, puis choisissez Supprimer le plan de rapport.

Étape 6 : Supprimer les rapports

Vous pouvez supprimer vos rapports en suivant les instructions relatives à la Suppression d'un seul objet pour chacun de vos rapports. Si vous n'avez plus besoin de votre compartiment S3 de destination, après avoir supprimé tous les objets du compartiment, vous pouvez le supprimer en suivant les instructions dans Suppression d'un compartiment.

Gestion des sauvegardes à l'aide de plans de sauvegarde

Dans AWS Backup, un plan de sauvegarde est une expression de politique qui définit quand et comment vous souhaitez sauvegarder vos AWS ressources, telles que les tables Amazon DynamoDB ou les systèmes de fichiers Amazon Elastic File System (Amazon EFS). Vous pouvez affecter des ressources à des plans de sauvegarde, puis sauvegarder et conserver AWS Backup automatiquement les sauvegardes de ces ressources conformément au plan de sauvegarde. Vous pouvez créer plusieurs plans de sauvegarde si vous avez des charges de travail avec des exigences de sauvegarde différentes. Par défaut, les fenêtres de sauvegarde sont optimisées par AWS Backup. Vous pouvez personnaliser la fenêtre de sauvegarde dans la console ou par programmation.

AWS Backup stocke efficacement vos sauvegardes périodiques de manière incrémentielle. La première sauvegarde d'une ressource AWS sauvegarde une copie complète de vos données. Pour chaque sauvegarde incrémentielle successive, seules les modifications apportées à vos AWS ressources sont sauvegardées. Les sauvegardes incrémentielles vous permettent de bénéficier de la protection des données grâce aux sauvegardes fréquentes tout en minimisant les coûts de stockage.

AWS Backup gère également de manière fluide le cycle de vie de votre plan de sauvegarde en fonction de vos paramètres de conservation, ce qui vous permet de procéder à des restaurations en cas de besoin.

Les sections suivantes présentent les principes de base de la gestion de votre stratégie de sauvegarde dans AWS Backup.

Rubriques

Création d'un plan de sauvegarde

Vous pouvez créer un plan de sauvegarde à l'aide de la AWS Backup console, de l'API, de la CLI, du SDK ou d'un AWS CloudFormation modèle.

Rubriques

- Création de plans de sauvegarde à l'aide de la console AWS Backup
- Création de plans de sauvegarde à l'aide du AWS CLI
- Options et configuration d'un plan de sauvegarde
- AWS CloudFormation modèles de plans de sauvegarde

Création de plans de sauvegarde à l'aide de la console AWS Backup

Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup. Dans le tableau de bord, choisissez Gérer les plans de sauvegarde. Ou, dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.

Options de démarrage

Trois options s'offrent à vous pour votre nouveau plan de sauvegarde :

- Étape 1 : Créer un plan de sauvegarde basé sur un plan existant
- Créez un nouveau plan
- Création de plans de sauvegarde à l'aide du AWS CLI

Dans ce didacticiel, nous allons choisir Créer un nouveau plan. Chaque partie de la configuration comporte un lien vers une section développée plus loin sur la page où vous pouvez naviguer pour plus de détails.

1. Entrez le nom du plan dans Nom du plan de sauvegarde. Vous ne pouvez pas modifier le nom d'un plan une fois celui-ci créé.

   Si vous essayez de créer un plan de sauvegarde identique à un plan existant, vous recevez un `AlreadyExistsException` message d'erreur.
2. Vous pouvez éventuellement ajouter des balises à votre plan de sauvegarde.
3. Configuration de règle de backup : dans la section de configuration des règles de sauvegarde, vous allez définir le calendrier, la fenêtre et le cycle de vie des sauvegardes.
4. Planification :

   a. Entrez un nom de la règle de sauvegarde dans le champ de texte.

   b. Dans le menu déroulant du coffre-fort de sauvegarde, choisissez Par défaut ou Créer un coffre de backup pour créer un nouveau coffre-fort.

c. Dans le menu déroulant de fréquence de sauvegarde, choisissez la fréquence à laquelle vous souhaitez que ce plan crée une sauvegarde.

5. Fenêtre de backup :

   a. L'heure de début par défaut est 00h30 (00h30 dans les 24 heures) dans le fuseau horaire local de votre système.

   b. Commencer dans est défini sur 8 heures par défaut. Vous pouvez modifier ce paramètre pour spécifier une fenêtre de temps pendant laquelle la sauvegarde doit démarrer.

   c. Terminer dans est défini sur 7 jours par défaut.

6. Sauvegardes et point-in-time restaurations continues (PITR): vous pouvez sélectionner Activer les sauvegardes continues pour la point-in-time restauration (PITR). Pour vérifier quelles ressources sont prises en charge pour ce type de sauvegarde, consultez la matrice Disponibilité des fonctionnalités par ressource.

7. Cycle de vie

   a. Stockage à froid : cochez cette case pour permettre aux types de ressources éligibles de passer au stockage à froid conformément au calendrier que vous spécifiez dans la période de rétention totale. Pour utiliser le stockage à froid, vous devez avoir une période de rétention totale de 90 jours ou plus.

   b. Le stockage à froid pour Amazon EBS est l'archive d'instantanés Amazon EBS. Les instantanés transférés vers le niveau de stockage d'archives s'afficheront dans la console en tant que niveau froid. Si le stockage à froid est activé et si votre fréquence de sauvegarde est tous les mois ou moins souvent, votre plan de sauvegarde peut transférer des instantanés EBS.

   c. La période totale de conservation est le nombre de jours pendant lesquels vous stockez votre ressource dans AWS Backup. Il s'agit du nombre total de jours de stockage au chaud plus le stockage au froid.

8. (Facultatif) Utilisez Copier vers la destination pour créer une copie inter-régions des ressources éligibles si vous souhaitez stocker une copie d'une sauvegarde dans une autre Région AWS.

9. (Facultatif) Balises ajoutées aux points de récupération.

10. Lorsque toutes les sections sont définies selon vos spécifications, choisissez Enregistrer la règle de backup.

Création de plans de sauvegarde à l'aide du AWS CLI

Vous pouvez également définir votre plan de sauvegarde dans un document JSON et le fournir à l'aide de la console AWS Backup ou de l' AWS CLI. Le document JSON suivant contient un exemple de plan de sauvegarde qui crée une sauvegarde quotidienne à 1 h 00, heure du Pacifique (l'heure locale s'adapte aux conditions d'heure du jour, de l'heure standard ou de l'heure d'été, le cas échéant). Il supprime automatiquement une sauvegarde au bout d'un an.

```
{
  "BackupPlan":{
    "BackupPlanName":"test-plan",
    "Rules":[
      {
        "RuleName":"test-rule",
        "TargetBackupVaultName":"test-vault",
        "ScheduleExpression":"cron(0 1 ? * * *)",
        "ScheduleExpressionTimezone":"America/Los_Angeles",
        "StartWindowMinutes":integer, // Value is in minutes
        "CompletionWindowMinutes":integer, // Value is in minutes
        "Lifecycle":{
          "DeleteAfterDays":integer, // Value is in days
        }
      }
    ]
  }
}
```

Vous pouvez stocker votre document JSON sous le nom de votre choix. La commande de l'interface de ligne de commande suivante affiche `create-backup-plan` avec un document JSON nommé `test-backup-plan.json` :

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

Notez que si certains systèmes numérotent les jours de la semaine de 0 à 6, nous les numérotons de 1 à 7. Pour plus d'informations, consultez la section Expressions Cron. Pour plus d'informations sur les fuseaux horaires, consultez TimeZonela référence de l'API Amazon Location Service.

Options et configuration d'un plan de sauvegarde

Lorsque vous définissez un plan de sauvegarde dans la AWS Backup console, vous configurez les options suivantes :

Nom du plan de sauvegarde

Le nom du plan de sauvegarde doit être unique.

Si vous choisissez un nom identique à celui d'un plan existant, vous recevez un message d'erreur.

Règles de sauvegarde

Les plans de sauvegarde comportent une ou plusieurs règles de sauvegarde. Pour ajouter des règles de sauvegarde à un plan de sauvegarde ou pour modifier des règles existantes dans un plan de sauvegarde :

1. Dans le volet de navigation de gauche de la AWS Backup console, sélectionnez Backup plans.
2. Sous Nom du plan de sauvegarde, sélectionnez un plan de sauvegarde.
3. Dans la section Règles de sauvegarde :
   - Pour ajouter une règle de sauvegarde, choisissez Ajouter une règle de sauvegarde.
   - Pour modifier une règle de sauvegarde existante, sélectionnez une règle, puis choisissez Modifier.

> **Note**
>
> Si vous disposez d'un plan de sauvegarde comportant plusieurs règles et que les délais des deux règles se chevauchent, AWS Backup optimise la sauvegarde et effectue une sauvegarde pour la règle dont la durée de conservation est la plus longue. L'optimisation prend en compte la fenêtre de démarrage complète, pas seulement le moment où la sauvegarde quotidienne est effectuée.

Chaque règle de sauvegarde comprend les éléments suivants.

Nom de la règle de sauvegarde

Les noms des règles de sauvegarde sont sensibles à la casse. Il doivent contenir entre 1 et 50 caractères alphanumériques ou traits d'union.

Backup frequency (Fréquence de sauvegarde)

La fréquence de sauvegarde détermine la fréquence à AWS Backup laquelle une sauvegarde instantanée est créée. Avec la console, vous pouvez choisir comme fréquence toutes les heures, toutes les 12 heures, une fois par jour, une fois par semaine ou une fois par mois. Vous pouvez également créer une expression cron qui crée des sauvegardes d'instantanés toutes les heures. À l'aide de la AWS Backup CLI, vous pouvez planifier des sauvegardes de snapshots toutes les heures.

Si vous sélectionnez une sauvegarde hebdomadaire, vous pouvez indiquer le jour de la semaine où elle doit avoir lieu. Si vous sélectionnez une sauvegarde mensuelle, vous pouvez choisir un jour spécifique du mois.

Vous pouvez également cocher la case Activer les sauvegardes continues pour les ressources prises en charge pour créer une règle de sauvegarde continue compatible avec la point-in-time restauration (PITR). Contrairement aux sauvegardes instantanées, les sauvegardes continues vous permettent d'effectuer des point-in-time restaurations. Pour en savoir plus sur les sauvegardes continues, consultez Récupération ponctuelle.

Fenêtre de sauvegarde

Une fenêtre de sauvegarde se compose de l'heure à laquelle la fenêtre de sauvegarde commence et de la durée en heures de cette fenêtre. Les tâches de sauvegarde sont démarrées dans cette fenêtre. Les paramètres par défaut de la console sont les suivants :

- 0 h 30, heure locale au fuseau horaire de votre système (0 h 30 dans les systèmes fonctionnant 24 heures sur 24)
- Commencer dans 8 heures
- Terminer dans 7 jours

  (Le paramètre Terminer dans ne s’applique pas aux ressources Amazon FSx.)

Vous pouvez personnaliser la fréquence de sauvegarde et l'heure de début de la fenêtre de sauvegarde à l'aide d'une expression cron. Pour voir les six champs des expressions AWS cron, consultez la section Expressions cron du guide de l'utilisateur Amazon CloudWatch Events. Deux exemples d'expressions AWS cron sont `15 * ? * * *` (effectuer une sauvegarde toutes les heures

15 minutes après l'heure) et `0 12 * * ? *` (effectuer une sauvegarde tous les jours à midi UTC). Pour consulter un tableau d'exemples, cliquez sur le lien précédent et faites défiler la page vers le bas.

AWS Backup évalue les expressions cron entre 00:00 et 23:59. Si vous créez une règle de sauvegarde pour « toutes les 12 heures », mais que vous indiquez une heure de début ultérieure à 11 h 59, elle ne sera exécutée qu'une fois par jour.

Les sauvegardes et point-in-time restaurations continues (PITR) font référence aux modifications enregistrées au fil du temps ; elles ne peuvent donc pas être planifiées à l'aide d'une expression temporelle ou cron.

> **Note**
>
> En général, les services de AWS base de données ne peuvent pas démarrer les sauvegardes 1 heure avant ou pendant leur fenêtre de maintenance et Amazon FSx ne peut pas démarrer les sauvegardes 4 heures avant ou pendant leur fenêtre de maintenance ou leur fenêtre de sauvegarde automatique (Amazon Aurora est exempté de cette restriction de fenêtre de maintenance). Les sauvegardes d'instantanés planifiées pendant ces périodes échoueront. Une exception se produit lorsque vous choisissez d'utiliser AWS Backup à la fois pour les sauvegardes d'instantanés et pour les sauvegardes continues d'un service pris en charge. AWS Backup planifie automatiquement les fenêtres de sauvegarde pour éviter les conflits. Consultez la section Point-in-Time Recovery pour obtenir une liste des services pris en charge et des instructions sur la manière de les utiliser AWS Backup pour effectuer des sauvegardes continues.

Règles de sauvegarde se chevauchant

Il peut arriver qu'un plan de sauvegarde contienne plusieurs règles qui se chevauchent. Lorsque les fenêtres de démarrage de différentes règles se chevauchent, AWS Backup conserve la sauvegarde conformément à la règle avec la période de conservation la plus longue. Par exemple, considérez un plan de sauvegarde comportant deux règles :

1. Sauvegarde toutes les heures, avec une fenêtre de démarrage sous 1 heure et une rétention pendant 1 jour.
2. Sauvegarde toutes les 12 heures, avec une fenêtre de démarrage sous 8 heures et une rétention pendant 1 semaine.

Après 24 heures, la deuxième règle crée deux sauvegardes (car la période de rétention est plus longue). La première règle crée huit sauvegardes (car la fenêtre de démarrage sous 8 heures de la seconde règle empêche l'exécution de plusieurs sauvegardes toutes les heures). En particulier :

Au cours de cette fenêtre de démarrage	Cette règle crée 1 sauvegarde
De minuit à 8 h	12 heures
8 à 9	Par heure
9 à 10	Par heure
10 à 11	Par heure
11 à 12	Par heure
De midi à 20 h	12 heures
8 à 9	Par heure
9 à 10	Par heure
10 à 11	Par heure
11 h à minuit	Par heure

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste `CREATED` jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à`RUNNING`) ou jusqu'à ce que le statut de la tâche passe à `EXPIRED` (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Cycle de vie et niveaux de stockage

Les sauvegardes sont stockées pendant le nombre de jours que vous spécifiez, connu sous le nom de cycle de vie des sauvegardes. Les sauvegardes peuvent être restaurées jusqu’à la fin de leur cycle de vie.

Il s'agit de la période de rétention totale définie dans la section du cycle de vie de la configuration des règles de sauvegarde dans la AWS Backup console.

Si vous utilisez AWS CLI, cela est défini à l'aide du paramètre `DeleteAfterDays`. La période de rétention des instantanés peut aller de 1 jour à 100 ans (ou indéfiniment si vous n'en entrez pas), tandis que celle des sauvegardes continues peut aller de 1 jour à 35 jours. La date de création d'une sauvegarde correspond à la date de début de la tâche de sauvegarde, et non à la date à laquelle elle s'est terminée. Si votre tâche de sauvegarde ne se termine pas à la même date de début, utilisez la date à laquelle elle a commencé pour calculer les périodes de rétention.

Les sauvegardes sont conservées dans un niveau de stockage. Chaque niveau entraîne des coûts de stockage et de restauration différents, comme indiqué dans la Tarification d'AWS Backup. Chaque sauvegarde est créée et stockée dans un espace de stockage à chaud. En fonction de la durée de conservation de votre sauvegarde, vous souhaiterez peut-être passer à un niveau moins coûteux appelé stockage à froid. Disponibilité des fonctionnalités par ressource affiche les ressources dotées de cette fonctionnalité facultative.

Console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Créez ou modifiez un plan de sauvegarde.
3. Dans la section sur le cycle de vie de la configuration des règles de sauvegarde, cochez la case Déplacer les sauvegardes du stockage à chaud au stockage à froid.
4. (Facultatif) Si Amazon EBS est l'une des ressources que vous sauvegardez et que votre fréquence de sauvegarde est tous les mois ou moins souvent, vous pouvez les faire passer au niveau froid à l'aide de l'archivage des instantanés EBS.
5. Entrez une valeur (en jours) indiquant que vous souhaitez que vos sauvegardes restent dans un espace de stockage chaud. AWS Backup recommande au moins 8 jours.
6. Entrez une valeur (en jours) pour la période totale de conservation. La différence entre la période totale de conservation et le temps passé en stockage à chaud sera le nombre de jours pendant lesquels les sauvegardes resteront en stockage à froid.

AWS CLI

1. Utiliser `create-backup-plan` ou `update-backup-plan`.
2.

3. Incluez le paramètre booléen `OptInToArchiveForSupportedResources` pour les ressources EBS.
4. Incluez le paramètre `MoveToColdStorageAfterdays`.
5. Utilisez le `DeleteAfterDays` paramètre. Cette valeur doit être 90 (jours) plus la valeur que vous avez saisie pour `MoveToColdStorageAfterDays`.

Le stockage à froid est actuellement disponible pour les types de ressources suivants :

Type de ressource	Sauvegarde incrémentielle ou complète en stockage à froid
AWS CloudFormation	Incrémentielle
DynamoDB avec les fonctionnalités avancées	Complète ; aucune sauvegarde incrémentielle à aucun niveau
Amazon EBS (à l'aide de l'archive d'instant anés EBS)	Complète ; les sauvegardes incrémentielles deviendront complètes après la transition.
Amazon EFS	Incrémentielle
Bases de données SAP HANA s'exécutant sur des instances Amazon EC2	Incrémentielle
Amazon Timestream	Incrémentielle
Machines virtuelles VMware	Incrémentielle

Une fois que vous avez activé la transition vers le stockage à froid via la console ou la ligne de commande, les conditions suivantes sont remplies pour les sauvegardes en stockage à froid (ou en archive) :

- Les sauvegardes transférées doivent être stockées dans un entrepôt frigorifique pendant au moins 90 jours, en plus du temps passé dans un stockage à chaud. AWS Backup exige que la durée de conservation soit prolongée de 90 jours par rapport au réglage « transition au froid après plusieurs jours ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

- Certains services prennent en charge les sauvegardes incrémentielles. Pour les sauvegardes incrémentielles, vous devez disposer d'au moins une sauvegarde complète à chaud. AWS Backup vous recommande de définir vos paramètres de cycle de vie de manière à ne pas déplacer votre sauvegarde vers un stockage à froid avant au moins 8 jours. Si la sauvegarde complète est transférée trop tôt vers le stockage à froid (par exemple, une transition vers le stockage à froid après 1 jour), une autre sauvegarde complète à chaud AWS Backup sera créée.
- Pour les types de ressources qui prennent en charge les sauvegardes incrémentielles, AWS Backup transfère les données du stockage à chaud vers le stockage à froid si les données transférées ne sont plus référencées par les sauvegardes à chaud. Les données des sauvegardes conservées dans un stockage à froid qui ne sont référencées que par d'autres sauvegardes à froid sont facturées au prix du niveau de stockage à froid. Les autres sauvegardes continuent au tarif du niveau de stockage à chaud.

Coffre-fort de sauvegarde

Un coffre-fort de sauvegarde est un conteneur dans lequel vous pouvez organiser vos sauvegardes. Les sauvegardes créées par une règle de sauvegarde sont organisées dans le coffre-fort de sauvegarde que vous spécifiez dans la règle de sauvegarde. Vous pouvez utiliser les coffres-forts de sauvegarde pour définir la clé de chiffrement AWS Key Management Service (AWS KMS) qui est utilisée pour chiffrer les sauvegardes dans le coffre-fort de sauvegarde et pour contrôler l'accès aux sauvegardes dans le coffre-fort de sauvegarde. Vous pouvez également ajouter des balises aux coffres-forts de sauvegarde pour mieux les organiser. Si vous ne souhaitez pas utiliser le coffre-fort par défaut, vous pouvez en créer un. Pour step-by-step obtenir des instructions sur la création d'un coffre-fort de sauvegarde, consultezÉtape 3 : Créer un coffre-fort de sauvegarde.

Copier vers les régions

Dans le cadre de votre plan de sauvegarde, vous pouvez également créer une copie de sauvegarde dans une autre Région AWS. Pour plus d'informations sur les copies de sauvegardes, consultez Création de copies de sauvegardes entre Régions AWS.

Lorsque vous définissez une copie de sauvegarde, vous configurez les options suivantes :

Région de destination

La région de destination de la copie de sauvegarde.

(Paramètres avancés) Coffre-fort de sauvegarde

Le coffre-fort de sauvegarde de destination pour la copie.

(Paramètres avancés) Rôle IAM

Rôle IAM AWS Backup utilisé lors de la création de la copie. Le rôle doit également être AWS Backup répertorié comme une entité de confiance, ce qui AWS Backup permet d'assumer le rôle. Si vous choisissez Par défaut et que le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle est créé pour vous avec les autorisations appropriées.

(Paramètres avancés) Cycle de vie

Spécifie le moment d'effectuer la transition de la copie de sauvegarde vers le stockage à froid et le moment d'expiration (suppression) de la copie. Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

Expiration indique le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid .

Balises ajoutées aux points de récupération

Les balises que vous répertoriez ici sont automatiquement ajoutées aux sauvegardes lorsqu'elles sont créées.

Balises ajoutées aux plans de sauvegarde

Ces balises sont associées au plan de sauvegarde lui-même afin de vous aider à organiser et effectuer le suivi de votre plan de sauvegarde.

Paramètres de sauvegarde avancés

Permet des sauvegardes cohérentes par rapport à l'application pour les applications tierces s'exécutant sur des instances Amazon EC2. Actuellement, AWS Backup prend en charge les sauvegardes Windows VSS. AWS Backup exclut certains types d'instances Amazon EC2 des sauvegardes Windows VSS. Pour plus d'informations, consultez Création de sauvegardes Windows VSS.

AWS CloudFormation modèles de plans de sauvegarde

Nous fournissons deux exemples de AWS CloudFormation modèles à titre de référence. Le premier modèle crée un plan de sauvegarde simple. Le second modèle autorise les sauvegardes VSS dans un plan de sauvegarde.

> **Note**
>
> Si vous utilisez la fonction du service par défaut, remplacez *fonction du service* par `AWSBackupServiceRolePolicyForBackup`.

```
Description: backup plan template to back up all resources daily at 5am UTC, and tag
 all recovery points with backup:daily.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        BackupPlanRule:
          - RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"
    DependsOn: BackupVaultWithDailyBackups
```

```
DDBTableWithDailyBackupTag:
  Type: "AWS::DynamoDB::Table"
  Properties:
    TableName: "TestTable"
    AttributeDefinitions:
      - AttributeName: "Album"
        AttributeType: "S"
    KeySchema:
      - AttributeName: "Album"
        KeyType: "HASH"
    ProvisionedThroughput:
      ReadCapacityUnits: "5"
      WriteCapacityUnits: "5"
    Tags:
      - Key: "backup"
        Value: "daily"

BackupRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: "Allow"
          Principal:
            Service:
              - "backup.amazonaws.com"
          Action:
            - "sts:AssumeRole"
    ManagedPolicyArns:
      - "arn:aws:iam::aws:policy/service-role/service-role"

TagBasedBackupSelection:
  Type: "AWS::Backup::BackupSelection"
  Properties:
    BackupSelection:
      SelectionName: "TagBasedBackupSelection"
      IamRoleArn: !GetAtt BackupRole.Arn
      ListOfTags:
        - ConditionType: "STRINGEQUALS"
          ConditionKey: "backup"
          ConditionValue: "daily"
    BackupPlanId: !Ref BackupPlanWithDailyBackups
```

```
    DependsOn: BackupPlanWithDailyBackups
```

```
Description: backup plan template to enable Windows VSS and add backup rule to take
 backup of assigned resources daily at 5am UTC.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        AdvancedBackupSettings:
          - ResourceType: EC2
            BackupOptions:
              WindowsVSS: enabled
        BackupPlanRule:
          - RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"

    DependsOn: BackupVaultWithDailyBackups
```

Affectation de ressources à un plan de sauvegarde

L'affectation des ressources indique quelles ressources AWS Backup seront protégées à l'aide de votre plan de sauvegarde. AWS Backup vous propose à la fois des paramètres par défaut simples et des contrôles précis pour affecter des ressources à votre plan de sauvegarde. Chaque fois que votre plan de sauvegarde est exécuté, il analyse toutes Compte AWS les ressources qui correspondent à vos critères d'attribution des ressources. Ce niveau d'automatisation vous permet de définir votre plan de sauvegarde et l'affectation des ressources une seule fois. AWS Backup fait abstraction du travail de recherche et de sauvegarde de nouvelles ressources correspondant à l'affectation des ressources que vous avez définie précédemment.

Vous pouvez attribuer tous les types de ressources AWS Backup pris en charge que vous avez choisi AWS Backup de gérer. Pour obtenir des instructions sur la manière d'opter pour des types de ressources plus AWS Backup pris en charge, voir Getting started 1 : Service Opt-in.

La AWS Backup console dispose de deux méthodes pour inclure des types de ressources dans un plan de sauvegarde : attribuer explicitement le type de ressource dans un plan de sauvegarde ou inclure toutes les ressources. Consultez les points ci-dessous pour comprendre comment ces sélections fonctionnent avec les activations de service.

- Si les attributions de ressources sont uniquement basées sur des balises, les paramètres d'acceptation du service sont appliqués.
- Si un type de ressource est explicitement attribué à un plan de sauvegarde, il sera inclus dans la sauvegarde même si l'opt-in n'est pas activé pour ce service en particulier. Cela ne s'applique pas à Aurora, Neptune et Amazon DocumentDB. Pour que ces services soient inclus, l'opt-in doit être activé.
- Si le type de ressource et les balises sont spécifiés dans une attribution de ressource, les types de ressources spécifiés sont d'abord filtrés, puis les balises filtrent davantage ces ressources.

  Les paramètres d'abonnement au service sont ignorés pour la plupart des types de ressources. Aurora, Neptune et Amazon DocumentDB nécessitent toutefois un abonnement au service.
- Lorsqu'un compte utilise AWS Backup (crée un coffre de sauvegarde ou un plan de sauvegarde) dans une région, il est automatiquement activé pour tous les types de ressources pris AWS Backup en charge par la région à ce moment-là. Les services pris en charge ajoutés ultérieurement à cette région ne seront pas automatiquement inclus dans un plan de sauvegarde. Vous pouvez choisir d'opter pour ces types de ressources une fois qu'ils seront pris en charge.

- Pour Amazon FSx for NetApp ONTAP, lorsque vous utilisez la sélection de ressources basée sur des balises, appliquez des balises à des volumes individuels plutôt qu'à l'ensemble du système de fichiers.

Votre attribution de ressources peut inclure (ou exclure) des types de ressources et des ressources.

- Un type de ressource inclut toutes les instances ou ressources d'un AWS service ou d'une application tierce AWS Backup pris en charge. Par exemple, le type de ressource DynamoDB fait référence à toutes vos tables DynamoDB.
- Une ressource est une instance unique d'un type de ressource, telle que l'une de vos tables DynamoDB. Vous pouvez spécifier une ressource à l'aide de son ID de ressource unique.

Vous pouvez affiner davantage votre attribution de ressources à l'aide de balises et d'opérateurs conditionnels.

Rubriques

Attribution des ressources à l'aide de la console

Pour accéder à la page Attribuer des ressources :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Choisissez Plans de sauvegarde.
3. Choisissez Créer un plan de sauvegarde.
4. Sélectionnez un modèle dans la liste déroulante Choisir un modèle, puis choisissez Créer un plan.
5. Saisissez un Nom du plan de sauvegarde.
6. Choisissez Créer un plan.
7. Choisissez Attribuer des ressources.

Pour commencer l'attribution des ressources dans la section Général :

1. Saisissez un Nom d'attribution de ressource.
2. Choisissez le Rôle par défaut ou Sélectionner un rôle IAM.

> **Note**
>
> Si vous choisissez un rôle IAM, vérifiez qu'il dispose des autorisations nécessaires pour sauvegarder toutes les ressources que vous allez attribuer. Si votre rôle trouve une ressource qui n'est pas autorisée à sauvegarder, votre plan de sauvegarde échoue.

Pour attribuer vos ressources, dans la section Attribuer des ressources, choisissez l'une des deux options sous Définir la sélection des ressources :

- Inclure tous les types de ressources. Cette option configure votre plan de sauvegarde afin de protéger toutes les ressources AWS Backup prises en charge actuelles et futures attribuées à votre plan de sauvegarde. Utilisez cette option pour protéger rapidement et facilement votre parc de données.

  Lorsque vous choisissez cette option, vous pouvez également Affiner la sélection à l'aide de balises à l'étape suivante.
- Inclure des types de ressources spécifiques. Lorsque vous choisissez cette option, vous devez Sélectionner des types de ressources spécifiques en suivant les étapes suivantes :
  1. À l'aide du menu déroulant Sélectionner des types de ressource, attribuez un ou plusieurs types de ressources.

     > **Important**
     >
     > RDS, Aurora, Neptune et DocumentDB partagent le même Amazon Resource Name (ARN). Le fait de choisir de gérer l'un de ces types de ressources avec AWS Backup les active tous lors de l'attribution à un plan de sauvegarde. Pour affiner votre sélection, utilisez des balises et des opérateurs conditionnels.

     Une fois que vous avez terminé, vous AWS Backup présente la liste des types de ressources que vous avez sélectionnés et son paramètre par défaut, qui est de protéger toutes les ressources pour chaque type de ressource sélectionné.

2. (Facultatif) Si vous souhaitez exclure des ressources spécifiques d'un type de ressource que vous avez sélectionné :

    1. Utilisez le menu déroulant Choisir des ressources et désélectionnez l'option par défaut.
    2. Sélectionnez les ressources spécifiques à attribuer à votre plan de sauvegarde.
3. (Facultatif) Vous pouvez Exclure des ID de ressources spécifiques des types de ressources sélectionnés. Utilisez cette option si vous souhaitez exclure une ou plusieurs ressources, car cela peut être plus rapide que de sélectionner de nombreuses ressources à l'étape précédente. Vous devez inclure un type de ressource avant de pouvoir exclure des ressources de ce type de ressource. Excluez un ID de ressource en procédant comme suit :

    1. Sous Exclure des ID de ressources spécifiques des types de ressources sélectionnés, choisissez un ou plusieurs des types de ressources que vous avez inclus avec Sélectionner des types de ressource.
    2. Pour chaque type de ressource, utilisez le menu Choisir les ressources pour sélectionner une ou plusieurs ressources à exclure.

Outre vos choix précédents, vous pouvez effectuer des sélections encore plus détaillées à l'aide de la fonctionnalité facultative Affiner la sélection à l'aide de balises. Cette fonctionnalité vous permet d'affiner votre sélection actuelle pour inclure un sous-ensemble de vos ressources à l'aide de balises.

Les balises sont des paires clé-valeur que vous pouvez attribuer à des ressources spécifiques pour vous aider à identifier, organiser et filtrer vos ressources. Les balises sont sensibles à la casse. Pour de plus amples informations, veuillez consulter Balisage des ressources AWS dans la section Référence générale d'AWS .

Lorsque vous affinez votre sélection à l'aide de deux balises ou plus, l'effet est une condition AND. Par exemple, si vous affinez votre sélection à l'aide de deux balises, `env: prod` et `role: application`, vous attribuez uniquement des ressources comportant LES DEUX balises à votre plan de sauvegarde.

Pour affiner votre sélection à l'aide de balises :

1. Sous Affiner la sélection à l'aide de balises, choisissez une Clé dans la liste déroulante.
2. Choisissez une Condition pour la valeur dans la liste déroulante.

    - La Valeur fait référence à l'entrée suivante, la valeur de votre paire clé-valeur.

- La Condition peut être `Equals`, `Contains`, `Begins with` ou `Ends with`, ou leur inverse : `Does not equal`, `Does not contain`, `Does not begin with` ou `Does not end with`.

3. Choisissez Valeur dans la liste déroulante.
4. Pour affiner davantage à l'aide d'une autre balise, choisissez Ajouter une balise.

Attribution de ressources par programmation

Vous pouvez définir une attribution de ressources dans un document JSON. Cet exemple d'attribution de ressources affecte toutes les instances Amazon EC2 au plan de sauvegarde *BACKUP-PLAN-ID* :

```
{
  "BackupPlanId":"BACKUP-PLAN-ID",
  "BackupSelection":{
    "SelectionName":"resources-list-selection",
    "IamRoleArn":"arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources":[
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

En supposant que ce JSON est stocké sous le nom `backup-selection.json`, vous pouvez attribuer ces ressources à votre plan de sauvegarde à l'aide de la commande d'interface de ligne de commande suivante :

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

Vous trouverez ci-dessous des exemples d'attribution de ressources, ainsi que le document JSON correspondant. Pour faciliter la lecture de ce tableau, les exemples omettent les champs `"BackupPlanId"`, `"SelectionName"` et `"IamRoleArn"`. Le caractère générique `*` représente zéro ou plusieurs caractères autres que des espaces blancs.

Example Exemple : sélectionner toutes les ressources de mon compte

```
{
  "BackupSelection":{
```

```
    "Resources":[
      "*"
    ]
  }
}
```

Example Exemple : sélectionner toutes les ressources de mon compte, mais exclure les volumes EBS

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ]
  }
}
```

Example Exemple : sélectionnez toutes les ressources étiquetées avec"backup":"true", mais excluez les volumes EBS

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example Exemple : sélectionnez tous les volumes EBS et les instances de base de données RDS marqués avec les deux balises et "backup":"true""stage":"prod"

L'arithmétique booléenne est similaire à celle des politiques IAM, celles dans "Resources" étant combinées à l'aide d'une valeur booléenne OR et celles dans `"Conditions"` combinées avec une valeur booléenne ET.

L'expression `"Resources"` `"arn:aws:rds:*:*:db:*"` sélectionne uniquement les instances de base de données RDS, car il n'existe aucune ressource Aurora, Neptune ou DocumentDB correspondante.

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        },
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"prod"
        }
      ]
    }
  }
}
```

Example Exemple : sélectionnez tous les volumes EBS et les instances RDS marqués avec mais non "backup":"true""stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:rds:*:*:db:*"
    ],
    "Conditions":{
```

```
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example Exemple : sélectionnez toutes les ressources étiquetées avec "key1" et une valeur commençant par "include" mais pas par "key2" et une valeur contenant le mot "exclude"

Vous pouvez utiliser le caractère générique au début, à la fin et au milieu d'une chaîne. Notez l'utilisation du caractère générique (*) dans `include*` et `*exclude*` dans l'exemple ci-dessus. Vous pouvez également utiliser le caractère générique au milieu d'une chaîne, comme indiqué dans l'exemple précédent, `arn:aws:rds:*:*:db:*`.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/key1",
          "ConditionValue":"include*"
        }
      ],
      "StringNotLike":[
        {
          "ConditionKey":"aws:ResourceTag/key2",
          "ConditionValue":"*exclude*"
        }
      ]
    }
```

```
  }
}
```

Example Exemple : sélectionnez toutes les ressources étiquetées avec, à "backup":"true" l'exception des systèmes de fichiers FSx et des ressources RDS, Aurora, Neptune et DocumentDB

Les éléments dans `NotResources` sont combinés à l'aide de la valeur booléenne OR.

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "NotResources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

Example Exemple : sélectionnez toutes les ressources étiquetées avec un tag "backup" et une valeur quelconque

```
{
  "BackupSelection":{
    "Resources":[
      "*"
    ],
    "Conditions":{
      "StringLike":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"*"
        }
      ]
```

```
    }
  }
}
```

Example Exemple : sélectionnez tous les systèmes de fichiers FSx, le cluster Aurora et toutes les ressources étiquetées avec "my-aurora-cluster""backup":"true", à l'exception des ressources étiquetées avec "stage":"test"

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:fsx:*",
      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
    ],
    "ListOfTags":[
      {
        "ConditionType":"StringEquals",
        "ConditionKey":"backup",
        "ConditionValue":"true"
      }
    ],
    "Conditions":{
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Example Exemple : sélectionnez toutes les ressources étiquetées avec une balise, **`"backup":"true"`** à l'exception des volumes EBS étiquetés avec **`"stage":"test"`**

Utilisez deux commandes de l'interface de ligne de commande pour créer deux sélections afin de sélectionner ce groupe de ressources. La première sélection s'applique à toutes les ressources à l'exception des volumes EBS. La deuxième sélection s'applique aux volumes EBS.

```
{
  "BackupSelection":{
    "Resources":[
```

```
      "*"
    ],
    "NotResources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ]
    }
  }
}
```

```
{
  "BackupSelection":{
    "Resources":[
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Conditions":{
      "StringEquals":[
        {
          "ConditionKey":"aws:ResourceTag/backup",
          "ConditionValue":"true"
        }
      ],
      "StringNotEquals":[
        {
          "ConditionKey":"aws:ResourceTag/stage",
          "ConditionValue":"test"
        }
      ]
    }
  }
}
```

Affectation de ressources à l'aide de AWS CloudFormation

Ce end-to-end AWS CloudFormation modèle crée une attribution de ressource, un plan de sauvegarde et un coffre de sauvegarde de destination :

- Un coffre de sauvegarde nommé *CloudFormationTestBackupVault*.
- Un plan de sauvegarde nommé *CloudFormationTestBackupPlan*. Ce plan exécutera deux règles de sauvegarde, qui effectuent toutes deux des sauvegardes tous les jours à midi (UTC) et les conservent pendant 210 jours.
- Une sélection de ressources nommée *BackupSelectionName*.
- • L'attribution des ressources sauvegarde les ressources suivantes :
  - Toute ressource balisée avec la paire clé-valeur `backupplan:dsi-sandbox-daily`.
  - Toute ressource balisée avec la valeur `prod` ou des valeurs commençant par `prod/`.
  - L'attribution des ressources ne sauvegarde pas les ressources suivantes :
    - Tout cluster RDS, Aurora, Neptune ou DocumentDB.
    - Toute ressource balisée avec la valeur `test` ou des valeurs commençant par `test/`.

```
Description: "Template that creates Backup Selection and its dependencies"
Parameters:
  BackupVaultName:
    Type: String
    Default: "CloudFormationTestBackupVault"
  BackupPlanName:
    Type: String
    Default: "CloudFormationTestBackupPlan"
  BackupSelectionName:
    Type: String
    Default: "CloudFormationTestBackupSelection"
  BackupPlanTagValue:
    Type: String
    Default: "test-value-1"
  RuleName1:
    Type: String
    Default: "TestRule1"
  RuleName2:
    Type: String
    Default: "TestRule2"
  ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
  StartWindowMinutes:
    Type: Number
    Default: 60
  CompletionWindowMinutes:
```

```
    Type: Number
    Default: 120
  RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
  MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
  DeleteAfterDays:
    Type: Number
    Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
          - RuleName: !Ref RuleName2
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
              test-recovery-point-key-1: !Ref RecoveryPointTagValue
            Lifecycle:
              MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
              DeleteAfterDays: !Ref DeleteAfterDays
      BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
```

```
    DependsOn: CloudFormationTestBackupVault

  TestRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "backup.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
  BasicBackupSelection:
    Type: 'AWS::Backup::BackupSelection'
    Properties:
      BackupPlanId: !Ref BasicBackupPlan
      BackupSelection:
        SelectionName: !Ref BackupSelectionName
        IamRoleArn: !GetAtt TestRole.Arn
        ListOfTags:
          - ConditionType: STRINGEQUALS
            ConditionKey: backupplan
            ConditionValue: dsi-sandbox-daily
        NotResources:
          - 'arn:aws:rds:*:*:cluster:*'
        Conditions:
          StringEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod
          StringNotEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test
          StringLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod/*
          StringNotLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test/*
```

Quotas relatifs à l'attribution des ressources

Les quotas suivants s'appliquent à une seule attribution de ressources :

- 500 Amazon Resource Name (ARN) sans caractères génériques
- 30 ARN avec des expressions à caractère générique
- 30 conditions
- 30 balises par attribution de ressource (et un nombre illimité de ressources par balise)

Suppression d'un plan de sauvegarde

Vous ne pouvez supprimer un plan de sauvegarde qu'une fois que toutes les sélections de ressources associées ont été supprimées. Ces sélections sont également appelées affectations de ressources. S'ils n'ont pas été supprimés avant la suppression du plan de sauvegarde, la console affiche le message d'erreur suivant : « Les sélections de plan de sauvegarde associées doivent être supprimées avant la suppression du plan de sauvegarde ». Utilisez la console ou utilisez `DeleteBackupSelection`.

La suppression d'un plan de sauvegarde supprime la version actuelle du plan. Les versions actuelles et précédentes, le cas échéant, existent toujours, mais elles ne sont plus répertoriées sur la console sous plans de sauvegarde.

> **Note**
>
> La suppression d'un plan de sauvegarde n’implique pas la suppression des sauvegardes existantes. Les sauvegardes existantes doivent être supprimées dans le coffre-fort de sauvegarde en suivant les étapes dans Suppression des sauvegardes.

Pour supprimer un plan de sauvegarde à l'aide de la AWS Backup console

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation de gauche, sélectionnez Backup plans (Plans de sauvegarde).
3. Choisissez votre plan de sauvegarde dans la liste.
4. Sélectionnez toutes les affectations de ressources qui sont associées au plan de sauvegarde.

5. Sélectionnez Delete (Supprimer).

Mise à jour d'un plan de sauvegarde

Après avoir créé un plan de sauvegarde, vous pouvez modifier le plan : vous pouvez, par exemple, ajouter des balises, ou vous pouvez ajouter, modifier ou supprimer des règles de sauvegarde. Les modifications que vous apportez à un plan de sauvegarde n'ont aucun effet sur les sauvegardes existantes créées par le plan de sauvegarde. Les modifications s'appliquent uniquement aux sauvegardes qui seront créés ultérieurement.

Par exemple, lorsque vous mettez à jour la période de rétention dans une règle de sauvegarde, la période de rétention des sauvegardes créées avant la mise à jour ne change pas. Toutes les sauvegardes créées par cette règle à partir de la modification reflètent la mise à jour de la période de rétention.

Vous ne pouvez pas modifier le nom d'un plan une fois celui-ci créé.

Pour modifier un plan de sauvegarde à l'aide de la AWS Backup console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup plans (Plans de sauvegarde).
3. Dans le deuxième volet, Backup plans, les backplans existants sont affichés. Sélectionnez le lien souligné dans la colonne Nom du plan de sauvegarde pour voir les détails du plan de sauvegarde choisi.
4. Vous pouvez modifier une règle de sauvegarde, afficher les affectations de ressources, consulter les tâches de sauvegarde, gérer les balises ou modifier les paramètres Windows VSS.
5. Pour mettre à jour une règle de sauvegarde, sélectionnez le nom de la règle de sauvegarde.

   Sélectionnez Gérer les balises pour ajouter ou supprimer des balises.

   Sélectionnez Modifier à côté de Paramètres de sauvegarde avancés pour activer ou désactiver Windows VSS.
6. Modifiez le ou les paramètres que vous préférez, puis sélectionnez Enregistrer.

Coffres-forts de sauvegarde

> **Note**
>
> À partir du 9 août 2023, propose AWS Backup une version préliminaire permettant d'utiliser un coffre-fort logiquement espacé. Pour vous inscrire à cette version préliminaire, envoyez une demande par e-mail à <aws-backup-vault-preview@amazon .com>.
> Les fonctionnalités peuvent changer ou être ajustées pendant et après la période de prévisualisation. Lorsque le service devient disponible pour tous (GA), les données et les configurations fournies lors de la version préliminaire ne sont plus disponibles. AWS recommande d'utiliser des données de test plutôt que des données de production avec la version préliminaire.

Dans AWS Backup, un coffre de sauvegarde est un conteneur qui stocke et organise vos sauvegardes.

Lorsque vous créez un coffre-fort de sauvegarde, vous devez spécifier la clé de chiffrement AWS Key Management Service (AWS KMS) qui chiffre certaines des sauvegardes placées dans ce coffre-fort. Le chiffrement des autres sauvegardes est géré par leurs AWS services sources. Pour plus d'informations sur le chiffrement, consultez le graphique dans Chiffrement pour les sauvegardes dans AWS.

Votre compte dispose toujours d'un coffre-fort de sauvegarde par défaut. Si vous avez besoin de clés de chiffrement ou de stratégies d'accès différentes pour différents groupes de sauvegardes, vous pouvez créer plusieurs coffres-forts de sauvegarde.

Cette section fournit une présentation de la gestion des coffres-forts de sauvegarde dans AWS Backup.

Rubriques

Coffres-forts à isolation logique (version préliminaire)

> **Note**
>
> À partir du 9 août 2023, propose AWS Backup une version préliminaire permettant d'utiliser un coffre-fort logiquement espacé. Pour vous inscrire à cette version préliminaire, envoyez une demande par e-mail à <aws-backup-vault-preview@amazon .com>.
> Les fonctionnalités peuvent changer ou être ajustées pendant et après la période de prévisualisation. Lorsque le service devient disponible pour tous (GA), les données et les configurations fournies lors de la version préliminaire ne sont plus disponibles. AWS recommande d'utiliser des données de test plutôt que des données de production avec la version préliminaire.

Présentation

AWS Backup affiche un aperçu d'un type de coffre-fort secondaire qui peut stocker des copies de sauvegardes dans d'autres coffres-forts. Un coffre-fort à isolation logique est un coffre-fort spécialisé qui offre des fonctionnalités de sécurité accrues, en plus de celles d'un coffre-fort de sauvegarde, ainsi que la possibilité de partager l'accès au coffre-fort avec d'autres comptes et organisations afin que le délai de reprise (RTO) soit plus rapide et plus flexible en cas d'incident nécessitant une restauration rapide des ressources.

Les coffres-forts hermétiques sont dotés de fonctionnalités de protection supplémentaires : chacun de ces coffres-forts est chiffré à l'aide d'une AWS clé personnelle, et chaque coffre-fort est doté d'un verrou de coffre-fort réglé en mode conformité.

Vous pouvez choisir de partager un coffre-fort à isolation logique entre des organisations et des comptes afin que les sauvegardes qui y sont stockées puissent être restaurées à partir d'un compte avec lequel le coffre-fort est partagé, si nécessaire.

Il n'y a pas de frais supplémentaires pour le stockage dans des coffres-forts à isolation logique pendant la période de prévisualisation. Les sauvegardes effectuées dans des coffres-forts de sauvegarde standard et les copies entre régions sont toujours facturées aux tarifs publiés (consultez Tarification), même si les copies de ces sauvegardes stockées dans des coffres-forts à isolation logique ne sont pas facturées.

Cas d’utilisation

Un coffre-fort à isolation logique est un coffre-fort secondaire qui fait partie d'une stratégie de protection des données. Ce coffre-fort peut contribuer à améliorer la rétention et la récupération de votre organisation lorsque vous souhaitez un coffre-fort pour vos sauvegardes qui

- est automatiquement configuré avec un verrouillage de coffre-fort en mode conformité.
- Contient des sauvegardes qui peuvent être partagées et restaurées à partir d'un compte différent de celui qui a créé la sauvegarde
- Livré crypté avec une AWS clé personnelle

Les ressources prises en charge dans un coffre-fort à isolation logique incluent

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon EFS
- Amazon RDS

Cette version préliminaire des coffres-forts à isolation logique n'est disponible que dans la région USA Est (Virginie du Nord). Puisque cette fonctionnalité n'est actuellement disponible que dans une seule région, la copie entre régions n'est pas prise en charge pendant cette période de prévisualisation.

Comparaison et contraste avec un coffre-fort de sauvegarde standard

Un coffre-fort de sauvegarde est le type de coffre-fort principal et standard utilisé dans AWS Backup. Chaque sauvegarde est stockée dans un coffre-fort de sauvegarde lors de sa création. Vous pouvez attribuer des politiques basées sur les ressources pour gérer les sauvegardes stockées dans le coffre-fort, telles que le cycle de vie des sauvegardes stockées dans le coffre-fort.

Un coffre-fort à isolation logique est un coffre-fort spécialisé offrant plus de sécurité et un partage flexible pour un délai de reprise (RTO) plus rapide. Ce coffre-fort stocke des copies des sauvegardes initialement créées et stockées dans un coffre-fort de sauvegarde standard.

Les coffres-forts de sauvegarde peuvent être chiffrés à l'aide d'une clé, un mécanisme de sécurité qui limite l'accès aux utilisateurs visés. Ces clés peuvent être gérées par le client ou AWS gérées. En

outre, un coffre-fort de sauvegarde peut être encore plus sécurisé par un verrouillage de coffre-fort ; logiquement, les coffres-forts à isolation logique sont équipés d'un verrouillage de coffre-fort en mode conformité.

Si la AWS KMS clé n'a pas été modifiée manuellement ou définie comme clé gérée par le client (CMK) au moment de la création de la ressource initiale, une sauvegarde ne peut pas être copiée dans un coffre-fort logiquement isolé.

Fonctionnalité	Coffre-fort de sauvegarde	Coffre-fort à isolation logique (version préliminaire)
Création d'une sauvegarde	Lorsqu'une sauvegarde est créée, elle est stockée en tant que point de récupération	Les sauvegardes ne sont pas stockées dans ce coffre-fort lors de leur création
Stockage d'une sauvegarde	Peut stocker les sauvegardes initiales des ressources et les copies des sauvegardes	Peut stocker des copies de sauvegardes provenant d'autres coffres-forts
Sécurité	Peut éventuellement être crypté à l'aide d'une clé (géré par le client ou AWS géré) (Facultatif) Peut être verrouillé avec un verrouillage de coffre-fort	Est chiffré à l'aide d'une clé AWS détenue Est toujours verrouillé à l'aide d'un verrouillage de coffre-fort en mode conformité
Capacité de partage	L'accès peut être géré via des politiques et AWS Organizations Non compatible avec AWS Resource Access Manager	(Facultatif) Peut être partagé entre comptes avec AWS RAM
Restauration	Les sauvegardes peuvent être restaurées par le même compte propriétaire du coffre-fort	Les sauvegardes peuvent être restaurées par un compte différent de celui qui possède la sauvegarde si le coffre-fo

Fonctionnalité	Coffre-fort de sauvegarde	Coffre-fort à isolation logique (version préliminaire)
		rt est partagé avec ce compte distinct
Régions	Disponible dans toutes les régions dans lesquelles AWS Backup elle opère	Disponible dans la région USA Est (Virginie du Nord) lors de la prévisualisation
Ressources	Peut stocker des sauvegardes contenant toutes les ressources AWS Backup prises en charge	Peut stocker des sauvegardes contenant des données Amazon EC2, Amazon EBS, Amazon EFS, Amazon S3 ou Amazon RDS

Création d'un coffre-fort à isolation logique à partir de la console

> **Important**
>
> Une fois le coffre-fort créé, le nom du coffre-fort, le type de coffre-fort et les périodes de rétention minimale et maximale ne peuvent pas être modifiés ; de plus, le verrouillage du coffre-fort ne peut pas être supprimé.
> Lorsque le service sera disponible pour tous, les données et les configurations fournies lors de la version préliminaire ne seront plus disponibles. AWS recommande d'utiliser des données de test plutôt que des données de production avec l'aperçu.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, sélectionnez Coffres-forts.
3. Les deux types de coffres-forts s'affichent. Sélectionnez Créer un nouveau coffre-fort.
4. Saisissez un nom pour votre coffre-fort de sauvegarde. Le nom de votre coffre-fort peut refléter ce que vous allez y stocker, ou faciliter la recherche des sauvegardes dont vous avez besoin. Vous pouvez par exemple nommer le coffre-fort `FinancialBackups`.
5. Sélectionnez la case d'option pour accéder à un coffre-fort à isolation logique.
6. Définissez la Période de conservation minimale.

Cette valeur (en jours, mois ou années) correspond à la durée la plus courte pendant laquelle une sauvegarde peut être conservée dans ce coffre-fort. Les sauvegardes dont la période de rétention est inférieure à cette valeur ne peuvent pas être copiées dans ce coffre-fort.

7. Définissez la Période de conservation maximale.

   Cette valeur (en jours, mois ou années) correspond à la durée la plus longue pendant laquelle une sauvegarde peut être conservée dans ce coffre-fort. Les sauvegardes dont la période de rétention est supérieure à cette valeur ne peuvent pas être copiées dans ce coffre-fort.

8. (Facultatif) Ajoutez des balises qui vous aideront à rechercher et à identifier votre coffre-fort à isolation logique. Par exemple, vous pouvez ajouter une balise `BackupType:Financial`.
9. Sélectionnez Créer un verrouillage de coffre.
10. Passez en revue les paramètres. Si tous les paramètres s'affichent comme prévu, sélectionnez Créer un coffre-fort logiquement isolé.
11. La console vous redirigera vers la page de détails de votre nouveau coffre-fort. Vérifiez que les détails du coffre-fort sont conformes aux attentes.

Affichage des détails du coffre-fort à isolation logique dans la console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Sélectionnez Coffres-forts dans le panneau de navigation de gauche.
3. Sous les descriptions des coffres-forts figurent deux listes, Coffres-forts appartenant à ce compte et Coffres-forts partagés avec ce compte. Sélectionnez l'onglet souhaité pour afficher les coffres-forts.
4. Sous Nom du coffre-fort, cliquez sur le nom du coffre-fort pour ouvrir la page de détails. Vous pouvez consulter le résumé, les points de récupération, les ressources protégées, le partage de compte, la stratégie d'accès et les détails des balises.

Copie depuis un coffre-fort de sauvegarde standard vers un coffre-fort à isolation logique dans la console

Les coffres-forts à isolation logique ne peuvent être que la cible de destination d'une tâche de copie dans un plan de sauvegarde ou une cible pour une tâche de copie à la demande.

Pour lancer une tâche de copie, vous devez avoir

- Un coffre-fort de sauvegarde
- Un coffre-fort à isolation logique
- Une sauvegarde contenant des données Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3 ou Amazon EFS
- L'autorisation `kms:CreateGrant` pour le rôle utilisé afin de créer la copie.
- Aucune sauvegarde chiffrée à l'aide d'une clé AWS gérée dans le cadre de votre travail de copie vers le coffre-fort hermétique

Une fois que vous avez confirmé ce qui précède,

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Sélectionnez Coffres-forts dans le panneau de navigation de gauche.
3. Sur la page détaillée du coffre-fort, tous les points de récupération de ce coffre-fort sont affichés. Cochez la case à côté du point de récupération que vous souhaitez copier.
4. Puis sélectionnez Actions et Copier dans le menu déroulant.
5. Sur l'écran suivant, saisissez les détails de la destination.
   a. La région doit être définie sur USA Est (Virginie du Nord)
   b. Le menu déroulant du coffre-fort de sauvegarde de destination affiche les coffres-forts de destination éligibles. Sélectionnez-en un avec le type `logically air-gapped vault`
6. Sélectionnez Copier une fois que tous les détails sont définis selon vos préférences.

Sur la page Tâches de la console, vous pouvez sélectionner des tâches de copie pour voir les tâches de copie en cours.

Pour plus d'informations, consultez Copie d'une sauvegarde, Sauvegarde entre régions et Sauvegarde entre comptes.

Partage d'un coffre-fort à isolation logique à partir de la console

> **Note**
>
> Seuls les comptes dotés de certains privilèges IAM peuvent partager et gérer le partage de comptes.

Vous pouvez l'utiliser AWS RAM pour partager un coffre-fort isolé de manière logique avec d'autres comptes que vous désignez. Pour partager en utilisant AWS RAM, assurez-vous de disposer des éléments suivants :

- Deux comptes ou plus pouvant accéder AWS Backup
- Un compte qui a l'intention de partager dispose des autorisations de RAM nécessaires. L'autorisation `ram:CreateResourceShare` est nécessaire pour cette procédure. La politique `AWSResourceAccessManagerFullAccess` contient toutes les autorisations liées à RAM nécessaires.
- Au moins un coffre-fort à isolation logique

Pour partager un coffre-fort à isolation logique

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Sélectionnez Coffres-forts dans le panneau de navigation de gauche.
3. Sous les descriptions des coffres-forts figurent deux listes, Coffres-forts appartenant à ce compte et Coffres-forts partagés avec ce compte. Sélectionnez la liste souhaitée pour afficher les coffres-forts.
4. Sous Nom du coffre-fort, cliquez sur le nom du coffre-fort à isolation logique pour ouvrir la page de détails.
5. Le volet partage de compte indique avec quels comptes le coffre-fort est partagé.
6. Pour commencer à partager avec un autre compte ou pour modifier des comptes déjà partagés, sélectionnez Gérer le partage.

AWS RAM la console s'ouvre lorsque l'option Gérer le partage est sélectionnée. Pour connaître les étapes à suivre pour partager une ressource à l'aide de la AWS RAM, consultez la section Création d'un partage de ressources dans la AWS RAM.

Assurez vous de disposer des autorisations appropriées. Backup Administrator IAM Policy [AWSBackupFullAccess] et Backup Operator IAM Policy [AWSBackupOperatorAccess] contiennent les autorisations requises pour consulter les comptes partagés ; toutefois, le rôle que vous utilisez pour partager nécessite les autorisations d'écriture de Resource Access Manager pour partager le compte depuis la RAM, telles que. `ram:CreateResourceShare`

Le compte invité à accepter une invitation afin de recevoir un partage dispose de 12 heures pour accepter l'invitation. Consultez Acceptation et rejet des invitations de partage de ressources dans le Guide de l'utilisateur AWS RAM.

Si les étapes de partage sont terminées et acceptées, la page récapitulative du coffre-fort s'affichera sous Partage de compte = « Partagé – voir le tableau de partage de compte ci-dessous ».

Restauration d'une sauvegarde à partir d'un coffre-fort à isolation logique avec la console

Vous pouvez restaurer une sauvegarde stockée dans un coffre-fort à isolation logique à partir du compte propriétaire du coffre-fort ou de tout compte avec lequel le coffre-fort est partagé.

Consultez Restauration d'une sauvegarde pour en savoir plus sur comment restaurer un point de récupération.

Suppression des détails du coffre-fort à isolation logique dans la console

> **Important**
>
> Lorsque le service sera disponible pour tous, les données et les configurations fournies lors de la version préliminaire ne seront plus disponibles. AWS recommande d'utiliser des données de test plutôt que des données de production avec l'aperçu.

Consultez Supprimer un coffre-fort de sauvegarde pour supprimer un coffre-fort. Les coffres-forts ne peuvent pas être supprimés s'ils contiennent encore des sauvegardes (points de récupération). Assurez-vous que le coffre-fort ne contient aucune sauvegarde avant de lancer une opération de suppression.

Coffres-forts à isolation logique via l'interface de ligne de commande/l'API

Vous pouvez l'utiliser AWS CLI pour effectuer des opérations par programmation pour des coffres-forts à espacement logique. Chaque CLI est spécifique au AWS service dont elle provient. Les commandes liées au partage sont précédées par `aws ram` ; toutes les autres commandes doivent être précédées par `aws backup`.

Création

L'exemple de commande de l'interface de ligne de commande suivant `CreateLogicallyAirGappedBackupVault` peut être modifié pour créer un coffre-fort de sauvegarde à isolation logique :

```
aws backup create-logically-air-gapped-backup-vault \
--region us-east-1 \
--backup-vault-name sampleName \
--min-retention-days 7 \
--max-retention-days 35 \
--creator-request-id 123456789012-34567-8901 // optional
```

View details (Afficher les détails)

L'exemple de commande de l'interface de ligne de commande suivant `DescribeBackupVault` peut être modifié pour obtenir des informations sur un coffre :

```
aws backup describe-backup-vault \
--region us-east-1  \
--backup-vault-name testvaultname
```

Partager

> **Note**
>
> Seuls les comptes disposant d'autorisations IAM suffisantes peuvent partager et gérer le partage de comptes.

Vous pouvez partager un coffre-fort à isolation logique via AWS Resource Access Manager (RAM), un service qui aide les utilisateurs à partager des ressources.

AWS RAM utilise la commande CLI`create-resource-share`. L'accès à cette commande n'est disponible que pour les comptes d'administrateur disposant d'autorisations suffisantes. Consultez Création d'un partage de ressources dans AWS RAM pour les étapes de l'interface de ligne de commande.

Les étapes 1 à 4 sont effectuées avec le compte propriétaire du coffre-fort à isolation logique. Les étapes 5 à 8 sont effectuées avec le compte avec lequel le coffre-fort à isolation logique sera partagé.

1. Connectez-vous au compte propriétaire OU demandez à un utilisateur de votre organisation disposant d'informations d'identification suffisantes d'accéder au compte source afin d'effectuer ces étapes.

   - Si un partage de ressources a déjà été créé et que vous souhaitez y ajouter une ressource supplémentaire, utilisez plutôt la commande `associate-resource-share` de l'interface de ligne de commande avec l'ARN du nouveau coffre-fort.

2. Récupérez les informations d'identification d'un rôle disposant d'autorisations suffisantes pour les partager via RAM. Saisissez-les dans l'interface de ligne de commande.

   - L'autorisation `ram:CreateResourceShare` est nécessaire pour cette procédure. La politique AWSResourceAccessManagerFullAccesscontient toutes les autorisations liées à la RAM.

3. Utilise create-resource-share.

   a. Incluez l'ARN du coffre-fort à isolation logique.

   b. Exemple d'entrée :

```
aws ram create-resource-share \
--name MyLogicallyAirGappedVault \
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1
 \
--principals 123456789012 \
--region us-east-1
```

   Exemple de sortie :

```
{
   "resourceShare":{
      "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
      "name":"MyLogicallyAirGappedVault",
      "owningAccountId":"123456789012",
      "allowExternalPrincipals":true,
      "status":"ACTIVE",
      "creationTime":"2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
   }
}
```

4. Copiez l'ARN du partage de ressources dans la sortie (nécessaire pour les étapes suivantes). Donnez l'ARN à l'opérateur du compte que vous invitez à recevoir le partage.
5. Obtenir l'ARN du partage de ressources

   a. Si vous n'avez pas effectué les étapes 1 à 4, obtenez-les auprès resourceShareArn de la personne qui l'a fait.

   b. Exemple : `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`
6. Dans l'interface de ligne de commande, utilisez les informations d'identification du compte du destinataire.
7. Recevez une invitation à partager des ressources avec `get-resource-share-invitations`. Pour plus d'informations, consultez Acceptation et refus des invitations dans le Guide de l'utilisateur AWS RAM .
8. Acceptez l'invitation sur le compte de destination (de récupération).

   - Utiliser `accept-resource-share-invitation` (ou également `reject-resource-share-invitation`).

Liste

La commande `ListBackupVaults` de l'interface de ligne de commande peut être modifiée pour répertorier tous les coffres-forts détenus par le compte et présents dans celui-ci :

```
aws backup list-backup-vaults \
--region us-east-1
```

Pour répertorier uniquement les coffres-forts à isolation logique, ajoutez le paramètre

```
--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

Pour répertorier les coffres-forts partagés avec le compte, utilisez

```
aws backup list-backup-vaults \
--region us-east-1 \
--by-shared
```

Texte

Un coffre-fort à isolation logique ne peut être que la cible d'une tâche de copie d'une sauvegarde, et non la cible d'une tâche de sauvegarde initiale. Utilisez `StartCopyJob` pour copier une sauvegarde existante dans un coffre-fort de sauvegarde vers un coffre-fort à isolation logique.

Le rôle utilisé pour créer la tâche de copie vers le coffre-fort à isolation logique doit contenir l'autorisation `kms:CreateGrant`.

Exemple d'entrée de l'interface de ligne de commande :

```
aws backup start-copy-job \
--region us-east-1 \
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567 \
--source-backup-vault-name sourcevaultname \
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-
vault:destinationvaultname \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

Restaurer

Une fois qu'une sauvegarde a été partagée depuis un coffre-fort à isolation logique vers votre compte, vous pouvez utiliser `StartRestoreJob` pour la restaurer. Exemple d'entrée de l'interface de ligne de commande :

```
aws backup start-restore-job \
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID \
--metadata {\"availabilityzone\":\"us-east-1d\"} \
--idempotency-token TokenNumber \
--resource-type ResourceType \
--iam-role arn:aws:iam::number:role/service-role/servicerole \
--region us-east-1
```

Suppression

L'exemple de commande de l'interface de ligne de commande suivant `DeleteBackupVault` peut être utilisé pour supprimer un coffre-fort. Un coffre-fort ne peut être supprimé que s'il ne contient aucune sauvegarde (point de récupération).

```
aws backup delete-backup-vault
```

```
--region us-east-1
--backup-vault-name testvaultname
```

Les autres options programmatiques disponibles incluent :

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

Création d'un coffre-fort de sauvegarde

Vous devez créer au moins un coffre-fort avant de créer un plan de sauvegarde ou de démarrer une tâche de sauvegarde.

Lorsque vous utilisez la AWS Backup console pour la première fois dans un Région AWS, la console crée automatiquement un coffre-fort par défaut.

Toutefois, si vous utilisez AWS Backup le AWS CLI AWS SDK ou AWS CloudFormation, aucun coffre par défaut n'est créé. Vous devez créer votre propre coffre-fort.

Autorisations nécessaires

Vous devez disposer des autorisations suivantes pour créer un coffre-fort de sauvegarde à l'aide de AWS Backup.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:RetireGrant",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource":
 "arn:aws:kms:region:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup:CreateBackupVault"
      ],
      "Resource": "arn:aws:backup:region:444455556666:backup-vault:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "backup-storage:MountCapsule"
      ],
      "Resource": "*"
    }
  ]
}
```

Création d'un coffre-fort de sauvegarde (console)

Pour step-by-step obtenir des instructions sur la création d'un coffre-fort de sauvegarde à l'aide de la AWS Backup console, reportez-vous Étape 3 : Créer un coffre-fort de sauvegarde au guide de démarrage.

Création d'un coffre-fort de sauvegarde (par programmation)

La AWS Command Line Interface commande suivante crée un coffre de sauvegarde :

```
aws backup create-backup-vault --backup-vault-name test-vault
```

Vous pouvez également préciser les configurations suivantes pour un coffre-fort de sauvegarde.

Nom du coffre-fort de sauvegarde

Les noms des coffres-forts de sauvegarde sont sensibles à la casse. Ils doivent contenir entre 2 et 50 caractères alphanumériques, traits d'union ou traits de soulignement.

AWS KMS clé de chiffrement

La clé de AWS KMS chiffrement protège vos sauvegardes dans ce coffre de sauvegarde. Par défaut, AWS Backup crée une clé KMS pour vous avec l'alias `aws/backup`. Vous pouvez choisir cette clé ou n'importe quelle autre clé de votre compte (les clés KMS entre comptes peuvent être utilisées via l'interface de ligne de commande).

Vous pouvez créer une nouvelle clé de chiffrement en suivant la procédure Création de clés dans le Guide du développeur AWS Key Management Service .

Une fois que vous avez créé un coffre-fort de sauvegarde et défini la clé de AWS KMS chiffrement, vous ne pouvez plus modifier la clé de ce coffre-fort de sauvegarde.

La clé de chiffrement spécifiée dans un AWS Backup coffre s'applique aux sauvegardes de certains types de ressources. Pour plus d'informations sur le chiffrement des sauvegardes, consultez Chiffrement pour les sauvegardes dans AWS Backup dans la section Sécurité. Les sauvegardes de tous les autres types de ressources sont sauvegardées à l'aide de la clé utilisée pour chiffrer la ressource source.

Balises du coffre-fort de sauvegarde

Ces balises sont associées au coffre-fort de sauvegarde afin de vous aider à organiser et effectuer le suivi de votre coffre-fort de sauvegarde.

Définition de stratégies d'accès sur des coffres-forts de sauvegarde

Vous pouvez ainsi attribuer des politiques aux coffres-forts de sauvegarde et aux ressources qu'ils contiennent. AWS Backup L'attribution de politiques vous permet d'accorder l'accès aux utilisateurs afin qu'ils puissent créer des plans de sauvegarde et des sauvegardes à la demande, mais de limiter leur capacité à supprimer des points de récupération après leur création.

Pour plus d'informations sur l'utilisation de politiques permettant d'accorder ou de restreindre l'accès aux ressources, consultez Stratégies basées sur l'identité et Stratégies basées sur une ressource dans le Guide de l'utilisateur IAM. Vous pouvez également contrôler l'accès à l'aide de balises.

Vous pouvez utiliser les exemples de politiques suivants comme guide pour limiter l'accès aux ressources lorsque vous travaillez avec des AWS Backup coffres-forts. Contrairement aux autres politiques basées sur l'IAM, les politiques AWS Backup d'accès ne prennent pas en charge l'ajout d'un caractère générique dans la clé. `Action`

Pour obtenir la liste des ARN (Amazon Resource Names) que vous pouvez utiliser pour identifier des points de récupération pour différents types de ressources, veuillez vous reporter à AWS Backup ARN des ressources afin de connaître les points de récupération spécifiques aux ressources.

Les politiques d'accès au coffre-fort contrôlent uniquement l'accès des utilisateurs aux AWS Backup API. Certains types de sauvegarde, tels que les instantanés Amazon Elastic Block Store (Amazon EBS) et Amazon Relational Database Service (Amazon RDS), sont également accessibles via les API de ces services. Vous pouvez créer des stratégies d'accès distinctes dans IAM qui contrôlent l'accès à ces API afin d'exercer un contrôle total sur l'accès à ces types de sauvegardes.

Quelle que soit la politique d'accès du AWS Backup coffre, l'accès entre comptes pour toute action autre que `backup:CopyIntoBackupVault` sera rejeté, c'est-à-dire qu'il AWS Backup rejettera toute autre demande provenant d'un compte différent du compte de la ressource référencée.

Rubriques

- Rejet de l'accès à un type de ressource dans un coffre-fort de sauvegarde
- Rejet de l'accès à un coffre-fort de sauvegarde
- Rejet de l'accès pour supprimer des points de récupération dans un coffre-fort de sauvegarde

Rejet de l'accès à un type de ressource dans un coffre-fort de sauvegarde

Cette politique rejette l'accès aux opérations d'API spécifiées pour tous les instantanés Amazon EBS d'un coffre-fort de sauvegarde.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:UpdateRecoveryPointLifecycle",
                "backup:DescribeRecoveryPoint",
                "backup:DeleteRecoveryPoint",
                "backup:GetRecoveryPointRestoreMetadata",
                "backup:StartRestoreJob"
            ],
```

```
            "Resource": ["arn:aws:ec2:Region::snapshot/*"]
        }
    ]
}
```

Rejet de l'accès à un coffre-fort de sauvegarde

Cette stratégie rejette l'accès aux opérations d'API spécifiées visant un coffre-fort de sauvegarde.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:DescribeBackupVault",
                "backup:DeleteBackupVault",
                "backup:PutBackupVaultAccessPolicy",
                "backup:DeleteBackupVaultAccessPolicy",
                "backup:GetBackupVaultAccessPolicy",
                "backup:StartBackupJob",
                "backup:GetBackupVaultNotifications",
                "backup:PutBackupVaultNotifications",
                "backup:DeleteBackupVaultNotifications",
                "backup:ListRecoveryPointsByBackupVault"
            ],
            "Resource": "arn:aws:backup:Region:Account ID:backup-vault:backup vault
 name"
        }
    ]
}
```

Rejet de l'accès pour supprimer des points de récupération dans un coffre-fort de sauvegarde

L'accès aux coffres-forts et la possibilité de supprimer des points de récupération qui y sont stockés sont déterminés par l'accès que vous accordez aux utilisateurs.

Suivez les étapes ci-après pour créer une stratégie d'accès basée sur les ressources sur un coffre-fort de sauvegarde qui empêche la suppression de toutes les sauvegardes dans le coffre-fort de sauvegarde.

Pour créer une stratégie d'accès basée sur les ressources pour un coffre-fort de sauvegarde

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation de gauche, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Choisissez un coffre-fort de sauvegarde dans la liste.
4. Dans la section Access policy (Stratégie d'accès), collez l'exemple JSON suivant. Cette stratégie empêche toute personne qui n'est pas le mandataire principal de supprimer un point de récupération dans le coffre-fort de sauvegarde cible.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:userId": [
                       "AAAAAAAAAAAAAAAAAAAAA:",
                       "BBBBBBBBBBBBBBBBBBBBB",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

Pour autoriser les identités IAM de liste à l'aide de leur ARN, utilisez la clé de condition `aws:PrincipalArn` globale dans l'exemple suivant.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                       "arn:aws:iam::112233445566:role/mys3role",
                       "arn:aws:iam::112233445566:user/shaheer",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

Pour plus d'informations sur l'obtention d'un ID unique pour une entité IAM, consultez Obtention de l'identifiant unique dans le Guide de l'utilisateur IAM.

Si vous souhaitez limiter cette possibilité à des types de ressources spécifiques, au lieu de `"Resource": "*"`, vous pouvez inclure explicitement les types de points de récupération à rejeter. Par exemple, pour les instantanés Amazon EBS, modifiez le type de ressource comme suit.

```
"Resource": ["arn:aws:ec2::Region::snapshot/*"]
```

5. Choisissez Attach policy (Attacher une politique).

AWS Backup Verrou de coffre-fort

> **Note**
>
> AWS Backup Vault Lock a été évalué par Cohasset Associates pour une utilisation dans des environnements soumis aux réglementations SEC 17a-4, CFTC et FINRA. Pour plus

d'informations sur le lien entre AWS Backup Vault Lock et ces réglementations, consultez l'évaluation de conformité de Cohasset Associates.

AWS Backup Vault Lock est une fonctionnalité optionnelle d'un coffre-fort de sauvegarde, qui peut être utile pour renforcer la sécurité et le contrôle de vos coffres-forts de sauvegarde. Lorsqu'un verrou est actif en mode conformité et que le délai de grâce est expiré, la configuration du coffre-fort ne peut pas être modifiée ou supprimée par un client, le propriétaire du compte/des données ou AWS. Chaque coffre-fort peut avoir un verrouillage de coffre-fort en place.

AWS Backup garantit que vos sauvegardes sont disponibles pour vous jusqu'à l'expiration de leur période de conservation. Si un utilisateur (y compris l'utilisateur root) tente de supprimer une sauvegarde ou de modifier les propriétés du cycle de vie dans un coffre verrouillé, AWS Backup il refusera l'opération.

- Les coffres-forts verrouillés en mode gouvernance peuvent être verrouillés par les utilisateurs disposant d'autorisations IAM suffisantes.
- Les coffres-forts verrouillés en mode conformité ne peuvent pas être supprimés une fois la période de réflexion (« délai de grâce ») expirée. Pendant le délai de grâce, vous pouvez toujours retirer le verrouillage de coffre-fort et modifier la configuration du verrouillage.

Modes de verrouillage du coffre-fort

Lorsque vous créez un verrouillage de coffre-fort, vous avez le choix entre deux modes : le mode Gouvernance ou le mode Conformité. Le mode Gouvernance est destiné à permettre à un coffre-fort d'être géré uniquement par des utilisateurs disposant de privilèges IAM suffisants. Le mode Gouvernance aide une organisation à répondre aux exigences de gouvernance, en garantissant que seul le personnel désigné peut apporter des modifications à un coffre-fort de sauvegarde. Le mode Conformité est destiné aux coffres-forts de sauvegarde dans lesquels le coffre-fort (et par extension, son contenu) ne devrait jamais être supprimé ou modifié avant la fin de la période de conservation des données. Une fois qu'un coffre-fort en mode conformité est verrouillé, il est immuable, ce qui signifie que le verrou ne peut pas être retiré.

Un coffre-fort verrouillé en mode Gouvernance peut être géré ou supprimé par les utilisateurs disposant des autorisations IAM appropriées.

Un verrouillage de coffre-fort en mode Conformité ne peut être modifié ou supprimé par un utilisateur ou par AWS. Un verrouillage de coffre-fort en mode conformité est soumis à un délai de grâce que vous définissez avant qu'il ne soit verrouillé et ne devienne immuable.

Avantages de Vault Lock

AWS Backup Vault Lock offre plusieurs avantages, notamment :

- Configuration WORM (écriture unique, lecture multiple) pour toutes les sauvegardes que vous stockez et créez dans un coffre-fort de sauvegarde.
- Une couche de défense supplémentaire qui protège les sauvegardes (points de récupération) de vos coffres-forts de sauvegarde contre les suppressions involontaires ou malveillantes.
- Application de périodes de conservation, qui empêchent les suppressions anticipées par les utilisateurs privilégiés (y compris l'utilisateur Compte AWS root) et respectent les politiques et procédures de protection des données de votre organisation.

Verrouillage d'un coffre-fort de sauvegarde à l'aide de la console

Vous pouvez ajouter un verrou de coffre-fort à votre AWS Backup coffre-fort à l'aide de la console Backup.

Pour ajouter un verrouillage à votre coffre-fort de sauvegarde :

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Coffres-forts de sauvegarde. Cliquez sur le lien imbriqué sous les coffres-forts de sauvegarde appelés Verrouillages de coffre.
3. Sous Fonctionnement des verrouillages de coffre ou Verrouillages de coffre, cliquez sur + Créer un verrouillage de coffre.
4. Dans le volet Détails de verrouillage du coffre, choisissez le coffre-fort auquel vous souhaitez appliquer votre verrouillage.
5. Dans Mode de verrouillage de coffre, choisissez le mode dans lequel vous souhaitez que votre coffre-fort soit verrouillé. Pour plus d'informations sur le choix de vos modes, consultez Modes de verrouillage du coffre-fort plus haut sur cette page.
6. Pour la Période de rétention, choisissez les périodes de rétention minimale et maximale (les périodes de rétention sont facultatives). Les nouvelles tâches de sauvegarde et de copie créées

dans le coffre-fort échoueront si elles ne sont pas conformes aux périodes de rétention que vous avez définies ; ces périodes ne s'appliqueront pas aux points de récupération déjà présents dans le coffre-fort.

7. Si vous avez choisi le mode Conformité, une section intitulée Date de début du verrouillage du coffre s'affiche. Si vous avez choisi le mode Gouvernance, rien ne s'affichera et cette étape peut être ignorée.

   En mode Conformité, un verrouillage de coffre-fort dispose d'une période de réflexion entre sa création et le moment où le coffre-fort et son verrouillage deviennent immuables et inchangeables. Vous choisissez la durée de cette période (appelée délai de grâce), mais elle doit être d'au moins 3 jours (72 heures).

   > **Important**
   >
   > Une fois le délai de grâce expiré, le coffre-fort et son verrouillage sont immuables. Il ne peut être modifié ou supprimé par un utilisateur ou par AWS.

8. Lorsque vous êtes satisfait des choix de configuration, cliquez sur Création d'un verrouillage de coffre-fort.
9. Pour confirmer que vous souhaitez créer ce verrouillage dans le mode choisi, tapez `confirm` dans la zone de texte, puis cochez la case confirmant que la configuration est conforme à vos attentes.

Si les étapes ont été effectuées, une bannière « Succès » apparaîtra en haut de la console.

Verrouillage d'un coffre-fort de sauvegarde par programmation

Pour configurer AWS Backup Vault Lock, utilisez l'API`PutBackupVaultLockConfiguration`. Les paramètres à inclure dépendent du mode de verrouillage du coffre-fort que vous souhaitez utiliser. Si vous souhaitez créer un verrouillage de coffre-fort en mode gouvernance, n'incluez pas `ChangeableForDays`. Si ce paramètre est inclus, le verrouillage du coffre-fort sera créé en mode conformité.

Voici un exemple d'interface de ligne de commande pour la création d'un verrouillage de coffre-fort en mode conformité :

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
```

```
        --changeable-for-days 3 \
        --min-retention-days 7 \
        --max-retention-days 30
```

Voici un exemple d'interface de ligne de commande pour la création d'un verrouillage de coffre-fort en mode gouvernance :

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --min-retention-days 7 \
        --max-retention-days 30
```

Vous pouvez configurer quatre options.

1. **`BackupVaultName`**

   Nom du coffre-fort à verrouiller.

2. **`ChangeableForDays`** (à inclure uniquement pour le mode conformité)

   Ce paramètre indique de AWS Backup créer le verrou du coffre-fort en mode de conformité. Omettez ce paramètre si vous avez l'intention de créer le verrouillage en mode gouvernance.

   Cette valeur est exprimée en jours. Le nombre doit être entre 3 et 36 500 ; dans le cas contraire, une erreur sera renvoyée.

   De la création de ce verrouillage de coffre-fort jusqu'à l'expiration de la date spécifiée, le verrouillage du coffre-fort peut être retiré du coffre-fort avec `DeleteBackupVaultLockConfiguration`. Pendant ce temps, vous pouvez également modifier la configuration avec `PutBackupVaultLockConfiguration`.

   À compter de la date spécifiée déterminée par ce paramètre, le coffre-fort de sauvegarde sera immuable et ne pourra être ni modifié ni supprimé.

3. **`MaxRetentionDays`** (facultatif)

   Cette valeur numérique est exprimée en jours. La période de rétention maximale pendant laquelle le coffre-fort conserve ses points de récupération.

   La durée de rétention maximale que vous choisissez doit être conforme aux politiques de rétention des données de votre organisation. Si votre organisation demande que les données soient conservées pendant un certain temps, cette valeur peut être définie sur cette période (en jours).

Par exemple, les données financières ou bancaires peuvent devoir être conservées pendant 7 ans (environ 2 557 jours, selon les années bissextiles).

Si ce n'est pas spécifié, AWS Backup Vault Lock n'appliquera pas de période de conservation maximale. Si cela est spécifié, les tâches de sauvegarde et de copie vers ce coffre-fort dont les périodes de rétention du cycle de vie sont supérieures à la période de rétention maximale échoueront. Les points de récupération déjà enregistrés dans le coffre-fort avant la création de son verrouillage ne sont pas affectés. La période de rétention maximale la plus longue que vous puissiez spécifier est de 36 500 jours (environ 100 ans).

4. **`MinRetentionDays`**(facultatif ; obligatoire pour CloudFormation)

   Cette valeur numérique est exprimée en jours. Il s'agit de la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération. Ce paramètre doit être défini en fonction de la durée requise par votre organisation pour conserver les données. Par exemple, si la réglementation ou la loi exigent que les données soient conservées pendant au moins sept ans, la valeur en jours serait d'environ 2 557, selon les années bissextiles.

   Si ce n'est pas spécifié, AWS Backup Vault Lock n'appliquera pas de période de conservation minimale. Si cela est spécifié, les tâches de sauvegarde et de copie vers ce coffre-fort dont les périodes de rétention du cycle de vie sont inférieures à la période de rétention minimale échoueront. Les points de récupération déjà enregistrés dans le coffre-fort avant le verrouillage du AWS Backup coffre-fort ne sont pas affectés. La période de rétention minimale la plus courte que vous puissiez spécifier est d'un jour.

Vérifiez la configuration Vault Lock d'un AWS Backup coffre-fort de sauvegarde

Vous pouvez consulter les informations de AWS Backup Vault Lock sur un coffre-fort à tout moment en appelant `DescribeBackupVault` ou en utilisant `ListBackupVaults` des API.

Pour déterminer si vous avez appliqué un verrouillage de coffre-fort à un coffre-fort de sauvegarde, appelez `DescribeBackupVault` et vérifiez la propriété `Locked`. Si`"Locked": true`, comme dans l'exemple suivant, vous avez appliqué AWS Backup Vault Lock à votre coffre-fort de sauvegarde.

```
{
    "BackupVaultName": "my_vault_to_lock",
```

```
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 1,
    "Locked": true,
    "MinRetentionDays": 7,
    "MaxRetentionDays": 30,
    "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

La sortie précédente confirme les options suivantes :

1. `Locked`est un booléen qui indique si vous avez appliqué AWS Backup Vault Lock à ce coffre-fort de sauvegarde. `True`signifie que AWS Backup Vault Lock entraîne l'échec des opérations de suppression ou de mise à jour des points de restauration stockés dans le coffre-fort (que vous soyez toujours dans le délai de grâce de refroidissement ou non).
2. `LockDate` est la date et l'heure UTC auxquelles votre délai de grâce de réflexion prend fin. Passé ce délai, vous ne pouvez plus ni supprimer ni modifier le verrouillage de ce coffre-fort. Utilisez n'importe quel convertisseur horaire accessible au public pour convertir cette chaîne en heure locale.

Si `"Locked":false`, comme dans l'exemple suivant, vous n'avez pas appliqué de verrouillage de coffre-fort (ou un verrouillage précédent a été supprimé).

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 3,
    "Locked": false
}
```

Suppression du verrouillage de coffre-fort pendant le délai de grâce (mode Conformité)

Pour supprimer le verrouillage de votre coffre-fort pendant le délai de grâce (le temps qui suit le verrouillage du coffre-fort mais avant votre`LockDate`) à l'aide de la AWS Backup console,

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le menu de navigation de gauche, sous Mon compte, cliquez sur Coffres de sauvegarde, puis sur Backup Vault Lock.
3. Cliquez sur le verrouillage de coffre-fort que vous souhaitez supprimer, puis sur Gérer le verrouillage de coffre.
4. Cliquez sur Supprimer le verrouillage du coffre.
5. Une boîte d'avertissement apparaît, vous demandant de confirmer votre intention de supprimer le verrouillage de coffre-fort. Tapez `confirm` dans la zone de texte, puis cliquez sur Confirmer.

Si toutes les étapes ont été effectuées, une bannière « Succès » apparaîtra en haut de l'écran de la console.

Pour supprimer le verrouillage de votre coffre-fort pendant le délai de grâce à l'aide d'une commande d'interface de ligne de commande, utilisez `DeleteBackupVaultLockConfiguration` comme cet exemple d'interface de ligne de commande :

```
aws backup delete-backup-vault-lock-configuration \
          --backup-vault-name my_vault_to_lock
```

Compte AWS fermeture avec coffre verrouillé

Lorsque vous fermez un site Compte AWS contenant un coffre-fort de sauvegarde AWS et que vous AWS Backup suspendez votre compte pendant 90 jours avec vos sauvegardes intactes. Si vous ne rouvrez pas votre compte pendant ces 90 jours, le contenu de votre coffre-fort de sauvegarde est AWS supprimé, même si AWS Backup Vault Lock était en place.

Considérations supplémentaires en matière de sécurité

AWS Backup Vault Lock ajoute une couche de sécurité supplémentaire à votre défense approfondie de la protection des données. Le verrouillage du coffre-fort peut être combiné avec les autres fonctionnalités de sécurité suivantes :

- Chiffrement de vos points de récupération
- AWS Backup les politiques d'accès au coffre-fort et au point de récupération, qui vous permettent d'accorder ou de refuser des autorisations au niveau du coffre-fort,
- AWS Backup les meilleures pratiques en matière de sécurité, y compris sa bibliothèque de politiques gérées par le client qui vous permet d'accorder ou de refuser des autorisations de sauvegarde et de restauration par le service AWS pris en charge, et
- AWS Backup Audit Manager, qui vous permet d'automatiser les contrôles de conformité de vos sauvegardes par rapport à une liste de contrôles que vous définissez.

  Vous pouvez utiliser Création de frameworks à l'aide de l' AWS Backup API pour le contrôle Les sauvegardes sont protégées par AWS Backup Vault Lock avec AWS Backup Audit Manager pour vous assurer que les ressources que vous souhaitez utiliser sont protégées par un verrouillage de coffre-fort.
- Les mécanismes qui rendent les ressources inactives peuvent avoir un impact sur la capacité à les restaurer. Bien qu'ils ne puissent toujours pas être supprimés dans un coffre verrouillé, ils peuvent être dans un état autre qu'actif. Par exemple, le paramètre Amazon Elastic Compute Cloud qui vous permet de désactiver une AMI peut bloquer temporairement la possibilité de restaurer les sauvegardes des instances EC2. Cela concerne tous les points de restauration EC2, même les sauvegardes touchées par le verrouillage d'un coffre-fort ou par un blocage légal.

  Si une sauvegarde EC2 est désactivée, vous pouvez réactiver une AMI désactivée. Une fois réactivé, il peut être restauré. Pour bloquer la fonctionnalité de désactivation de l'AMI, vous pouvez utiliser des politiques IAM pour ne pas l'autoriser`ec2:DisableImage`.

> **Note**
>
> AWS Backup Vault Lock n'est pas la même fonctionnalité qu'Amazon S3 Glacier Vault Lock, qui est compatible uniquement avec S3 Glacier.

Suppression d'un coffre-fort de sauvegarde

Pour vous protéger contre les suppressions massives accidentelles ou malveillantes, vous ne pouvez supprimer un coffre-fort de sauvegarde dans AWS Backup qu'après avoir supprimé (ou après avoir supprimé le cycle de vie de votre plan de sauvegarde) tous les points de récupération de votre coffre-fort de sauvegarde. Pour supprimer vos points de récupération manuellement, consultez la section Nettoyer les ressources.

Lorsque vous supprimez un coffre-fort de sauvegarde, mettez à jour vos plans de sauvegarde afin qu'ils pointent vers les nouveaux coffres-forts de sauvegarde. La création de la sauvegarde échoue si un plan de sauvegarde pointe vers un coffre-fort de sauvegarde supprimé.

> **Note**
>
> Vous ne pouvez pas supprimer deux coffres-forts de sauvegarde : le coffre-fort de sauvegarde AWS Backup par défaut et le coffre-fort de sauvegarde automatique Amazon EFS.

Pour supprimer un coffre-fort de sauvegarde à l'aide de la AWS Backup console

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Choisissez le nom du coffre de sauvegarde pour ouvrir sa page de détails.
4. Choisissez et supprimer toutes les sauvegardes associées au coffre-fort de sauvegarde.
5. Choisissez Supprimer le coffre. Lorsque vous êtes invité à confirmer, entrez le nom du coffre-fort, puis choisissez Delete Backup vault.

Utilisation des sauvegardes

Une sauvegarde, également appelée point de récupération, représente le contenu d'une ressource, comme par exemple un volume Amazon Elastic Block Store (Amazon EBS) ou une table Amazon DynamoDB, à un instant donné. Le point de restauration est un terme qui fait généralement référence aux différentes sauvegardes des AWS services, telles que les instantanés Amazon EBS et les sauvegardes DynamoDB. Les termes point de récupération et sauvegarde sont utilisés indifféremment.

AWS Backup enregistre les points de restauration dans des coffres-forts de sauvegarde, que vous pouvez organiser en fonction des besoins de votre entreprise. Par exemple, vous pouvez enregistrer un ensemble de ressources contenant des informations financières pour l'exercice 2020. Lorsque vous devez récupérer une ressource, vous pouvez utiliser la AWS Backup console ou le AWS Command Line Interface (AWS CLI) pour rechercher et récupérer la ressource dont vous avez besoin.

Chaque point de récupération présente un ID unique. L'ID unique est à la fin de l'Amazon Resource Name (ARN) du point de récupération. Pour des exemples d'ARN de points de récupération et d'ID uniques, consultez le tableau dans Ressources et opérations.

> **Important**
>
> Pour éviter des frais supplémentaires, configurez votre politique de rétention avec une durée de stockage à chaud d'au moins une semaine. Pour plus d’informations, consultez Mesure, coûts et facturation.

Les sections suivantes proposent une vue d'ensemble des tâches de gestion des sauvegardes élémentaires dans AWS Backup.

Rubriques

- Création d'une sauvegarde
- Copie d'une sauvegarde
- Suppression de sauvegardes
- Modification d'une sauvegarde
- Restauration d'une sauvegarde

- Tests de restauration
- Affichage d'une liste de sauvegardes

Création d'une sauvegarde

Avec AWS Backup, vous pouvez créer des sauvegardes automatiquement à l'aide de plans de sauvegarde ou manuellement en lançant une sauvegarde à la demande.

Création de sauvegardes automatiques

Lorsque les sauvegardes sont créées automatiquement par des plans de sauvegarde, elles sont configurées avec les paramètres de cycle de vie définis dans le plan de sauvegarde. Elles sont organisées dans le coffre-fort de sauvegarde spécifié dans le plan de sauvegarde. Elles sont également marquées avec les balises répertoriées dans le plan de sauvegarde. Pour plus d'informations sur les plans de sauvegarde, consultez Gestion des sauvegardes à l'aide de plans de sauvegarde.

Création de sauvegardes à la demande

Lorsque vous créez une sauvegarde à la demande, vous pouvez configurer ces paramètres pour la sauvegarde en cours de création. Lorsqu'une sauvegarde est créée automatiquement ou manuellement, une tâche de sauvegarde est lancée. Pour savoir comment créer une sauvegarde à la demande, consultez Création d'une sauvegarde à la demande à l'aide de AWS Backup.

Remarque : une sauvegarde à la demande crée une tâche de sauvegarde ; l'état de la tâche de sauvegarde passera à `Running` dans un délai d'une heure (ou lorsque cela est spécifié). Vous pouvez choisir une sauvegarde à la demande si vous souhaitez créer une sauvegarde à un moment autre que celui défini dans un plan de sauvegarde. Une sauvegarde à la demande peut être utilisée, par exemple, pour tester la sauvegarde et les fonctionnalités à tout moment.

Les sauvegardes à la demande ne peuvent pas être utilisées avec la point-in-time restauration (PITR), car une sauvegarde à la demande préserve les ressources dans l'état dans lequel elles se trouvent au moment de la sauvegarde, tandis que la sauvegarde PITR utilise des sauvegardes continues qui enregistrent les modifications au fil du temps.

Statuts des tâches de sauvegarde

Chaque tâche de sauvegarde a un ID unique. Par exemple, `D48D8717-0C9D-72DF-1F56-14E703BF2345`.

Vous pouvez afficher l'état de votre tâche de sauvegarde sur la page Jobs (Tâches) de la console AWS Backup . Les statuts des tâches de sauvegarde incluent `CREATEDPENDING`,`RUNNING`,`ABORTING`,`ABORTED`,`COMPLETED`, `FAILEDEXPIRED`, et`PARTIAL`.

Fonctionnement des sauvegardes incrémentielles

De nombreuses ressources prennent en charge la sauvegarde incrémentielle avec AWS Backup. Une liste complète est disponible dans la section de sauvegarde incrémentielle du tableau Disponibilité des fonctionnalités par ressource.

Bien que chaque sauvegarde effectuée après la première soit incrémentielle (c'est-à-dire qu'elle ne capture que les modifications par rapport à la sauvegarde précédente), toutes les sauvegardes effectuées avec cette sauvegarde AWS Backup conservent les données de référence nécessaires pour permettre une restauration complète. Cela est vrai même si la sauvegarde d'origine (complète) a atteint la fin de son cycle de vie et a été supprimée.

Par exemple, si votre sauvegarde (complète) du premier jour a été supprimée en raison d'une politique de cycle de vie de 3 jours, vous pourrez toujours effectuer une restauration complète avec les sauvegardes des jours 2 et 3. AWS Backup conserve les données de référence nécessaires dès le premier jour pour ce faire.

Accès aux ressources source

AWS Backup a besoin d'accéder à vos ressources sources pour les sauvegarder. Par exemple :

- Pour sauvegarder une instance Amazon EC2, celle-ci peut avoir l'état `stopped` ou `running`, mais pas à l'état `terminated`. Cela est dû au fait qu'une `stopped` instance `running` or peut communiquer avec AWS Backup, mais pas une `terminated` instance.
- Pour sauvegarder une machine virtuelle, son hyperviseur doit avoir le statut de passerelle de sauvegarde `ONLINE`. Pour plus d'informations, consultez Compréhension du statut de l'hyperviseur.
- Pour sauvegarder une base de données Amazon RDS, Amazon Aurora ou un cluster Amazon DocumentDB, ces ressources doivent avoir le statut `AVAILABLE`.
- Pour sauvegarder un Amazon Elastic File System (Amazon EFS), celui-ci doit avoir le statut `AVAILABLE`.
- Pour sauvegarder un système de fichiers Amazon FSx, celui-ci doit avoir le statut `AVAILABLE`. Si le statut est `UPDATING`, la demande de sauvegarde est mise en file d'attente jusqu'à ce que le système de fichiers devienne `AVAILABLE`.

FSx pour ONTAP ne prend pas en charge la sauvegarde de certains types de volumes, notamment les volumes DP (protection des données), les volumes LS (partage de charge), les volumes complets ou les volumes sur des systèmes de fichiers pleins. Pour plus d'informations, consultez Fonctionnement de FSx pour ONTAP avec les sauvegardes.

AWS Backup conserve les sauvegardes créées précédemment conformément à votre politique de cycle de vie, quel que soit l'état de votre ressource source.

Rubriques

- Création d'une sauvegarde à la demande à l'aide de AWS Backup
- Sauvegardes et point-in-time restaurations continues (PITR)
- Sauvegardes Amazon S3
- Sauvegardes de machines virtuelles
- Sauvegarde DynamoDB avancée
- Sauvegardes Amazon Timestream
- Sauvegarde de bases de données SAP HANA sur des instances Amazon EC2
- Sauvegardes Amazon Redshift
- Sauvegardes Amazon Relational Database Service
- AWS CloudFormation empiler des sauvegardes
- Création de sauvegardes Windows VSS
- Amazon EBS et AWS Backup
- Copie de balises sur des sauvegardes
- Arrêt d'une tâche de sauvegarde

Création d'une sauvegarde à la demande à l'aide de AWS Backup

Sur la AWS Backup console, la page Ressources protégées répertorie les ressources qui ont été sauvegardées au AWS Backup moins une fois. Si vous l'utilisez AWS Backup pour la première fois, aucune ressource (telle que les volumes Amazon EBS ou les bases de données Amazon RDS) n'est répertoriée sur cette page. C'est le cas même si une ressource a été affectée à un plan de sauvegarde, si ce plan de sauvegarde n'a pas exécuté de tâche de sauvegarde planifiée au moins une fois.

Remarque : une sauvegarde à la demande commence immédiatement à sauvegarder votre ressource. Vous pouvez choisir une sauvegarde à la demande si vous souhaitez créer une sauvegarde à un moment autre que celui défini dans un plan de sauvegarde. Une sauvegarde à la demande peut être utilisée, par exemple, pour tester la sauvegarde et les fonctionnalités à tout moment.

Les sauvegardes à la demande ne peuvent pas être utilisées avec la point-in-time restauration (PITR), car une sauvegarde à la demande préserve les ressources dans l'état dans lequel elles se trouvent au moment de la sauvegarde, tandis que la sauvegarde PITR utilise des sauvegardes continues qui enregistrent les modifications au fil du temps.

Considérations

- Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle est créé pour vous avec les autorisations appropriées.
- Lorsque les sauvegardes expirent et sont marquées pour suppression dans le cadre de votre politique de cycle de vie, AWS Backup supprime les sauvegardes à un moment choisi au hasard au cours des 8 heures suivantes. Cette fenêtre permet de garantir des performances constantes.
- Pour les ressources Amazon EC2, copie AWS Backup automatiquement les balises de ressources individuelles et de groupe existantes, en plus de toutes les balises que vous ajoutez au cours de cette étape.
- AWS Backup utilise les sauvegardes EC2 avec « aucun redémarrage » comme comportement par défaut. AWS Backup prend actuellement en charge les ressources exécutées sur Amazon EC2, et certains types d'instances ne sont pas pris en charge. Pour plus d’informations, consultez Création de sauvegardes Windows VSS.

Pour créer une sauvegarde à la demande

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le tableau de bord, choisissez Créer une sauvegarde à la demande. Ou, dans le panneau de navigation, choisissez Ressources protégées, puis Créer une sauvegarde à la demande.
3. Pour la page Type de ressource, choisissez le type de ressource que vous souhaitez sauvegarder. Par exemple, choisissez DynamoDB pour les tables Amazon DynamoDB.
4. Choisissez le nom ou l'ID de la ressource à protéger. Par exemple, choisissez le nom de la table DynamoDB pour Amazon DynamoDB.
5. Assurez-vous que Create backup now (Créer une sauvegarde maintenant) est sélectionné.

6. Si le type de ressource prend en charge la transition vers le stockage à froid, le stockage à froid est présent. Pour plus d'informations, consultez la colonne Cycle de vie du stockage à froid dans le tableau Disponibilité des fonctionnalités par ressource.

   Pour spécifier à quel moment cette sauvegarde sera mise en stockage à froid, choisissez Déplacer les sauvegardes du stockage à chaud vers le stockage à froid, puis spécifiez la durée du stockage à chaud.
7. Pour Durée de conservation totale, spécifiez le nombre de jours. Si vous avez spécifié le temps de stockage au froid, la période de conservation est divisée entre le stockage à chaud et le stockage au froid.
8. Sélectionnez un Coffre de sauvegarde existant ou créez-en un. Si vous choisissez Créer un coffre de sauvegarde, une nouvelle page s'ouvre afin que vous puissiez créer un coffre. Une fois que vous avez terminé, vous revenez à la page Créer une sauvegarde à la demande.
9. Pour le rôle IAM, choisissez le rôle par défaut ou un rôle que vous avez créé.
10. Pour attribuer un tag à votre sauvegarde à la demande, développez le champ Tags ajoutés aux points de restauration, choisissez Ajouter un nouveau tag, puis entrez une clé de tag et une valeur de tag.
11. Si le type de ressource est EC2, les paramètres de sauvegarde avancés sont présents. Pour prendre des instantanés cohérents avec les applications à l'aide du service Windows Volume Shadow Copy (VSS), choisissez Windows VSS.
12. Choisissez Create on-demand backup (Créer une sauvegarde à la demande). Cela ouvre la page Tâches, où vous pouvez voir la liste des tâches et consulter le statut des tâches.

Sauvegardes et point-in-time restaurations continues (PITR)

Rubriques

- Considérations relatives au oint-in-time rétablissement

Pour certaines ressources, AWS Backup prend en charge les sauvegardes et point-in-time restaurations continues (PITR) en plus des sauvegardes instantanées.

Avec les sauvegardes continues, vous pouvez restaurer les ressources AWS Backup prises en charge en les rétablissant à l'heure précise de votre choix, avec une seconde de précision (en remontant au maximum 35 jours en arrière). La sauvegarde continue fonctionne en créant d'abord une sauvegarde complète de votre ressource, puis en sauvegardant constamment les journaux de transactions de votre ressource. La restauration PITR fonctionne en accédant à votre sauvegarde complète et en relisant le journal des transactions jusqu'à l'heure indiquée AWS Backup pour la restauration.

Il est également possible d'effectuer des sauvegardes d'instantanés toutes les heures. Les sauvegardes d'instantanés peuvent être stockées pendant 100 ans au maximum. Les instantanés peuvent être copiés pour des sauvegardes complètes ou incrémentielles.

Étant donné que les sauvegardes continues et d'instantanés présentent des avantages différents, nous vous recommandons de protéger vos ressources à l'aide de règles de sauvegarde continues et instantanées.

Remarque : une sauvegarde à la demande commence immédiatement à sauvegarder votre ressource. Vous pouvez choisir une sauvegarde à la demande si vous souhaitez créer une sauvegarde à un moment autre que celui défini dans un plan de sauvegarde. Une sauvegarde à la demande peut être utilisée, par exemple, pour tester la sauvegarde et les fonctionnalités à tout moment.

Les sauvegardes à la demande ne peuvent pas être utilisées avec la point-in-time restauration (PITR), car une sauvegarde à la demande préserve les ressources dans l'état dans lequel elles se trouvent au moment de la sauvegarde, tandis que la sauvegarde PITR utilise des sauvegardes continues qui enregistrent les modifications au fil du temps.

Vous pouvez opter pour des sauvegardes continues pour les ressources prises en charge lorsque vous créez un plan de sauvegarde à AWS Backup l'aide de la AWS Backup console ou de l'API.

Pour activer les sauvegardes continues à l'aide de la console

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.

2. Dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sous Règles de sauvegarde, choisissez Ajouter une règle de sauvegarde.
4. Dans la section Configuration de règle de backup, sélectionnez Activer les sauvegardes continues pour les ressources prises en charge.

Services pris en charge pour la sauvegarde continue/la restauration ponctuelle (PITR)

AWS Backup prend en charge les sauvegardes et point-in-time les restaurations continues pour les services et applications suivants :

Amazon S3

Pour activer la PITR pour les sauvegardes S3, les sauvegardes continues doivent faire partie du plan de sauvegarde.

Bien que la PITR puisse être active dans cette sauvegarde d'origine du compartiment source, les copies de destination entre régions ou entre comptes ne comporteront pas la PITR, et la restauration à partir de ces copies les rétablira la date à laquelle elles ont été créées (les copies seront des copies instantanées) au lieu d'être restaurées à un moment précis.

RDS

Programmes de sauvegarde : lorsqu'un AWS Backup plan crée à la fois des instantanés Amazon RDS et des sauvegardes continues, il AWS Backup planifie intelligemment vos fenêtres de sauvegarde afin de les coordonner avec la fenêtre de maintenance Amazon RDS afin d'éviter les conflits. Pour éviter davantage les conflits, la configuration manuelle de la fenêtre de sauvegarde automatique Amazon RDS n'est pas disponible. RDS prend des instantanés une fois par jour, qu'un plan de sauvegarde prévoie une fréquence de sauvegarde d'instantanés autre qu'une fois par jour.

Paramètres : une fois que vous avez appliqué une règle de sauvegarde AWS Backup continue à une instance Amazon RDS, vous ne pouvez pas créer ou modifier les paramètres de sauvegarde continue pour cette instance dans Amazon RDS ; les modifications doivent être effectuées via la AWS Backup console ou la CLI AWS Backup .

Transfert du contrôle de la sauvegarde continue d'une instance Amazon RDS vers Amazon RDS :

Console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.

2. Dans le panneau de navigation, choisissez Backup plans (Plans de sauvegarde).
3. Supprimez tous les plans de sauvegarde Amazon RDS avec une sauvegarde continue protégeant cette ressource.
4. Choisissez Coffres-forts de sauvegarde. Supprimez le point de récupération des sauvegardes continues de votre coffre-fort de sauvegarde. Vous pouvez également attendre la fin de leur période de conservation, ce qui entraînera AWS Backup la suppression automatique du point de récupération.

Une fois ces étapes terminées, le contrôle continu des sauvegardes de vos ressources AWS Backup sera transféré à Amazon RDS.

AWS CLI

Appelez l'opération de l'API `DisassociateRecoveryPoint`.

Pour en savoir plus, veuillez consulter la section DisassociateRecoveryPoint.

Autorisations IAM requises pour les sauvegardes continues Amazon RDS

- À utiliser AWS Backup pour configurer des sauvegardes continues pour votre base de données Amazon RDS, vérifiez que l'autorisation d'API `rds:ModifyDBInstance` existe dans le rôle IAM défini par la configuration de votre plan de sauvegarde. Pour restaurer les sauvegardes continues Amazon RDS, vous devez ajouter l'autorisation `rds:RestoreDBInstanceToPointInTime` au rôle IAM que vous avez soumis pour la tâche de restauration. Vous pouvez utiliser le `AWS Backup default service role` pour effectuer des sauvegardes et des restaurations.
- Pour décrire la plage de temps disponible pour le point-in-time rétablissement, AWS Backup appelez`rds:DescribeDBInstanceAutomatedBackupsAPI`. Dans la AWS Backup console, vous devez disposer de l'autorisation d'`rds:DescribeDBInstanceAutomatedBackupsAPI` dans votre politique gérée AWS Identity and Access Management (IAM). Vous pouvez utiliser les politiques gérées par `AWSBackupFullAccess` ou `AWSBackupOperatorAccess`. Les deux politiques disposent de toutes les autorisations requises. Pour plus d'informations, consultez Stratégies gérées .

Périodes de conservation : lorsque vous modifiez la période de conservation de votre PITR, AWS Backup appelez `ModifyDBInstance` et appliquez immédiatement cette modification. Si vous avez d'autres mises à jour de la configuration en attente de la prochaine fenêtre de maintenance, la modification de votre période de rétention PITR appliquera également ces mises à jour de la

configuration immédiatement. Pour plus d'informations, consultez `ModifyDBInstance` dans la Référence des API d'Amazon Relational Database Service.

Copies des sauvegardes continues d'Amazon RDS :

- Les tâches de copie d'instantanés incrémentielles sont traitées plus rapidement que les tâches de copie d'instantanés complets. La conservation d'une copie précédente d'un instantané jusqu'à ce que la nouvelle tâche de copie soit terminée peut réduire la durée de la tâche de copie. Si vous choisissez de copier des instantanés à partir d'instances de base de données RDS, il est important de noter que la suppression initiale des copies précédentes entraînera la création de copies instantanées complètes (au lieu de copies incrémentielles). Pour plus d'informations sur l'optimisation des copies, consultez Copie d'instantané incrémentielle dans le Guide de l'utilisateur Amazon RDS.
- Création de copies des sauvegardes continues Amazon RDS : vous ne pouvez pas créer de copies des sauvegardes continues Amazon RDS car AWS Backup Amazon RDS n'autorise pas la copie des journaux de transactions. Il AWS Backup crée plutôt un instantané et le copie à la fréquence spécifiée dans le plan de sauvegarde.

Restaurations : vous pouvez effectuer une point-in-time restauration à l'aide d'Amazon RDS AWS Backup ou d'Amazon RDS. Pour les instructions relatives à AWS Backup la console, consultez Restaurer une base de données Amazon RDS. Pour obtenir des instructions Amazon RDS, consultez Restauration d'une instance de base de données à une date spécifiée dans le Guide de l'utilisateur Amazon RDS.

> **Tip**
>
> Une instance de base de données multi-AZ (zone de disponibilité) définie sur ne `Always On` doit pas avoir de rétention des sauvegardes définie sur zéro. Si des erreurs se produisent, utilisez la AWS CLI commande `disassociate-recovery-point` au lieu de`delete-recovery-point`, puis modifiez le paramètre de rétention sur 1 dans vos paramètres Amazon RDS.

Pour des informations générales sur le fonctionnement avec Amazon RDS, consultez le Guide de l'utilisateur Amazon RDS.

Aurora

Pour activer la sauvegarde continue de vos ressources Aurora, consultez les étapes décrites dans la première section de cette page.

La procédure de restauration d'un cluster Aurora à un instant dans le passé est une variante des étapes de restauration d'un instantané d'un cluster Aurora.

Lorsque vous effectuez une restauration à un instant dans le passé, la console affiche une section heure de restauration. Consultez Restauration d'une sauvegarde continue plus bas sur cette page dans Utilisation des sauvegardes continues.

SAP HANA sur des instances Amazon EC2

Vous pouvez effectuer des sauvegardes continues, qui peuvent être utilisées avec la point-in-time restauration (PITR) (notez que les sauvegardes à la demande préservent les ressources dans l'état dans lequel elles ont été prises, tandis que PITR utilise des sauvegardes continues qui enregistrent les modifications au fil du temps).

Avec les sauvegardes continues, vous pouvez restaurer votre base de données SAP HANA sur une instance EC2 en la rétablissant à l'heure précise de votre choix, avec une seconde de précision (en remontant au maximum 35 jours en arrière). La sauvegarde continue fonctionne en créant d'abord une sauvegarde complète de votre ressource, puis en sauvegardant constamment les journaux de transactions de votre ressource. La restauration PITR fonctionne en accédant à votre sauvegarde complète et en relisant le journal des transactions jusqu'à l'heure indiquée AWS Backup pour la restauration.

Vous pouvez opter pour les sauvegardes continues lorsque vous créez un plan de sauvegarde à AWS Backup l'aide de la AWS Backup console ou de l'API.

Pour activer les sauvegardes continues à l'aide de la console

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sous Règles de sauvegarde, choisissez Ajouter une règle de sauvegarde.
4. Dans la section Configuration de règle de backup, sélectionnez Activer les sauvegardes continues pour les ressources prises en charge.

Une fois que vous avez désactivé le PITR (point-in-timerestauration) pour les sauvegardes de base de données SAP HANA, les journaux continueront d'être envoyés AWS Backup jusqu'à expiration du point de restauration (statut égal à). `EXPIRED`) Vous pouvez passer à un autre emplacement de sauvegarde des journaux dans SAP HANA pour arrêter la transmission des journaux à AWS Backup.

Un point de restauration continue dont l'état est égal à `STOPPED` indique qu'un point de restauration continue a été interrompu ; en d'autres termes, les journaux transmis par SAP HANA à AWS Backup ce point et indiquant les modifications incrémentielles apportées à une base de données présentent une lacune. Les points de récupération qui se produisent pendant cet intervalle de temps ont un statut `STOPPED`..

Pour les problèmes que vous pouvez rencontrer lors des tâches de sauvegardes continues (points de récupération), consultez la section Dépannage de la restauration SAP HANA dans ce guide.

Résultat d'une sauvegarde continue

Vous pouvez utiliser la AWS Backup console pour trouver votre sauvegarde continue.

Pour rechercher une sauvegarde continue à l'aide de la AWS Backup console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Coffres de sauvegarde, puis choisissez votre coffre-fort de sauvegarde dans la liste.
3. Dans la section Sauvegardes, dans la colonne Type de sauvegarde, triez les points de restauration En continu. Vous pouvez également trier par ID de point de récupération pour le préfixe En continu.

Restaurationd'une sauvegarde continue

Pour restaurer une sauvegarde continue à l'aide de la AWS Backup console

- Pendant le processus de restauration PITR, la AWS Backup console affiche une section sur l'heure de restauration. Dans cette section, vous effectuez les opérations suivantes :
  - Choisir de restaurer à la Dernière heure de restauration.
  - Choisir Spécifier la date et l'heure pour entrer vos propres date et heure pendant votre période de rétention.

Pour restaurer une sauvegarde continue à l'aide de l' AWS Backup API

1. Pour Amazon S3, consultez Utiliser l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration S3.
2. Pour Amazon RDS, voir Utiliser l' AWS Backup API, la CLI ou le SDK pour restaurer les points de récupération Amazon RDS.

Arrêt ou suppression des sauvegardes continues

Vous pouvez arrêter la création de sauvegardes continues ou supprimer des sauvegardes spécifiques (point-in-time-recovery ou points PITR).

Si vous souhaitez arrêter les sauvegardes continues, vous devez supprimer la règle de sauvegarde continue de votre plan de sauvegarde. Si vous souhaitez arrêter les sauvegardes continues pour une ou plusieurs ressources, mais pas pour toutes les ressources, créez un nouveau plan de sauvegarde avec la règle de sauvegarde continue pour les ressources que vous souhaitez toujours sauvegarder en continu. Si au contraire vous supprimez uniquement un point de récupération de sauvegarde continue de votre coffre-fort de sauvegarde, votre plan de sauvegarde continuera à exécuter la règle de sauvegarde continue, créant ainsi un nouveau point de récupération.

Cependant, même après avoir supprimé votre règle de sauvegarde continue, AWS Backup mémorise la période de conservation indiquée par votre règle de sauvegarde désormais supprimée. Il supprimera automatiquement votre point de récupération continue de votre coffre-fort de sauvegarde en fonction de la période de rétention que vous avez spécifiée.

Lorsque vous supprimez des points de récupération Amazon RDS, pensez à :

- Une instance de base de données multi-AZ (zone de disponibilité) définie sur ne `Always On` doit pas avoir de rétention des sauvegardes définie sur zéro. Si des erreurs se produisent, utilisez la AWS CLI commande `disassociate-recovery-point` au lieu de`delete-recovery-point`, puis modifiez le paramètre de rétention sur 1 dans vos paramètres Amazon RDS.
- Lorsqu'un point de point-in-time restauration (une sauvegarde créée par une sauvegarde continue) pour Amazon RDS est supprimé, le redémarrage de la base de données est déclenché et les journaux binaires sont désactivés. Pour plus de détails, consultez Période de rétention des sauvegardes dans le Guide de l'utilisateur Amazon RDS.

Lorsque vous supprimez des points de restauration Aurora, prenez en compte les points suivants :

Si cette option est sélectionnée pour un point de restauration Amazon Aurora, AWS Backup définit la période de rétention à 1 jour. Les sauvegardes Aurora ne peuvent pas être complètement supprimées tant que le cluster source n'a pas également été supprimé.

Copie des sauvegardes continues

Si une règle de sauvegarde continue spécifie également une copie entre comptes ou entre régions, AWS Backup prend un instantané de la sauvegarde continue et copie cet instantané dans le coffre-fort de destination. Pour en savoir plus sur la copie de vos points de récupération entre comptes et régions, consultez Copie d'une sauvegarde.

Les sauvegardes continues créent des sauvegardes périodiques conformément à la fréquence définie dans la règle du plan de sauvegarde du compte et/ou de la région de destination.

AWS Backup ne prend pas en charge les copies à la demande de sauvegardes continues.

Modification de votre période de rétention

Vous pouvez l'utiliser AWS Backup pour augmenter ou diminuer la période de rétention de votre règle de sauvegarde continue existante. La période de rétention minimale est de 1 jour. La période de rétention maximale est de 35 jours.

Si vous augmentez votre période de rétention, l'effet est immédiat. Si vous réduisez votre période de conservation, vous AWS Backup attendrez que suffisamment de temps se soit écoulé avant d'appliquer la modification afin de vous protéger contre la perte de données. Par exemple, si vous réduisez votre période de rétention de 35 jours à 20 jours, vous AWS Backup continuerez à conserver 35 jours de sauvegarde continue jusqu'à ce que 15 jours se soient écoulés. Cette conception protège vos 15 derniers jours de sauvegarde au moment où vous avez effectué la modification.

Suppression de la seule règle de sauvegarde continue d'un plan de sauvegarde

Lorsque vous créez un plan de sauvegarde avec une règle de sauvegarde continue, puis que vous supprimez cette règle, AWS Backup mémorise la période de conservation de votre règle désormais supprimée. Il supprimera la sauvegarde continue de votre coffre-fort de sauvegarde à l'expiration de la période de rétention.

Sauvegardes continues superposées sur la même ressource

En général, vous devez protéger chaque ressource à l'aide d'une seule règle de sauvegarde continue. Cela est dû au fait que les sauvegardes continues supplémentaires sont redondantes.

Toutefois, au fur et à mesure que vous augmentez votre parc de sauvegarde, il est possible que plusieurs plans, règles et coffres-forts de sauvegarde se chevauchent sur une seule ressource. AWS Backup gère ces chevauchements comme suit.

Si vous incluez la même ressource dans plusieurs plans de sauvegarde dotés d'une règle de sauvegarde continue, cela ne AWS Backup créera une sauvegarde continue que pour le premier plan de sauvegarde évalué. Il créera des sauvegardes d'instantanés pour tous les autres plans de sauvegarde.

Si vous incluez plusieurs règles de sauvegarde continue dans un seul plan de sauvegarde :

- Si vos règles pointent vers le même coffre de sauvegarde, crée une sauvegarde continue AWS Backup uniquement pour la règle dont la période de conservation est la plus longue. Il ne tient pas compte de toutes les autres règles.
- Si vos règles indiquent différents coffres-forts de sauvegarde, AWS Backup rejette le plan au motif qu'il n'est pas valide.

Considérations relatives au oint-in-time rétablissement

Tenez compte des considérations suivantes en matière de point-in-time rétablissement :

- Retour automatique aux instantanés : si AWS Backup n'est pas en mesure d'effectuer une sauvegarde continue, il essaie plutôt d'effectuer une sauvegarde par instantané.
- Aucune prise en charge des sauvegardes continues à la demande : AWS Backup ne prend pas en charge la sauvegarde continue à la demande, car la sauvegarde à la demande enregistre un moment précis, alors que la sauvegarde continue enregistre les modifications au fil du temps.
- Aucune prise en charge pour la transition vers le stockage à froid : les sauvegardes continues ne prennent pas en charge la transition vers le stockage à froid, car la transition vers le stockage à froid nécessite une période de transition minimale de 90 jours, tandis que les sauvegardes continues ont une période de rétention maximale de 35 jours.
- Restauration de l'activité récente : l'activité Amazon RDS autorise les restaurations jusqu'aux 5 dernières minutes d'activité ; Amazon S3 autorise les restaurations jusqu'aux 15 dernières minutes d'activité.

Sauvegardes Amazon S3

AWS Backup prend en charge la sauvegarde et la restauration centralisées des applications stockant des données dans S3 uniquement ou conjointement avec d'autres AWS services de base de données, de stockage et de calcul. De nombreuses fonctionnalités sont disponibles pour les sauvegardes S3, notamment Backup Audit Manager.

Vous pouvez utiliser une politique de sauvegarde unique AWS Backup pour automatiser de manière centralisée la création de sauvegardes des données de vos applications. AWS Backup organise automatiquement les sauvegardes entre différents AWS services et applications tierces dans un emplacement crypté centralisé (appelé coffre de sauvegarde) afin que vous puissiez gérer les sauvegardes de l'ensemble de votre application via une expérience centralisée. Pour S3, vous pouvez créer des sauvegardes continues, restaurer les données de votre application stockées dans S3 et restaurer les sauvegardes point-in-time en un seul clic.

Avec AWS Backup, vous pouvez créer les types de sauvegardes suivants de vos compartiments S3, notamment des données d'objets, des balises, des listes de contrôle d'accès (ACL) et des métadonnées définies par l'utilisateur :

- Les sauvegardes continues vous permettent de procéder à des restaurations à n'importe quel moment au cours des 35 derniers jours. Les sauvegardes continues d'un compartiment S3 ne doivent être configurées que dans le cadre d'un seul plan de sauvegarde.

  Consultez Récupération ponctuelle pour obtenir une liste des services pris en charge et des instructions sur la manière d'utiliser AWS Backup pour effectuer des sauvegardes continues.
- Les sauvegardes périodiques utilisent des instantanés de vos données pour vous permettre de conserver les données pendant la durée spécifiée, jusqu'à 99 ans. Vous pouvez planifier des sauvegardes périodiques à des fréquences telles que 1 heure, 12 heures, 1 jour, 1 semaine ou 1 mois. AWS Backup effectue des sauvegardes périodiques pendant la fenêtre de sauvegarde que vous définissez dans votre plan de sauvegarde.

  Consultez la section Création d'un plan de sauvegarde pour comprendre comment AWS Backup appliquer votre plan de sauvegarde à vos ressources.

Des copies entre comptes et entre régions sont disponibles pour les sauvegardes S3, mais les copies de sauvegardes continues ne disposent pas de fonctionnalités de point-in-time restauration.

Les sauvegardes continues et périodiques des compartiments S3 doivent toutes deux résider dans le même coffre-fort de sauvegarde.

Pour les deux types de sauvegarde, la première sauvegarde est complète, tandis que les sauvegardes suivantes sont incrémentielles au niveau de l'objet.

> **Note**
>
> Vous devez activer la gestion des versions S3 sur votre compartiment S3 pour pouvoir l'utiliser AWS Backup pour Amazon S3. Nous avons conservé cette condition préalable, car dans AWS , nous recommandons la gestion des versions S3 comme bonne pratique pour la protection des données.
> Nous vous recommandons de définir une période d'expiration du cycle de vie pour vos versions S3. Le fait de ne pas définir de période d'expiration du cycle de vie peut augmenter vos coûts S3, AWS Backup car toutes les versions non expirées de vos données S3 sont sauvegardées et stockées. Pour en savoir plus sur la configuration des politiques de cycle de vie S3, suivez les instructions sur cette page.

Comparaison des types de sauvegarde S3

Votre stratégie de sauvegarde des ressources S3 peut impliquer uniquement des sauvegardes continues, des sauvegardes périodiques (instantanés) ou une combinaison des deux. Les informations ci-dessous peuvent vous aider à choisir ce qui convient le mieux à votre organisation :

Sauvegardes continues uniquement :

- Une fois la première sauvegarde complète de vos données existantes terminée, les modifications apportées aux données de votre compartiment S3 sont suivies au fur et à mesure qu'elles se produisent.
- Les modifications suivies vous permettent d'utiliser le PITR (point-in-time restauration) pendant la période de conservation de la sauvegarde continue. Pour exécuter une tâche de restauration, vous choisissez l'instant dans le passé auquel vous souhaitez effectuer la restauration.
- La période de rétention de chaque sauvegarde continue est de 35 jours au maximum.

Sauvegardes périodiques (instantanés) uniquement, planifiées ou à la demande :

- AWS Backup analyse l'intégralité du compartiment S3, récupère l'ACL et les balises de chaque objet et lance une requête Head pour chaque objet figurant dans le cliché précédent mais introuvable dans le cliché en cours de création.
- La sauvegarde est point-in-time cohérente.
- La date et l'heure de sauvegarde enregistrées correspondent à l'heure à laquelle la traversée du compartiment est AWS Backup terminée, et non à l'heure à laquelle une tâche de sauvegarde a été créée.
- La première sauvegarde d'un compartiment est une sauvegarde complète. Chaque sauvegarde suivante est incrémentielle et représente l'évolution des données depuis le dernier instantané.
- L'instantané créé par la sauvegarde périodique peut avoir une période de rétention allant jusqu'à 99 ans.

Sauvegardes continues associées à des sauvegardes périodiques/d'instantanés :

- Une fois la première sauvegarde complète de vos données existantes (chaque compartiment) terminée, les modifications apportées à votre compartiment sont suivies au fur et à mesure qu'elles se produisent.
- Vous pouvez effectuer une point-in-time restauration à partir d'un point de restauration continu.
- Les instantanés sont point-in-time cohérents.
- Les instantanés sont pris directement depuis le point de récupération continue, ce qui élimine le besoin d'analyser à nouveau un compartiment pour accélérer les processus.
- Les instantanés et les points de récupération continue partagent la même lignée de données ; le stockage des données entre les points de récupération d'instantanés et continue n'est pas dupliqué.

Classes de stockage S3 prises en charge

AWS Backup vous permet de sauvegarder vos données S3 stockées dans les classes de stockage S3 suivantes :

- S3 Standard
- Standard S3 - Accès peu fréquent (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval

- S3 Hiérarchisation intelligente (S3 INT)

Les sauvegardes d'un objet de la classe de stockage S3 Intelligent-Tiering (INT) accèdent à ces objets. Cet accès déclenche S3 Intelligent-Tiering pour déplacer automatiquement ces objets vers Frequent Access.

Les sauvegardes qui accèdent aux niveaux d'accès peu fréquents, y compris les classes S3 Standard - Infrequent Access (IA) et S3 One Zone-IA, sont soumises aux frais de stockage S3 liés à l'accès fréquent (s'applique aux niveaux d'accès peu fréquent ou d'accès instantané aux archives).

À l'exception de Glacier Instant Retrieval, les classes de stockage archivées ne sont pas prises en charge.

Pour plus d'informations sur la tarification du stockage pour Amazon S3, consultez la section Tarification d'Amazon S3.

Considérations AWS Backup relatives à Amazon S3

Les points suivants doivent être pris en compte lors de la sauvegarde des ressources S3 :

- Support ciblé des métadonnées d'objets : AWS Backup prend en charge les métadonnées suivantes : balises, listes de contrôle d'accès (ACL), métadonnées définies par l'utilisateur, date de création d'origine et ID de version. Vous pouvez également restaurer toutes les données et métadonnées sauvegardées, à l'exception de la date de création d'origine, de l'ID de version, de la classe de stockage et des balises électroniques.
- Le nom d'une clé d'objet S3 peut être composé de la plupart des chaînes encodables en UTF-8. Les caractères Unicode suivants sont acceptés : `#x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF` .

  Les noms de clés d'objet qui incluent des caractères ne figurant pas dans cette liste peuvent être exclus des sauvegardes. Pour plus d'informations, consultez la spécification W3C en matière de caractères.
- Transition vers le stockage à froid : la politique AWS Backup de gestion du cycle de vie vous permet de définir le calendrier d'expiration des sauvegardes, mais la transition vers le stockage à froid des sauvegardes S3 n'est actuellement pas prise en charge.
- Les sauvegardes de compartiments S3 contenant de nombreuses versions du même objet créées à la même seconde ne sont pas prises en charge pour le moment.

- Pour les sauvegardes périodiques, AWS Backup faites de votre mieux pour suivre toutes les modifications apportées aux métadonnées de votre objet. Toutefois, si vous mettez à jour une balise ou une liste ACL plusieurs fois en une minute, AWS Backup peut ne pas capturer tous les états intermédiaires.
- AWS Backup ne prend actuellement pas en charge les sauvegardes d'objets chiffrés en SSE-C. AWS Backup ne prend pas non plus en charge actuellement les sauvegardes des configurations de compartiment, y compris la politique, les paramètres, le nom ou le point d'accès des compartiments.
- AWS Backup ne prend actuellement pas en charge les sauvegardes de S3 sur AWS Outposts.

> **Important**
>
> Dans les comptes enregistrant des événements de lecture de données, les compartiments S3 dont CloudTrail les journaux sont activés ont besoin que leurs journaux d'accès soient enregistrés dans un compartiment cible différent ; si les CloudTrail journaux sont enregistrés dans le même compartiment qu'ils enregistrent, une boucle infinie se forme. Cette boucle peut déclencher des frais inattendus et indésirables.
> Pour plus d'informations, consultez la section Événements liés aux données dans le Guide de CloudTrail l'utilisateur.

Fenêtres de fin de sauvegarde S3

Le tableau ci-dessous présente des exemples de compartiments de différentes tailles pour vous aider à estimer le temps d'exécution de la sauvegarde complète initiale d'un compartiment S3. Les durées de sauvegarde varient en fonction de la taille, du contenu, de la configuration et des paramètres de chaque compartiment.

Taille de compartiment	Nombre d'objets	Durée estimée pour terminer la sauvegarde initiale
425 Go (gigaoctets)	135 millions	31 heures
800 To (téraoctets)	670 millions	38 heures
6 Po (pétaoctets)	5 milliards	100 heures

Taille de compartiment	Nombre d'objets	Durée estimée pour terminer la sauvegarde initiale
370 To (téraoctets)	7,5 milliards	180 heures

Autorisations et politiques relatives à la sauvegarde et à la restauration Amazon S3

Pour sauvegarder, copier et restaurer des ressources S3, vous devez disposer des politiques appropriées à votre rôle. Pour ajouter ces politiques, accédez à Politiques gérées par AWS. Ajoutez le AWSBackupServiceRolePolicyForS3Backupet AWSBackupServiceRolePolicyForS3Restoreaux rôles que vous souhaitez utiliser pour sauvegarder et restaurer les compartiments S3.

Si vous ne disposez pas des autorisations suffisantes, demandez au responsable du compte administratif (admin) de votre organisation d'ajouter les politiques aux rôles prévus.

Pour plus d’informations, consultez Politiques gérées et politiques en ligne dans le Guide de l’utilisateur IAM.

AWS Backup pour S3 repose sur la réception d'événements S3 via Amazon EventBridge. Si ce paramètre est désactivé dans les paramètres de notification des compartiments S3, les sauvegardes continues s'arrêteront pour ces compartiments, le paramètre étant désactivé. Pour plus d'informations, consultez la section Utilisation EventBridge.

Bonnes pratiques et considérations financières pour les sauvegardes S3

Bonnes pratiques

Pour les compartiments contenant plus de 300 millions d'objets :

- Pour les compartiments contenant plus de 300 millions d'objets, le taux de sauvegarde peut atteindre 17 000 objets par seconde lors de la sauvegarde complète initiale du compartiment (les sauvegardes incrémentielles auront une vitesse différente) ; les compartiments contenant moins de 300 millions d'objets sont sauvegardés à un rythme proche de 1 000 objets par seconde.
- Des sauvegardes continues sont recommandées.
- Si le cycle de vie des sauvegardes est prévu pour plus de 35 jours, vous pouvez également activer les sauvegardes d'instantanés pour le compartiment dans le même coffre-fort dans lequel vos sauvegardes continues sont stockées.

Considérations relatives aux coûts

- Les politiques de cycle de vie S3 comportent une fonctionnalité optionnelle appelée Supprimer les marqueurs de suppression d'objet arrivés à expiration. Lorsque cette fonctionnalité est supprimée, les marqueurs de suppression, parfois par millions, expirent sans plan de nettoyage. Lorsque des compartiments dépourvus de cette fonctionnalité sont sauvegardés, deux problèmes ont un impact sur le temps et les coûts :
  - Les marqueurs de suppression sont sauvegardés, tout comme les objets. Le temps de sauvegarde et le temps de restauration peuvent être attribués en fonction du rapport entre les objets et les marqueurs de suppression.
  - Chaque objet ou marqueur sauvegardé est soumis à des frais minimum. Chaque marqueur de suppression est facturé de la même manière qu'un objet de 128 Ko.
- Pour les comptes qui effectuent des sauvegardes au moins une fois par jour ou plus fréquemment, il est possible de réaliser des économies en utilisant des sauvegardes continues si les données contenues dans les sauvegardes subissent des modifications minimales entre chaque sauvegarde.
- Les compartiments plus volumineux qui ne changent pas fréquemment peuvent tirer parti des sauvegardes continues, car cela peut se traduire par une réduction des coûts lorsque les analyses de l'ensemble du compartiment ainsi que plusieurs demandes par objet n'ont pas besoin d'être exécutées sur des objets préexistants (objets inchangés par rapport à la sauvegarde précédente).
- Les compartiments contenant plus de 100 millions d'objets et dont le taux de suppression est faible par rapport à la taille globale de la sauvegarde peuvent réaliser des économies grâce à un plan de sauvegarde qui inclut à la fois une sauvegarde continue avec une période de rétention de 2 jours et des instantanés d'une rétention plus longue.
- La durée des sauvegardes périodiques (instantanés) coïncide avec le début du processus de sauvegarde lorsqu'une analyse des compartiments n'est pas nécessaire. Les analyses ne sont pas nécessaires dans un compartiment contenant à la fois une sauvegarde continue et des instantanés, car dans ces cas, les instantanés sont pris à partir d'un point de récupération continue.
- Pour chaque objet d'un seul S3-GIR (Amazon S3 Glacier Instant Retrieval), il AWS Backup effectue plusieurs appels, ce qui entraîne des frais de récupération lors de l'exécution d'une sauvegarde.

  Des coûts de récupération similaires s'appliquent aux compartiments contenant des objets des classes de stockage S3-IA et S3 One Zone-IA.
- AWS KMS CloudTrail, et les CloudWatch fonctionnalités Amazon qui font partie de votre stratégie de sauvegarde peuvent entraîner des coûts supplémentaires au-delà du stockage des données

dans les compartiments S3. Consultez les sections suivantes pour en savoir plus sur ces fonctionnalités :

- Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3 dans le Guide de l'utilisateur Amazon S3.
- Vous pouvez réduire les CloudTrail coûts en excluant les AWS KMS événements et en désactivant les événements de données S3 :
  - Exclure AWS KMS des événements : dans le guide de CloudTrail l'utilisateur, la création d'un parcours dans la console (sélecteurs d'événements de base) permet d'exclure AWS KMS des événements afin de les exclure de votre suivi (le paramètre par défaut inclut tous les événements KMS) :
  - L'option de journalisation ou d'exclusion des événements KMS n'est disponible que si vous journalisez les événements de gestion sur votre journal de suivi. Si vous choisissez de ne pas journaliser les événements de gestion, les événements KMS ne sont pas journalisés, et vous ne pouvez pas modifier les paramètres de journalisation des événements KMS.
  - AWS KMS des actions telles que `EncryptDecrypt`, et génèrent `GenerateDataKey` généralement un grand volume (plus de 99 %) d'événements. Ces actions sont désormais journalisées en tant qu'événements Lecture. Les actions KMS pertinentes de faible volume, telles que `Disable`, `Delete` et `ScheduleKey` (qui comptent généralement moins de 0,5 % du volume des événements KMS) sont journalisées en tant qu'événements Écrire.
  - Pour exclure les événements de volume important tels que `Encrypt`, `Decrypt` et `GenerateDataKey`, tout en continuant de journaliser les événements pertinents tels que `Disable`, `Delete` et `ScheduleKey`, choisissez de journaliser les événements de gestion Écrire et effacez la case à cocher pour Exclure les événements AWS KMS .
  - Désactiver les événements de données S3 : par défaut, les journaux de suivi et les stockages de données d'événement ne journalisent pas les événements de données. Désactivez les événements de données S3 avant votre sauvegarde initiale afin de réduire les coûts.
- Pour réduire les CloudWatch coûts, vous pouvez arrêter d'envoyer CloudTrail des événements aux CloudWatch journaux lorsque vous mettez à jour un journal pour désactiver les paramètres CloudWatch des journaux.

Restauration de sauvegardes S3

Vous pouvez restaurer les données S3 que vous avez sauvegardées AWS Backup à l'aide de la classe de stockage standard S3. Vous pouvez restaurer vos données S3 dans un compartiment existant, y compris le compartiment d'origine. Pendant la restauration, vous pouvez également

créer un nouveau compartiment S3 comme cible de restauration. Vous ne pouvez restaurer les sauvegardes S3 que là Région AWS où se trouve votre sauvegarde.

Vous pouvez restaurer l'intégralité du compartiment S3, ou les dossiers ou objets qu'il contient. AWS Backup restaure la version actuelle de cet objet.

Pour restaurer vos données S3 à l'aide de AWS Backup, consultezRestauration des données S3.

Sauvegardes de machines virtuelles

AWS Backup prend en charge la protection centralisée et automatisée des données pour les machines virtuelles (VM) VMware sur site ainsi que pour les machines virtuelles dans VMware Cloud™ (VMC) sur AWS et VMware Cloud™ (VMC) sur. AWS Outposts Vous pouvez effectuer des sauvegardes depuis vos machines virtuelles sur site et VMC vers. AWS Backup Vous pouvez ensuite effectuer une restauration depuis AWS Backup vers des machines virtuelles sur site, des machines virtuelles dans Ir VMC ou Ir VMC sur AWS Outposts.

AWS Backup vous fournit également des fonctionnalités AWS natives de gestion des sauvegardes de machines virtuelles entièrement gérées, telles que la découverte des machines virtuelles, la planification des sauvegardes, la gestion de la rétention, un niveau de stockage peu coûteux, la copie entre régions et entre comptes, la prise en charge de AWS Backup Vault Lock et d' AWS Backup Audit Manager, un chiffrement indépendant des données sources et des politiques d'accès aux sauvegardes. Pour obtenir une liste complète des fonctionnalités et des détails, consultez le tableau Disponibilité des fonctionnalités par ressource.

Vous pouvez l'utiliser AWS Backup pour protéger vos machines virtuelles sur VMware Cloud™ on AWS Outposts. AWS Backup stocke les sauvegardes de vos machines virtuelles dans le répertoire Région AWS auquel votre VMware Cloud™ on AWS Outposts est connecté. Vous pouvez l'utiliser AWS Backup pour protéger votre VMware Cloud™ sur des AWS Backup machines virtuelles lorsque vous utilisez VMware Cloud™ AWS Outposts pour répondre à vos besoins en matière de faible latence et de traitement local des données de vos applications. En fonction de vos exigences en matière de résidence des données, vous pouvez AWS Backup choisir de stocker des sauvegardes des données de votre application dans le parent Région AWS auquel vous AWS Outposts êtes connecté.

Machines virtuelles prises en charge

AWS Backup peut sauvegarder et restaurer des machines virtuelles gérées par un VMware vCenter.

Actuellement pris en charge :

- vSphere 8, 7.0 et 6.7
- Tailles de disque virtuel multiples de 1 KiB
- Banques de données NFS, VMFS et VSAN sur site et dans VMC sur AWS
- Modes de transport SCSI Hot-Add et NBDSSL (Network Block Device Secure Sockets Layer) pour copier des données depuis des machines virtuelles sources vers VMware sur site AWS
- Mode Hot-Add pour protéger les machines virtuelles sur VMware Cloud on AWS

Non pris en charge actuellement :

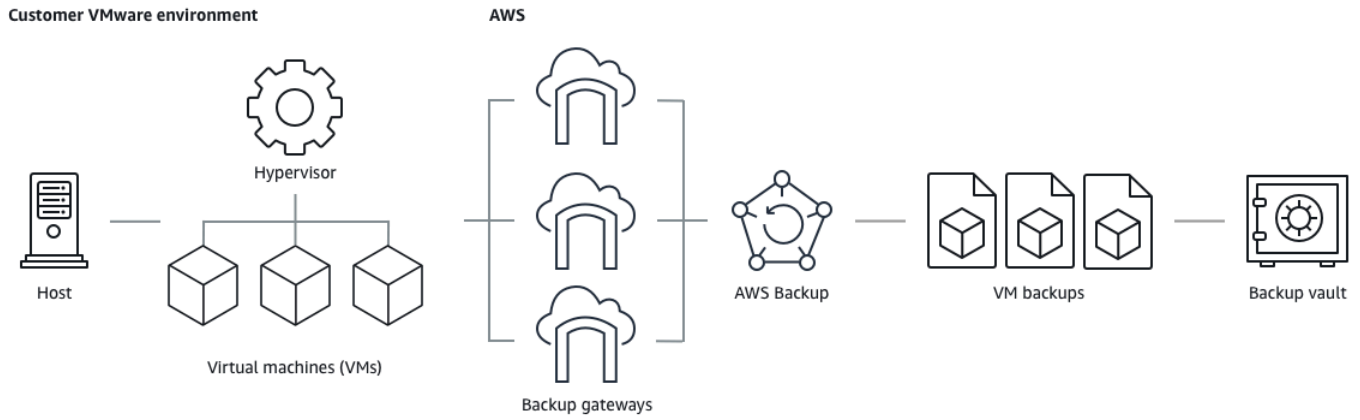
- Disques RDM (mappage de disque brut) ou contrôleurs NVMe et leurs disques
- Modes de disque indépendants persistants et indépendants non persistants

Cohérence de sauvegarde

AWS Backup, par défaut, capture les sauvegardes cohérentes avec les applications des machines virtuelles à l'aide du paramètre de mise au repos de VMware Tools sur la machine virtuelle. Vos sauvegardes sont cohérentes avec les applications si celles-ci sont compatibles avec VMware Tools. Si la fonctionnalité de mise au repos n'est pas disponible, AWS Backup capture les sauvegardes cohérentes en cas de crash. Vérifiez que vos sauvegardes répondent aux besoins de votre entreprise en testant vos restaurations.

Backup gateway

Backup Gateway est AWS Backup un logiciel téléchargeable que vous déployez sur votre infrastructure VMware pour connecter vos machines virtuelles VMware à AWS Backup celles-ci. La passerelle se connecte à votre serveur de gestion de machines virtuelles pour découvrir les machines virtuelles, découvrir vos machines virtuelles, chiffrer les données et les transférer efficacement vers AWS Backup. Le schéma suivant illustre la connexion de Backup Gateway à vos machines virtuelles :



Pour télécharger le logiciel Backup Gateway, suivez la procédure pour Utilisation des passerelles.

Pour plus d'informations sur les points de terminaison VPC (Virtual Private Cloud), consultez AWS Backup la section et connectivité. AWS PrivateLink

Backup gateway est doté de sa propre API, qui est gérée séparément de l'API AWS Backup . Pour consulter la liste des actions de l'API Backup gateway, consultez Actions de Backup gateway. Pour consulter la liste des types de données de l'API Backup gateway, consultez Types de données Backup gateway.

Points de terminaison

Les utilisateurs existants qui utilisent actuellement un point de terminaison public et qui souhaitent passer à un point de terminaison d'un VPC (cloud privé virtuel) peuvent créer une nouvelle passerelle avec un point de terminaison d'un VPC en utilisant AWS PrivateLink, associer l'hyperviseur existant à la passerelle, puis supprimer la passerelle contenant le point de terminaison public.

Configuration de votre infrastructure pour utiliser Backup gateway

Backup gateway nécessite les configurations réseau, de pare-feu et matérielles suivantes pour sauvegarder et restaurer vos machines virtuelles.

Configuration réseau

Backup gateway requiert que certains ports soient autorisés pour fonctionner. Autorisez les ports suivants :

1. TCP 443 sortant
   - Source : Backup gateway

- Destination : AWS
- Utilisation : autorise la passerelle Backup à communiquer avec AWS.

2. TCP 80 entrant
   - Source : L'hôte que vous utilisez pour vous connecter au AWS Management Console
   - Destination : Backup gateway
   - Utilisation : par les systèmes locaux pour obtenir la clé d'activation Backup gateway. Le port 80 n'est utilisé que lors de l'activation de la passerelle Backup. AWS Backup ne nécessite pas que le port 80 soit accessible au public. Le niveau requis de l’accès au port 80 dépend de la configuration de votre réseau. Si vous activez votre passerelle depuis le AWS Management Console, l'hôte à partir duquel vous vous connectez à la console doit avoir accès au port 80 de votre passerelle.
3. UDP 53 sortant
   - Source : Backup gateway
   - Destination : serveur DNS (Domain Name Service)
   - Utilisation : autorise Backup gateway à communiquer avec le DNS.
4. TCP 22 sortant
   - Source : Backup gateway
   - Destination : AWS Support
   - Utilisation : Permet d'accéder AWS Support à votre passerelle pour vous aider à résoudre les problèmes. Il n'est pas nécessaire que ce port soit ouvert pour que votre passerelle fonctionne normalement, mais il doit l'être pour résoudre les problèmes.
5. UDP 123 sortant
   - Source : client NTP
   - Destination : serveur NTP
   - Utilisation : par les systèmes locaux pour synchroniser l'heure de la machine virtuelle et celle de l'hôte.
6. TCP 443 sortant
   - Source : Backup gateway
   - Destination : VMware vCenter
   - Utilisation : autorise Backup gateway à communiquer avec VMware vCenter.
7. TCP 443 sortant
   - Source : Backup gateway

- Destination : hôtes ESXi
- Utilisation : autorise Backup gateway à communiquer avec les hôtes ESXi.

8. TCP 902 sortant
   - Source : Backup gateway
   - Destination : hôtes VMware ESXi
   - Utilisation : pour le transfert de données via Backup gateway.

Les ports ci-dessus sont nécessaires pour la passerelle Backup. Consultez Création d'un point de AWS Backup terminaison VPC pour plus d'informations sur la configuration des points de terminaison Amazon VPC pour. AWS Backup

Configuration de pare-feu

La passerelle de sauvegarde nécessite l'accès aux points de terminaison de service suivants pour communiquer avec Amazon Web Services. Si vous utilisez un pare-feu ou un routeur pour filtrer ou limiter le trafic réseau, vous devez les configurer afin de permettre les communications sortantes vers AWS pour ces points de terminaison de service. L'utilisation d'un proxy HTTP entre Backup gateway et les points de service n'est pas prise en charge.

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

Configuration de votre passerelle pour plusieurs NIC dans VMware

Vous pouvez gérer des réseaux distincts pour votre trafic interne et externe en connectant plusieurs connexions d'interface réseau virtuelle (NIC) à votre passerelle, puis en dirigeant le trafic interne (passerelle vers l'hyperviseur) et le trafic externe (passerelle vers AWS) séparément.

Par défaut, les machines virtuelles connectées à la AWS Backup passerelle disposent d'un adaptateur réseau (`eth0`). Ce réseau inclut l'hyperviseur, les machines virtuelles et la passerelle réseau (passerelle de sauvegarde) qui communique avec l'Internet au sens large.

Voici un exemple de configuration avec plusieurs interfaces réseau virtuelles :

```
        eth0:
```

```
            - IP: 10.0.3.83
            - routes: 10.0.3.0/24

            eth1:
            - IP: 10.0.0.241
            - routes: 10.0.0.0/24
            - default gateway: 10.0.0.1
```

- Dans cet exemple, la connexion est à un hyperviseur avec l'adresse IP `10.0.3.123`, la passerelle utilisera `eth0`, car l'adresse IP de l'hyperviseur fait partie du bloc `10.0.3.0/24`.
- Pour se connecter à un hyperviseur via l'adresse IP `10.0.0.234`, la passerelle utilisera `eth1`.
- Pour se connecter à une adresse IP en dehors des réseaux locaux (par exemple `34.193.121.211`), la passerelle reviendra à la passerelle par défaut `10.0.0.1`, qui se trouve dans le bloc `10.0.0.0/24` et passera donc par `eth1`.

La première séquence d'ajout d'un adaptateur réseau supplémentaire se produit dans le client vSphere :

1. Dans le client VMware vSphere, ouvrez le menu contextuel (clic droit) pour votre machine virtuelle de passerelle., puis choisissez Modifier les paramètres.
2. Dans l'onglet Matériel virtuel de la boîte de dialogue Propriétés de la machine virtuelle, ouvrez le menu Ajouter un nouvel appareil et sélectionnez Adaptateur réseau pour ajouter un nouvel adaptateur réseau.
3. a. Développez les détails du Nouveau réseau pour configurer le nouvel adaptateur.
   b. Assurez-vous que l'option Se connecter lors de la mise sous tension est sélectionnée.
   c. Pour Type d'adaptateur, consultez la section Types d'adaptateur réseau dans la Documentation d'ESXi et de vCenter Server.
4. Cliquez sur OK pour enregistrer les nouveaux paramètres de l'adaptateur réseau.

La séquence d'étapes suivante pour configurer un adaptateur supplémentaire s'effectue dans la console de AWS Backup passerelle (notez qu'il ne s'agit pas de la même interface que la console de AWS gestion dans laquelle les sauvegardes et les autres services sont gérés).

Une fois que la nouvelle NIC est ajoutée à la machine virtuelle de la passerelle, vous devez

- Accéder à `Command Prompt` et activer les nouveaux adaptateurs

- Configurer des adresses IP statiques pour chaque nouvelle NIC
- Définir la NIC préférée comme votre choix par défaut

Pour cela :

1. Dans le client VMware vSphere, sélectionnez votre machine virtuelle de passerelle et lancez la console Web pour accéder à la console locale de la passerelle Backup.
   - Pour plus d'informations sur l'accès à une console locale, consultez Accès à la console locale de la passerelle avec VMware ESXi.
2. Quittez l'invite de commande et accédez à Configuration réseau > Configurer l'adresse IP statique et suivez les instructions de configuration pour mettre à jour la table de routage.
   a. Attribuez une adresse IP statique dans le sous-réseau de l'adaptateur réseau.
   b. Définissez un masque réseau.
   c. Entrez l'adresse IP de la passerelle par défaut. Il s'agit de la passerelle réseau qui se connecte à tout le trafic en dehors du réseau local.
3. Sélectionnez Définir l'adaptateur par défaut pour désigner l'adaptateur qui sera connecté au cloud comme appareil par défaut.
4. Toutes les adresses IP de la passerelle peuvent être affichées à la fois dans la console locale et sur la page de résumé de la machine virtuelle dans VMware vSphere.

Configuration matérielle requise

Vous devez être en mesure de consacrer les ressources minimales suivantes sur un hôte de machine virtuelle pour la passerelle de sauvegarde :

- 4 processeurs virtuels
- 8 Gio de mémoire RAM réservée

Autorisations VMware

Cette section répertorie les autorisations VMware minimales requises pour l'utilisation AWS Backup gateway. Ces autorisations sont nécessaires pour que Backup gateway.puisse découvrir, sauvegarder et restaurer des machines virtuelles.

Pour utiliser la passerelle de sauvegarde avec VMware Cloud™ activé AWS ou VMware Cloud™ activé AWS Outposts, vous devez utiliser l'utilisateur administrateur par défaut `cloudadmin@vmc.local` ou attribuer le CloudAdmin rôle à votre utilisateur dédié.

Pour utiliser la passerelle Backup avec des machines virtuelles VMware sur site, créez un utilisateur dédié doté des autorisations répertoriées ci-dessous.

Globale

- Désactiver les méthodes
- Activer les méthodes
- Licences
- Journaliser les événements
- Gérer les attributs personnalisés
- Définir les attributs personnalisés

Balisage vSphere

- Attribuer ou annuler l'attribution d'une balise vSphere

DataStore

- Allouer de l'espace
- Consulter l'entrepôt de données
- Configurer l'entrepôt de données (pour un entrepôt de données vSAN)
- Opérations de fichiers de bas niveau
- Mettre à jour les fichiers des machines virtuelles

Host (Hôte)

- Configuration
  - Paramètres avancés
  - Configuration des partitions de stockage

Dossier

- Créer un dossier

Réseau

- Attribuer un réseau

Groupe dvPort

- Création
- Suppression

Ressource

- Attribuer une machine virtuelle au groupe de ressources

Machine virtuelle

- Modification de la configuration
  - Obtenir un contrat de location disque
  - Ajouter un disque existant
  - Ajouter un nouveau disque
  - Configuration avancée
  - Modifier les paramètres de l'
  - Configurer l'appareil brut
  - Modifier les paramètres de l'appareil
  - Supprimer le disque
  - Définir une annotation
  - Activer/désactiver le suivi des modifications du disque
- Modifier l'inventaire
  - Créer à partir d'un existant
  - Créer un nouveau
  - Enregistrement

  - Remove (suppression)
  - Annuler l'enregistrement
- Interaction
  - Éteindre
  - Allumer
- Allouer
  - Autoriser l'accès disque
  - Autoriser l'accès disque en lecture seule
  - Autoriser le téléchargement de la machine virtuelle
- Gestion des instantanés
  - Créer un instantané
  - Supprimer un instantané
  - Revenir à un instantané

Utilisation des passerelles

Pour sauvegarder et restaurer vos machines virtuelles (VM) à l'aide de AWS Backup, vous devez d'abord installer une passerelle de sauvegarde. Une passerelle est un logiciel sous la forme d'un modèle OVF (Open Virtualization Format) qui connecte Amazon Web Services Backup à votre hyperviseur, ce qui lui permet de détecter automatiquement vos machines virtuelles et de vous permettre de les sauvegarder et de les restaurer.

Une passerelle unique peut exécuter jusqu'à 4 tâches de sauvegarde ou de restauration à la fois. Pour exécuter plus de 4 tâches à la fois, créez d'autres passerelles et associez-les à votre hyperviseur.

Création d’une passerelle

Pour créer une passerelle NAT :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Passerelles.
3. Cliquez sur Create gateway (Créer une passerelle).
4. Dans la section Configurer une passerelle, suivez ces instructions pour télécharger et déployer le modèle OVF.

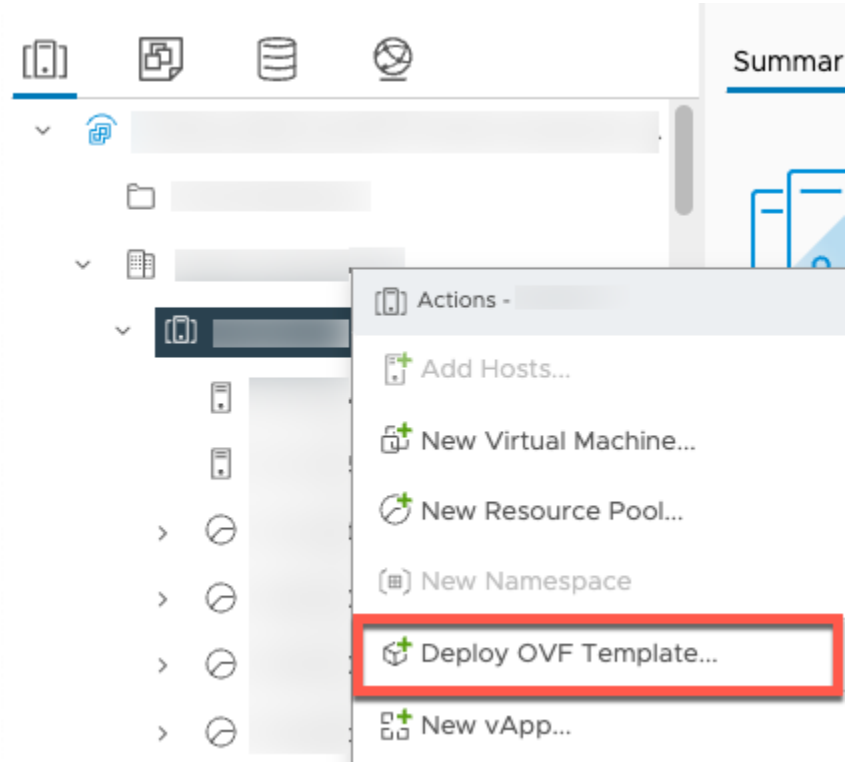
Téléchargement de logiciels VMware

Connexion de l'hyperviseur

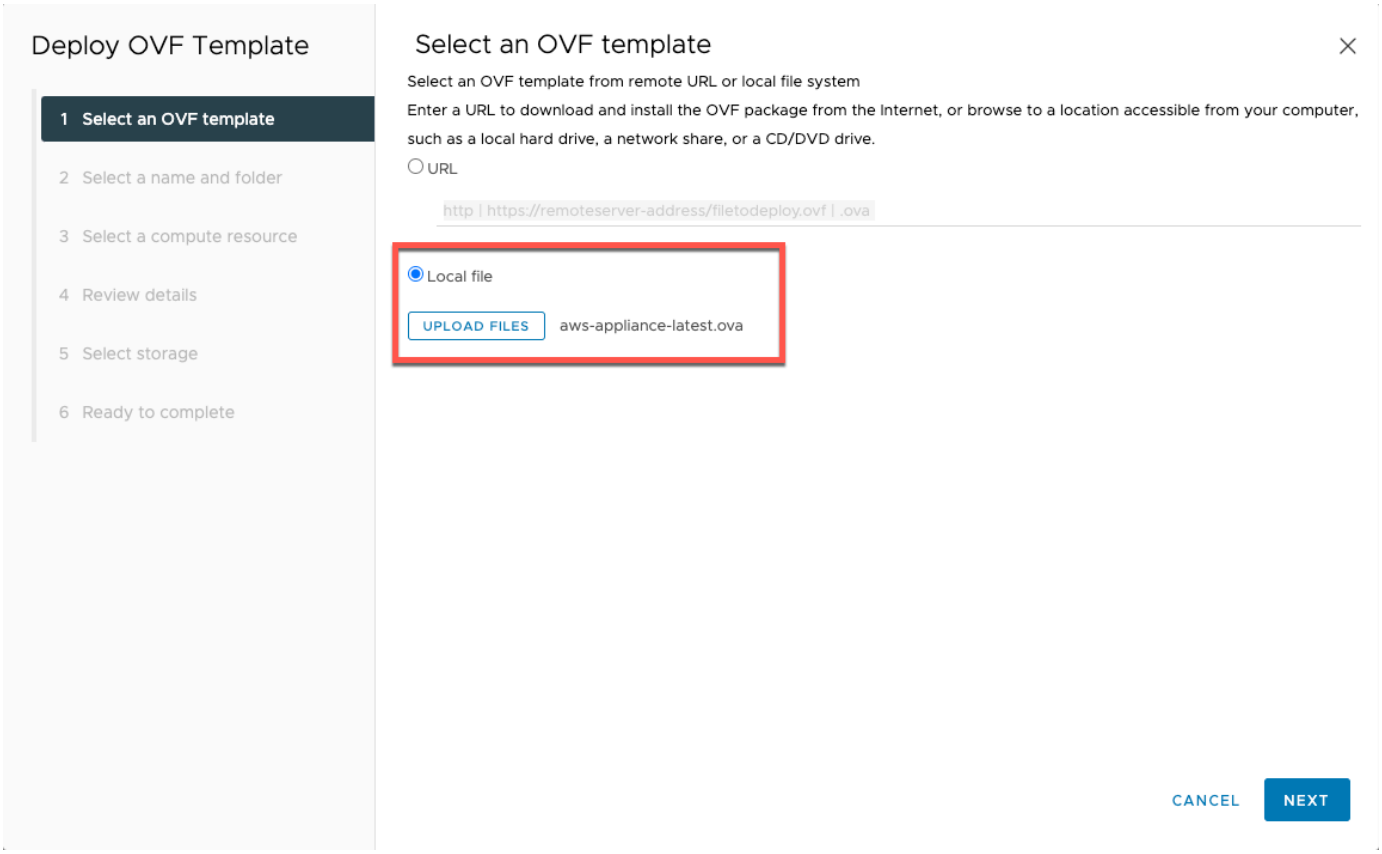
Les passerelles se connectent AWS Backup à votre hyperviseur afin que vous puissiez créer et stocker des sauvegardes de vos machines virtuelles. Pour configurer votre passerelle sur VMware ESXi, téléchargez le modèle OVF. Le téléchargement peut prendre environ 10 minutes.

Une fois l'opération terminée, procédez comme suit :

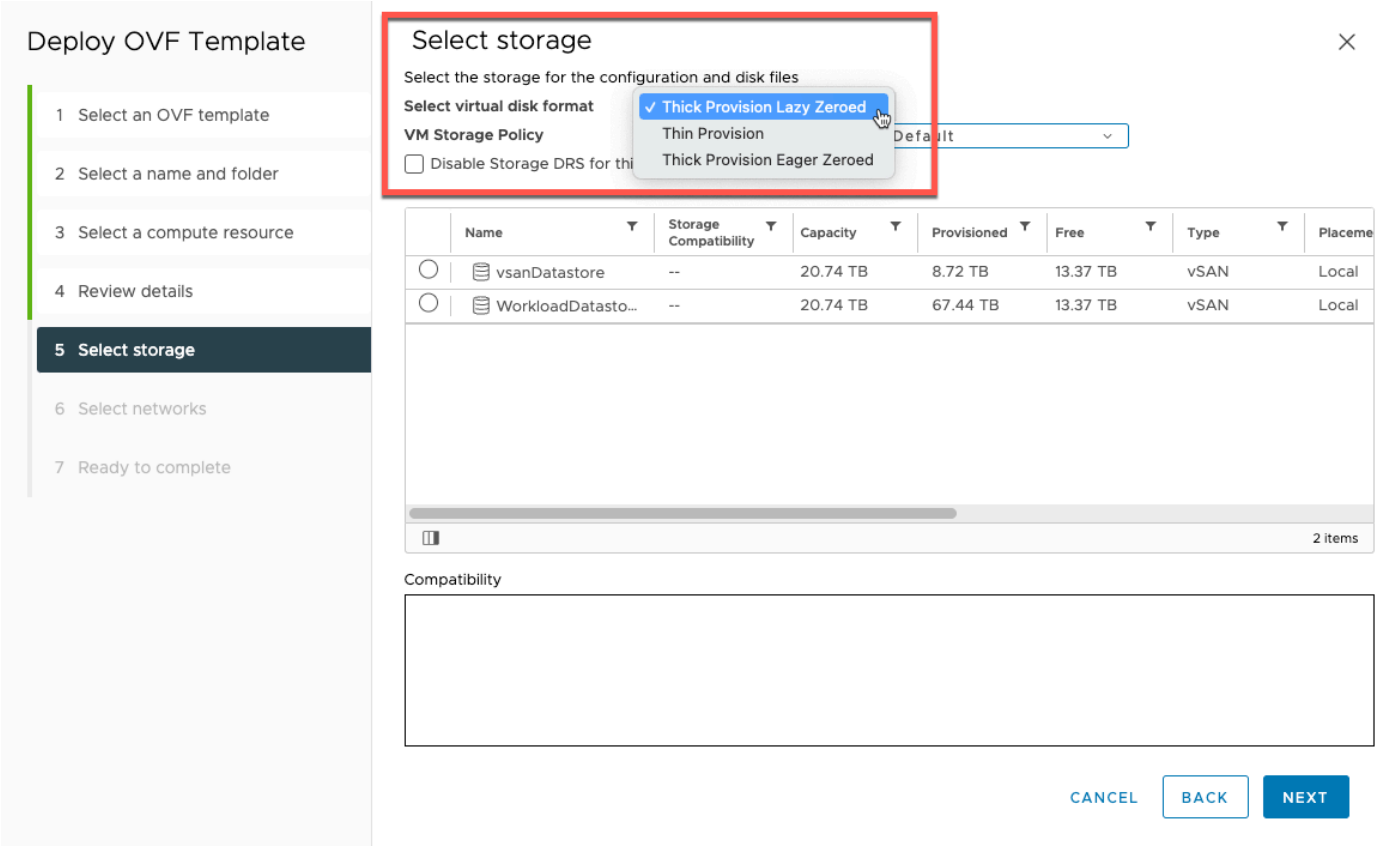
1. Connectez-vous à l'hyperviseur de votre machine virtuelle à l'aide de VMware vSphere.
2. Cliquez avec le bouton droit sur un objet parent d'une machine virtuelle et sélectionnez Déployer le modèle OVF.



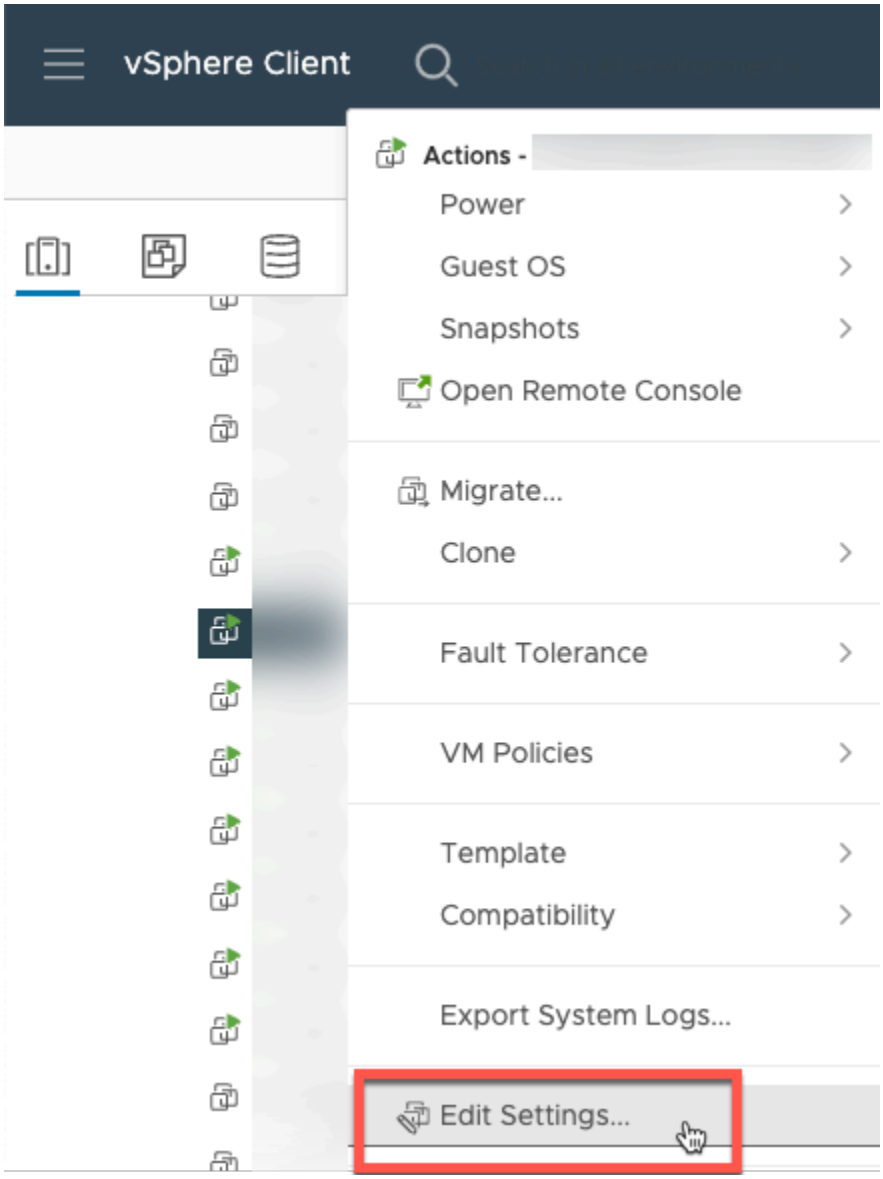
3. Choisissez Fichier local, puis chargez le fichier aws-appliance-latest.ova que vous avez téléchargé.



4. Suivez les étapes de l'assistant de déploiement pour le déployer. Sur la page Sélectionner le stockage, sélectionnez le format de disque virtuel Thick Provision Lazy Zeroed.

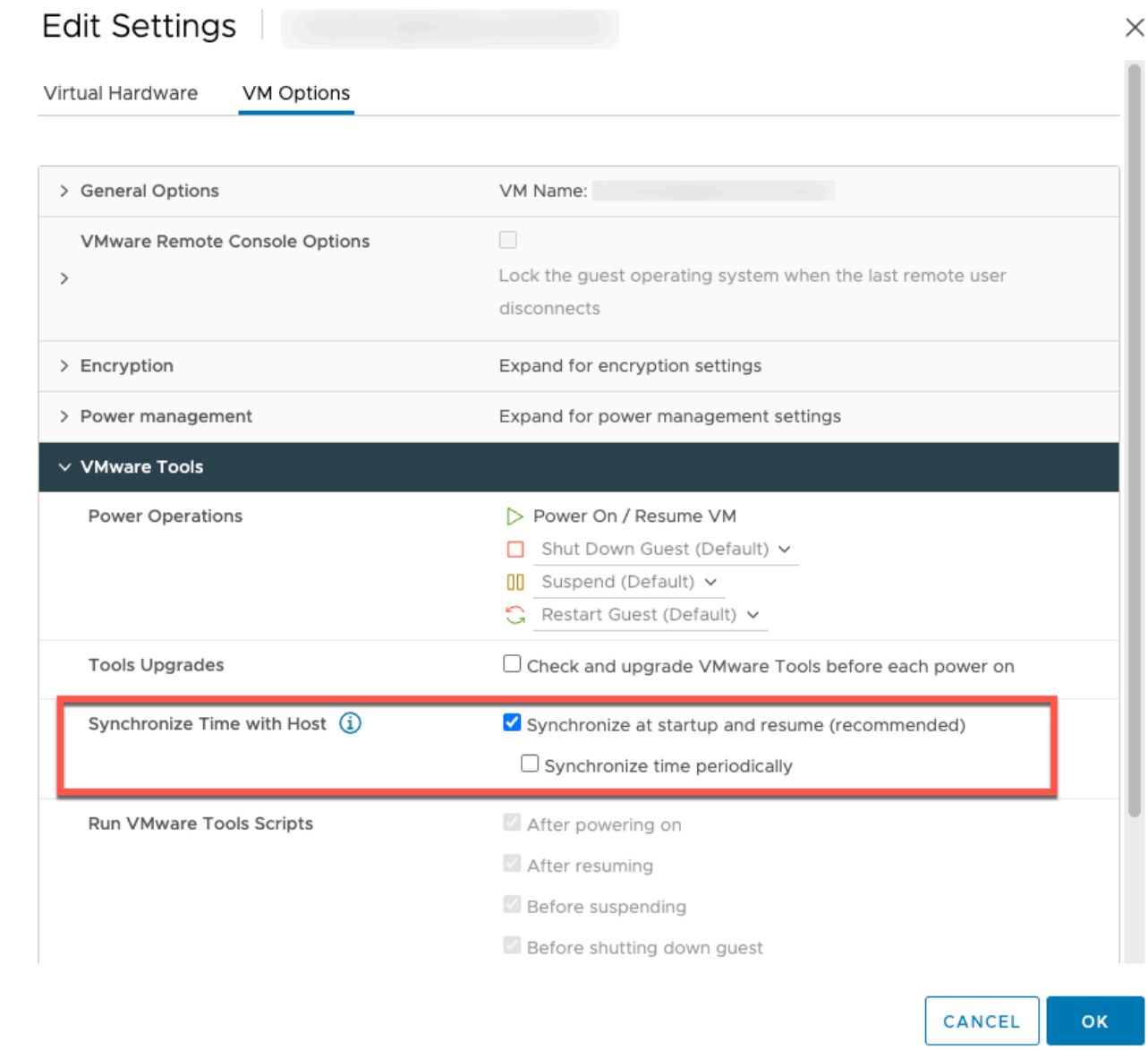


5. Après avoir déployé l'OVF, cliquez avec le bouton droit sur la passerelle et choisissez Modifier les paramètres.

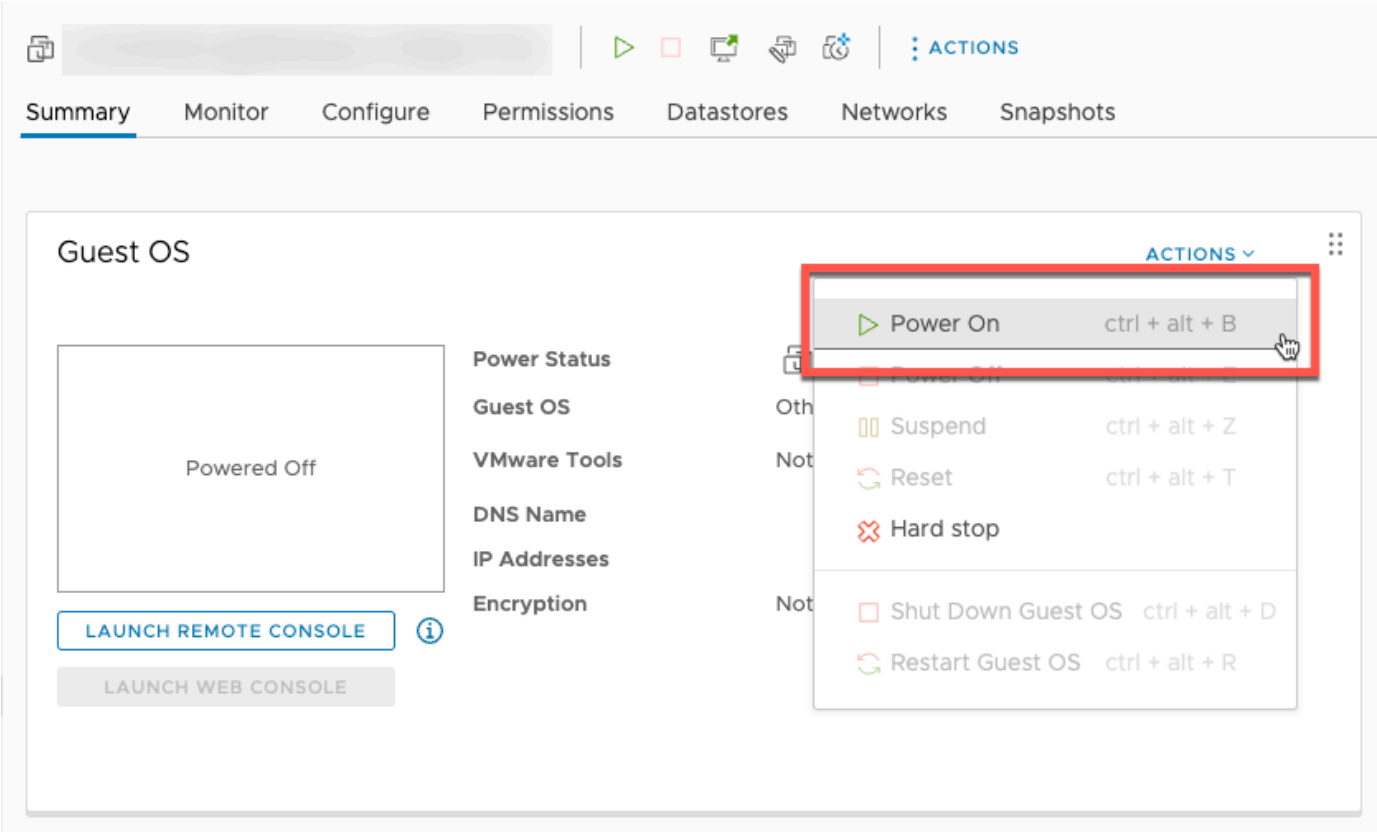


a. Sous Options de machine virtuelle, accédez à Outils de machine virtuelle.

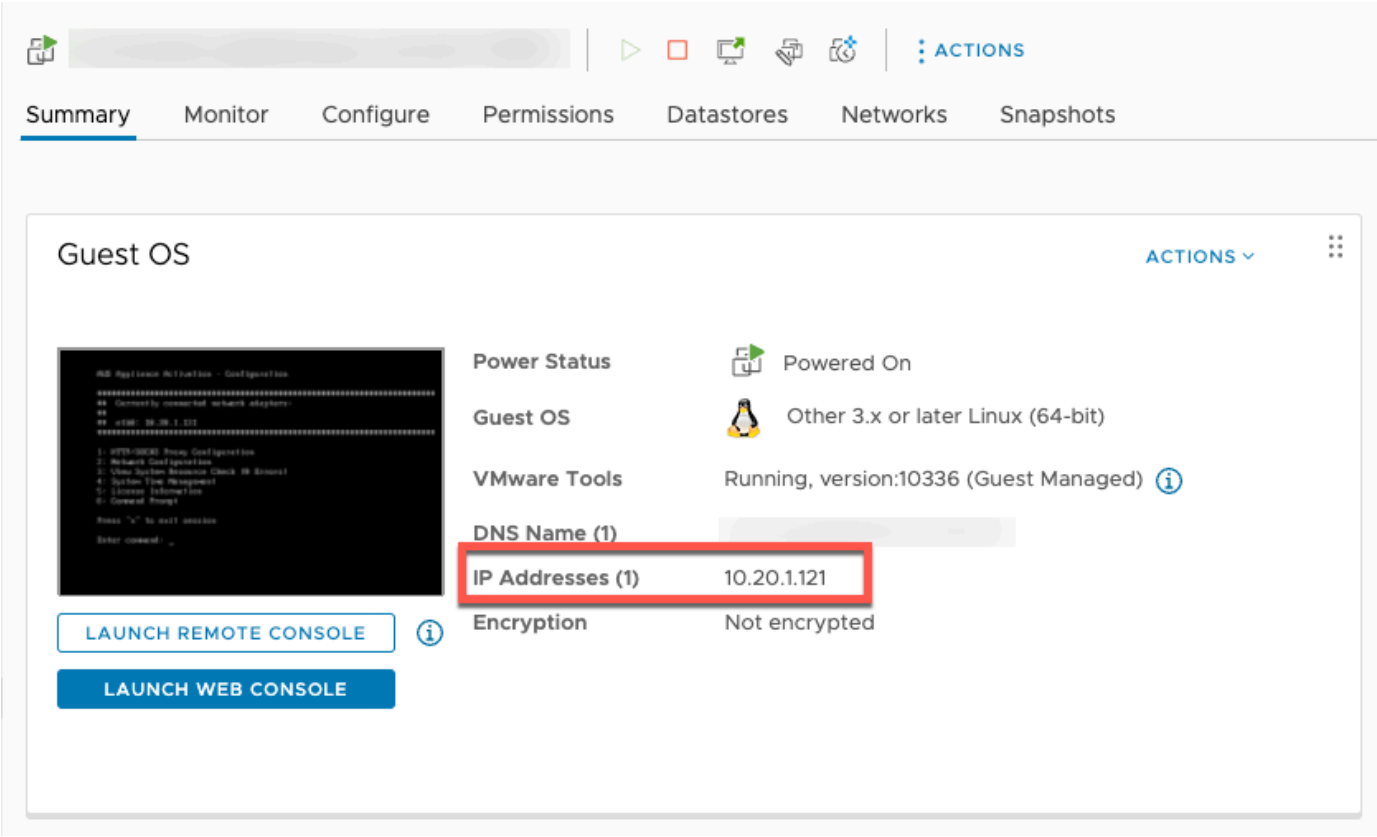
b. Assurez-vous que pour Synchroniser l'heure avec l'hôte, l'option Synchroniser au démarrage et à la reprise est sélectionnée.



6. Allumez la machine virtuelle en sélectionnant « Allumer » dans le menu Actions.



7. Copiez l'adresse IP depuis le résumé de la machine virtuelle et entrez-la ci-dessous.



Une fois le logiciel VMware téléchargé, suivez les étapes ci-dessous :

1. Dans la section Connexion à la passerelle, saisissez l'adresse IP de la passerelle.
   a. Pour trouver cette adresse IP, accédez à vSphere Client.
   b. Sélectionnez votre passerelle sous l'onglet Résumé.
   c. Copiez l'adresse IP et collez-la dans la barre de texte de la AWS Backup console.
2. Dans la section Paramètres de la passerelle,
   a. Saisissez un Nom de passerelle.
   b. Vérifiez la AWS région.
   c. Choisissez si le point de terminaison est accessible au public ou hébergé dans votre cloud privé virtuel (VPC).
   d. En fonction du point de terminaison choisi, entrez le nom DNS du point de terminaison du VPC.

      Pour plus d'informations, consultez Création d'un point de terminaison d'un VPC.
3. [Facultatif] Dans la section Identifications de la passerelle, vous pouvez attribuer des balises en saisissant la clé et la valeur facultative. Pour ajouter plusieurs balises, cliquez sur Ajouter une autre balise.
4. Pour terminer le processus, cliquez sur Créer une passerelle, qui vous amène à la page détaillée de la passerelle.

Modification ou suppression d'une passerelle

Pour modifier ou supprimer une passerelle :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Passerelles.
2. Dans la section Passerelles, choisissez une passerelle en fonction de son Nom de passerelle.
3. Pour modifier le nom de la passerelle, choisissez Modifier.
4. Pour supprimer la passerelle, choisissez Supprimer, puis Supprimer la passerelle.

   Vous ne pouvez pas réactiver une passerelle supprimée. Si vous souhaitez vous connecter à nouveau à l'hyperviseur, suivez la procédure décrite dans Création d'une passerelle.
5. Pour vous connecter à un hyperviseur, dans la section Hyperviseur connecté, choisissez Connecter.

Chaque passerelle se connecte à un seul hyperviseur. Cependant, vous pouvez connecter plusieurs passerelles au même hyperviseur pour augmenter la bande passante entre elles au-delà de celle de la première passerelle.

6. Pour attribuer, modifier ou gérer des balises, dans la section Balises, choisissez Gérer les balises.

Limitation de bande passante de la passerelle de sauvegarde

> **Note**
>
> Cette fonctionnalité sera disponible sur les nouvelles passerelles déployées après le 15 décembre 2022. Pour les passerelles existantes, cette nouvelle fonctionnalité sera disponible via une mise à jour logicielle automatique au plus tard le 30 janvier 2023. Pour mettre à jour manuellement la passerelle vers la dernière version, utilisez AWS CLI la commande `UpdateGatewaySoftwareNow`.

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

Vous pouvez configurer un calendrier de limite de bande passante à l'aide de la AWS Backup console ou de l'API via le AWS CLI () `PutBandwidthRateLimitSchedule`. Lorsque vous utilisez une planification de limite de débit de la bande passante, vous pouvez configurer les limites pour qu'elles changent automatiquement au cours de la journée ou de la semaine.

La limitation du taux de bande passante fonctionne en équilibrant le débit de toutes les données téléchargées, en moyenne chaque seconde. Bien qu'il soit possible que les téléchargements dépassent brièvement la limite de taux de bande passante pendant une micro ou une milliseconde donnée, cela n'entraîne généralement pas de pics importants sur de longues périodes.

Vous pouvez ajouter jusqu'à 20 intervalles. La valeur maximale du taux de téléchargement est de 8 000 000 (millions) de mégaoctets par seconde (Mbits/s).

Consultez et modifiez le calendrier de limite de bande passante pour votre passerelle à l'aide de la AWS Backup console.

Cette section explique comment afficher et modifier la planification de limite de débit de la bande passante pour votre passerelle.

Pour consulter et modifier la planification de limite de débit de la bande passante

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, sélectionnez Passerelles. Dans le volet Passerelles, les passerelles sont affichées par nom. Cliquez sur la case d'option à côté du nom de la passerelle que vous souhaitez gérer.
3. Une fois que vous avez sélectionné une case d'option, vous pouvez cliquer sur le menu déroulant Action. Cliquez sur Actions, puis sur Modifier la planification de limite de débit de la bande passante. La planification actuelle s'affiche. Par défaut, aucune limite de débit de bande passante n'est définie pour une passerelle nouvelle ou non modifiée.

   > **Note**
   >
   > Vous pouvez également cliquer sur Gérer la planification dans la page des détails de la passerelle pour accéder à la page Modifier la bande passante.

4. (Facultatif) Choisissez Ajouter un intervalle pour ajouter un nouvel intervalle configurable à la planification. Pour chaque intervalle, saisissez les informations suivantes :

   a. Jours de la semaine : sélectionnez le ou les jours récurrents auxquels vous souhaitez appliquer l'intervalle. Une fois sélectionnés, les jours s'affichent sous le menu déroulant. Vous pouvez les supprimer en cliquant sur le X à côté du jour.

   b. Heure de début : entrez l'heure de début de l'intervalle de bande passante, en utilisant le format 24 heures HH:MM. L'heure doit être exprimée au format UTC (temps universel coordonné).

      Remarque : Votre bandwidth-rate-limit intervalle commence au début de la minute spécifiée.

   c. Heure de fin : entrez l'heure de fin de l'intervalle de bande passante, en utilisant le format 24 heures HH:MM. L'heure doit être exprimée au format UTC (temps universel coordonné).

> **Important**
>
> L' bandwidth-rate-limit intervalle prend fin à la fin de la minute spécifiée. Pour planifier un intervalle se terminant au bout d'une heure, entrez 59. Pour planifier des intervalles continus consécutifs, en effectuant la transition au début de l'heure, sans interruption entre les intervalles, entrez 59 pour la minute de fin du premier intervalle. Entrez `00` pour la minute de début de l'intervalle suivant.

d. Débit de chargement : entrez la limite de débit de téléchargement, en mégabits par seconde (Mbits/s). La valeur minimale est de 102 mégaoctets par seconde (Mbits/s).

5. (Facultatif) Répétez l'étape précédente comme vous le souhaitez jusqu'à ce que votre planification de limite de débit de la bande passante soit terminée. Si vous devez supprimer un intervalle de votre planification, choisissez Supprimer.

> **Important**
>
> Les intervalles de limite de taux de bande passante ne peuvent pas se chevaucher. L'heure de début d'un intervalle doit être postérieure à l'heure de fin d'un intervalle précédent et antérieure à l'heure de début d'un intervalle suivant ; son heure de fin doit être antérieure à l'heure de début de l'intervalle suivant.

6. Lorsque vous avez terminé, cliquez sur le bouton Enregistrer les modifications.

Consultez et modifiez la planification de limite de débit de la bande passante pour votre passerelle à l'aide de l' AWS CLI.

L'action `GetBandwidthRateLimitSchedule` peut être utilisée pour afficher la planification de limitation de bande passante pour une passerelle spécifiée. Si aucune planification n'est définie, la planification sera une liste vide d'intervalles. Voici un exemple d'utilisation du AWS CLI pour récupérer le planning de bande passante d'une passerelle :

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

Pour modifier la planification de limitation de bande passante d'une passerelle, vous pouvez utiliser l'action `PutBandwidthRateLimitSchedule`. Notez que vous ne pouvez mettre à jour la planification d'une passerelle que dans son ensemble, plutôt que de modifier, d'ajouter ou de

supprimer des intervalles individuels. Cette action remplacera la planification précédente de limitation de bande passante de la passerelle.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

Utilisation des hyperviseurs

Une fois que vous avez terminéCréation d'une passerelle, vous pouvez le connecter à un hyperviseur pour AWS Backup permettre de travailler avec les machines virtuelles gérées par cet hyperviseur. Par exemple, l'hyperviseur pour les machines virtuelles VMware est VMware vCenter Server. Assurez-vous que votre hyperviseur est configuré avec les autorisations nécessaires pour AWS Backup.

Ajout d'un hyperviseur

Pour ajouter un hyperviseur :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.
2. Choisissez Ajouter un hyperviseur.
3. Dans la section Paramètres de l'hyperviseur, saisissez le Nom de l'hyperviseur.
4. Pour Hôte du serveur vCenter, utilisez le menu déroulant pour sélectionner l'adresse IP ou le Nom de domaine complet (FQDN). Saisissez la valeur correspondante.
5. Pour permettre AWS Backup de découvrir les machines virtuelles sur l'hyperviseur, entrez le nom d'utilisateur et le mot de passe de l'hyperviseur.
6. Chiffrez votre mot de passe. Vous pouvez spécifier ce chiffrement en sélectionnant une clé KMS gérée par un service spécifique ou une clé KMS gérée par le client à l'aide du menu déroulant ou en choisissant Créer une clé KMS. Si vous ne sélectionnez pas de clé spécifique, AWS Backup chiffrera votre mot de passe à l'aide d'une clé appartenant au service.
7. Dans la section Connexion de passerelle, utilisez la liste déroulante pour spécifier la passerelle à connecter à votre hyperviseur.
8. Choisissez Tester la connexion de la passerelle pour vérifier vos entrées précédentes.
9. (Facultatif) Dans la section Identifications de l'hyperviseur, vous pouvez attribuer des balises à l'hyperviseur en choisissant Ajouter une nouvelle balise.
10. Mappage de balises VMware facultatif : vous pouvez ajouter jusqu'à 10 balises VMware que vous utilisez actuellement sur vos machines virtuelles pour générer des AWS balises.

11. Dans le panneau de configuration du groupe de journaux, vous pouvez choisir d'intégrer Amazon CloudWatch Logs pour conserver les journaux de votre hyperviseur (la tarification standard CloudWatch des journaux s'appliquera en fonction de l'utilisation). Chaque hyperviseur peut appartenir à un seul et même groupe de journaux.

    a. Si vous n'avez pas encore créé de groupe de journaux, sélectionnez la case d'option Créer un nouveau groupe de journaux. L'hyperviseur que vous êtes en train de modifier sera associé à ce groupe de journaux.

    b. Si vous avez déjà créé un groupe de journaux pour un autre hyperviseur, vous pouvez utiliser ce groupe de journaux pour cet hyperviseur. Sélectionnez Utiliser un groupe de journaux existant.

    c. Si vous ne souhaitez pas la CloudWatch journalisation, sélectionnez Désactiver la journalisation.

12. Choisissez Ajouter un hyperviseur pour accéder à sa page détaillée.

> **Tip**
>
> Vous pouvez utiliser Amazon CloudWatch Logs (voir étape 11 ci-dessus) pour obtenir des informations sur votre hyperviseur, notamment la surveillance des erreurs, la connexion réseau entre la passerelle et l'hyperviseur, ainsi que des informations de configuration réseau. Pour plus d'informations sur les groupes de CloudWatch journaux, consultez la section Working with Log Groups and Log Streams dans le guide de CloudWatch l'utilisateur Amazon.

Affichage des machines virtuelles gérées par un hyperviseur

Pour afficher les machines virtuelles sur un hyperviseur :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.
2. Dans la section Hyperviseurs, choisissez un hyperviseur en fonction du Nom de l'hyperviseur pour accéder à sa page détaillée.
3. Dans la section sous Résumé de l'hyperviseur, choisissez l'onglet Machines virtuelles.
4. Dans la section Machines virtuelles connectées, une liste de machines virtuelles est automatiquement renseignée.

Affichage des passerelles connectées à un hyperviseur

Pour afficher les passerelles connectées à l'hyperviseur :

1. Choisissez l'onglet Passerelles.
2. Dans la section Passerelles connectées, une liste de passerelles est automatiquement renseignée.

Connexion d'un hyperviseur à des passerelles supplémentaires

Vos vitesses de sauvegarde et de restauration peuvent être limitées par la bande passante de la connexion entre votre passerelle et l'hyperviseur. Vous pouvez augmenter ces vitesses en connectant une ou plusieurs passerelles supplémentaires à votre hyperviseur. Vous pouvez le faire dans la section Passerelles connectées comme suit :

1. Choisissez Se connecter.
2. Sélectionnez une autre passerelle à l'aide du menu déroulant. Vous pouvez également choisir Créer une passerelle pour créer une nouvelle passerelle.
3. Choisissez Se connecter.

Modification de la configuration d'un hyperviseur

Si vous n'utilisez pas la fonctionnalité Tester la connexion de la passerelle, vous pouvez ajouter un hyperviseur avec un nom d'utilisateur ou un mot de passe incorrect. Dans ce cas, le statut de connexion de l'hyperviseur est toujours `Pending`. Vous pouvez également alterner le nom d'utilisateur ou le mot de passe pour accéder à votre hyperviseur. Mettez à jour ces informations à l'aide de la procédure suivante :

Pour modifier un hyperviseur déjà ajouté :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.
2. Dans la section Hyperviseurs, choisissez un hyperviseur en fonction du Nom de l'hyperviseur pour accéder à sa page détaillée.
3. Choisissez Modifier.
4. Le panneau supérieur s'appelle Paramètres de l'hyperviseur.
    a. Sous Hôte du serveur vCenter, vous pouvez également modifier le FQDN (nom de domaine complet) ou l'adresse IP.

b. (Facultatif) Entrez le Nom d'utilisateur et le Mot de passe de l'hyperviseur.

5. Dans le panneau de configuration du groupe de journaux, vous pouvez choisir d'intégrer Amazon CloudWatch pour conserver les journaux de votre hyperviseur (la CloudWatch tarification standard s'appliquera en fonction de l'utilisation). Chaque hyperviseur peut appartenir à un seul et même groupe de journaux.

   a. Si vous n'avez pas encore créé de groupe de journaux, sélectionnez la case d'option Créer un nouveau groupe de journaux. L'hyperviseur que vous êtes en train de modifier sera associé à ce groupe de journaux.

   b. Si vous avez déjà créé un groupe de journaux pour un autre hyperviseur, vous pouvez utiliser ce groupe de journaux pour cet hyperviseur. Sélectionnez Utiliser un groupe de journaux existant.

   c. Si vous ne souhaitez pas la CloudWatch journalisation, sélectionnez Désactiver la journalisation.

> **Tip**
>
> Vous pouvez utiliser Amazon CloudWatch Logs (voir étape 5 ci-dessus) pour obtenir des informations sur votre hyperviseur, notamment la surveillance des erreurs, la connexion réseau entre la passerelle et l'hyperviseur, ainsi que des informations de configuration réseau. Pour plus d'informations sur les groupes de CloudWatch journaux, consultez la section Working with Log Groups and Log Streams dans le guide de CloudWatch l'utilisateur Amazon.

Pour mettre à jour un hyperviseur par programmation, utilisez la commande de la CLI update-hypervisor et l'appel d'API. UpdateHypervisor

Suppression de la configuration d'un hyperviseur

Si vous devez supprimer un hyperviseur déjà ajouté, supprimez la configuration de l'hyperviseur et ajoutez-en une autre. Cette opération de suppression s'applique à la configuration de connexion à l'hyperviseur. Cela ne supprime pas l'hyperviseur.

Pour supprimer la configuration afin de vous connecter à un hyperviseur déjà ajouté :

1. Dans le volet de navigation de gauche, sous Ressources externes, choisissez Hyperviseurs.

2. Dans la section Hyperviseurs, choisissez un hyperviseur en fonction du Nom de l'hyperviseur pour accéder à sa page détaillée.
3. Choisissez Supprimer, puis Supprimer l'hyperviseur.
4. Facultatif : remplacez la configuration de l'hyperviseur supprimée en suivant la procédure pour Ajout d'un hyperviseur.

Compréhension du statut de l'hyperviseur

Ce qui suit décrit chacun des statuts possibles de l'hyperviseur et, le cas échéant, les étapes de correction. Le statut `ONLINE` est le statut normal de l'hyperviseur. Un hyperviseur doit avoir ce statut tout le temps ou la plupart du temps lorsqu'il est utilisé pour la sauvegarde et la restauration des machines virtuelles gérées par l'hyperviseur.

Statuts de l'hyperviseur

Statut	Signification et remédiation
`ONLINE`	Vous y avez ajouté un hyperviseur AWS Backup, vous lui avez associé une passerelle, et vous pouvez vous connecter à cette passerelle via votre réseau pour effectuer la sauvegarde et la restauration des machines virtuelles gérées par l'hyperviseur. Vous pouvez effectuer des sauvegardes à la demande et planifiées de ces machines virtuelles à tout moment.
`PENDING`	Vous avez ajouté un hyperviseur à AWS Backup mais : • Il n'est associé à aucune passerelle, ou • Il est associé à une ou plusieurs passerelles, mais toutes ces passerelles ont été supprimées ou ne sont pas actives.

Statut	Signification et remédiation
	Pour modifier le statut d'un hyperviseur de `PENDING` à `ONLINE`, créez une passerelle et connectez votre hyperviseur à cette passerelle.
`OFFLINE`	Vous avez ajouté un hyperviseur AWS Backup et l'avez associé à une passerelle, mais la passerelle ne peut pas se connecter à l'hyperviseur via votre réseau. Pour modifier le statut d'un hyperviseur de `OFFLINE` à `ONLINE`, vérifiez l'exactitude de la configuration de votre réseau. Si le problème persiste, vérifiez que l'adresse IP ou le nom de domaine complet de votre hyperviseur est correct. S'ils sont incorrects, ajoutez à nouveau votre hyperviseur en utilisant les informations correctes et testez votre connexion à la passerelle.
`ERROR`	Vous avez ajouté un hyperviseur AWS Backup et l'avez associé à une passerelle, mais la passerelle ne peut pas communiquer avec l'hyperviseur. Pour modifier le statut d'un hyperviseur de `ERROR` à `ONLINE`, vérifiez que le nom d'utilisateur et le mot de passe de l'hyperviseur sont corrects. S'ils sont incorrects, modifiez la configuration de votre hyperviseur.

Étapes suivantes

Pour sauvegarder des machines virtuelles sur votre hyperviseur, consultez Sauvegarde des machines virtuelles.

Sauvegarde des machines virtuelles

Après Ajout d'un hyperviseur, Backup gateway répertorie automatiquement vos machines virtuelles. Vous pouvez afficher vos machines virtuelles en choisissant Hyperviseurs ou Machines virtuelles dans le volet de navigation de gauche.

- Choisissez Hyperviseurs pour afficher uniquement les machines virtuelles gérées par un hyperviseur spécifique. Avec cette vue, vous pouvez travailler avec une machine virtuelle à la fois.
- Choisissez Machines virtuelles pour afficher toutes les machines virtuelles sur tous les hyperviseurs que vous avez ajoutés à votre. Compte AWS Avec cette vue, vous pouvez travailler avec une partie ou la totalité de vos machines virtuelles sur plusieurs hyperviseurs.

Quelle que soit la vue choisie, pour effectuer une opération de sauvegarde sur une machine virtuelle spécifique, choisissez le nom de cette machine virtuelle pour ouvrir sa page détaillée. La page détaillée de la machine virtuelle constitue le point de départ des procédures suivantes.

Création d'une sauvegarde à la demande d'une machine virtuelle

Une sauvegarde à la demande est une sauvegarde complète unique que vous lancez manuellement. Vous pouvez utiliser des sauvegardes à la demande pour tester AWS Backup les fonctionnalités de sauvegarde et de restauration.

Pour créer une sauvegarde à la demande d'une machine virtuelle :

1. Choisissez Create on-demand backup (Créer une sauvegarde à la demande).
2. Configurer votre sauvegarde à la demande.
3. Choisissez Create on-demand backup (Créer une sauvegarde à la demande).
4. Vérifiez que votre tâche de sauvegarde a le statut `Completed`. Dans le menu de navigation de gauche, choisissez Tâches.
5. Choisissez ID de tâche de backup pour afficher les informations relatives à la tâche de sauvegarde, telles que la Taille de sauvegarde et le temps écoulé entre la Date de création et Date de fin.

Sauvegardes de machines virtuelles incrémentielles

Les nouvelles versions de VMware contiennent une fonctionnalité appelée Suivi des blocs modifiés (CBT), qui permet de suivre les blocs de stockage des machines virtuelles à mesure qu'ils changent

au fil du temps. Lorsque vous AWS Backup sauvegardez une machine virtuelle, AWS Backup tente d'utiliser les données CBT si elles sont disponibles. AWS Backup utilise les données CBT pour accélérer le processus de sauvegarde ; sans données CBT, les tâches de sauvegarde sont souvent plus lentes et utilisent davantage de ressources d'hyperviseur. La sauvegarde peut toujours être effectuée, même lorsque les données CBT ne sont pas valides ou disponibles. Par exemple, les données CBT peuvent ne pas être valides ou disponibles en cas d'arrêt brutal de la machine virtuelle ou de l'hôte ESXi.

Lorsque les données CBT ne sont pas valides ou disponibles, le statut de la sauvegarde affiche `Successful` avec un message. Dans ces cas, le message indiquera qu'en l'absence de données CBT, il a AWS Backup utilisé son propre mécanisme de détection des modifications pour effectuer la sauvegarde au lieu des données CBT de VMware. Les sauvegardes suivantes essaieront à nouveau d'utiliser les données CBT et, dans la plupart des cas, les données CBT seront valides et disponibles. Si le problème persiste, consultez la section Dépannage de VMware pour savoir comment y remédier.

Pour que CBT fonctionne correctement, les conditions suivantes doivent être remplies :

- L'hôte doit être ESXi version 4.0 ou ultérieure
- La machine virtuelle propriétaire des disques doit disposer du matériel version 7 ou ultérieure
- Le CBT doit être activé pour la machine virtuelle (il est activé par défaut)

Pour vérifier si le CBT est activé sur un disque virtuel, procédez comme suit :

1. Ouvrez le client vSphere et sélectionnez une machine virtuelle hors tension.
2. Cliquez avec le bouton droit sur la machine virtuelle et accédez à Modifier les paramètres > Options > Avancé/Général > Paramètres de configuration.
3. L'option `ctkEnabled` doit être égale à `True`.

Automatisation de la sauvegarde des machines virtuelles en attribuant des ressources à un plan de sauvegarde

Un plan de sauvegarde est une politique de protection des données définie par l'utilisateur qui automatise la protection des données dans de nombreux services AWS et applications tierces. Vous créez d'abord votre plan de sauvegarde en spécifiant sa fréquence de sauvegarde, sa période de rétention, sa politique de cycle de vie et de nombreuses autres options. Pour créer un plan de sauvegarde, consultez le Didacticiel de démarrage.

Après avoir créé votre plan de sauvegarde, vous attribuez des ressources AWS Backup prises en charge, notamment des machines virtuelles, à ce plan de sauvegarde. AWS Backup propose de nombreuses méthodes pour attribuer des ressources, notamment en affectant toutes les ressources de votre compte, y compris ou en excluant des ressources spécifiques, ou en ajoutant des ressources avec certaines balises.

Outre ses fonctionnalités d'attribution de ressources existantes, la prise en AWS Backup charge des machines virtuelles introduit plusieurs nouvelles fonctionnalités qui vous aident à attribuer rapidement des machines virtuelles à des plans de sauvegarde. Depuis la page Machines virtuelles, vous pouvez attribuer des balises à plusieurs machines virtuelles ou utiliser la nouvelle fonctionnalité Affecter des ressources au plan. Utilisez ces fonctionnalités pour attribuer vos machines virtuelles déjà découvertes par AWS Backup Gateway.

Si vous prévoyez de découvrir et d'attribuer des machines virtuelles supplémentaires à l'avenir, et que vous souhaitez automatiser l'étape d'attribution des ressources pour inclure ces futures machines virtuelles, utilisez la nouvelle fonctionnalité Créer une affectation de groupe.

Balises VMware

Les balises sont des paires clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources.

Une balise VMware est composée d'une catégorie et d'un nom de balise. Les balises VMware sont utilisées pour regrouper les machines virtuelles. Un nom de balise est une étiquette attribuée à une machine virtuelle. Une catégorie est un ensemble de noms de balises.

Dans les AWS balises, vous pouvez utiliser des caractères tels que des lettres UTF-8, des chiffres, des espaces et des caractères spéciaux. `+ - = . _ : /`

Si vous utilisez des balises sur vos machines virtuelles, vous pouvez ajouter jusqu'à 10 balises correspondantes dans AWS Backup pour une meilleure organisation. Vous pouvez associer jusqu'à 10 balises VMware à des AWS balises. Dans la AWS Backup console, vous pouvez les trouver dans Mon organisation > Machines virtuelles > AWS balises ou balises VMware.

Mappage des balises VMware

Si vous utilisez des balises sur vos machines virtuelles, vous pouvez ajouter jusqu'à 10 balises correspondantes dans AWS Backup pour plus de clarté et une meilleure organisation. Les mappages s'appliquent à n'importe quelle machine virtuelle de l'hyperviseur.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans la console, accédez à Modifier l'hyperviseur (cliquez sur Ressources externes, puis sur Hyperviseurs, puis sur le nom de l'hyperviseur, puis sur Gérer les mappages).
3. Le dernier volet, le mappage des balises VMware, contient quatre champs de texte dans lesquels vous pouvez saisir les informations de vos balises VMware existantes dans les balises correspondantes AWS . Les quatre champs sont la catégorie de balise VMware, le nom de balise VMware, la clé de AWS AWS balise et la valeur de la balise (exemple : Catégorie = système d'exploitation ; nom de balise = Windows ; clé de AWS balise = OS-Windows et valeur de AWS balise = Windows).
4. Une fois que vous avez entré vos valeurs préférées, cliquez sur Ajouter un mappage. En cas d'erreur, vous pouvez cliquer sur Supprimer pour supprimer les informations entrées.
5. Après avoir ajouté un ou plusieurs mappages, spécifiez le rôle IAM que vous souhaitez utiliser pour appliquer ces balises AWS aux machines virtuelles VMware.

   La politique `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` contient les autorisations nécessaires. Vous pouvez associer cette politique au rôle que vous utilisez (ou demander à un administrateur de l'associer) ou vous pouvez créer une politique personnalisée pour le rôle utilisé.
6. Enfin, cliquez sur Ajouter un hyperviseur ou Enregistrer.

La relation d'approbation du rôle IAM doit être modifiée pour ajouter les services backup-gateway.amazonaws.com et backup.amazonaws.com. Sans ce service, vous risquez de rencontrer une erreur lors du mappage des balises. Pour modifier la relation d'approbation pour un rôle existant,

1. Connectez-vous à la console IAM.
2. Dans le volet de navigation de la console, choisissez Rôles.
3. Choisissez le nom du rôle que vous voulez modifier, puis sélectionnez l'onglet Relations d'approbation dans la page des détails.
4. Dans Document de stratégie, collez ce qui suit :

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

```
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. Choisissez Mettre à jour la politique d'approbation.

Pour plus de détails, consultez Modification de la relation d'approbation pour un rôle existant dans le Guide d'administration AWS Directory Service.

Affichage des mappages de balises VMware

Dans la console AWS Backup, cliquez sur Ressources externes, puis sur Hyperviseurs, puis sur le lien du nom de l'hyperviseur pour afficher les propriétés de l'hyperviseur sélectionné. Sous le volet récapitulatif se trouvent quatre onglets, le dernier étant consacré aux Mappages de balises VMware. Notez que si vous n'avez pas encore de mappage, « Aucun mappage de balises VMware. » sera affiché.

À partir de là, vous pouvez synchroniser les métadonnées des machines virtuelles découvertes par l'hyperviseur, vous pouvez copier des mappages vers vos hyperviseurs, vous pouvez ajouter des AWS balises mappées aux balises VMware à la sélection de sauvegarde d'un plan de sauvegarde, ou vous pouvez gérer les mappages.

Dans la console, pour voir quelles balises sont appliquées à une machine virtuelle sélectionnée, cliquez sur Machines virtuelles, puis sur le nom de la machine virtuelle, puis sur Balises AWS ou Balises VMware. Vous pouvez afficher et gérer les balises associées à cette machine virtuelle.

Attribution de machines virtuelles au plan à l'aide des mappages de balises VMware

Pour attribuer des machines virtuelles à un plan de sauvegarde à l'aide de balises mappées, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans la console, accédez à Mappages de balises VMware sur la page des détails de l'hyperviseur (cliquez sur Ressources externes, puis sur Hyperviseurs, puis sur le nom de l'hyperviseur).

3. Cochez la case à côté de plusieurs balises mappées pour attribuer ces balises au même plan de sauvegarde.
4. Cliquez sur Ajouter à l'attribution de ressource.
5. Choisissez un Plan de sauvegarde existant dans la liste déroulante. Vous pouvez également choisir Créer un plan de sauvegarde pour créer un nouveau plan de sauvegarde.
6. Cliquez sur Confirmer. Cela ouvre la page Affecter des ressources avec des valeurs préremplies dans le champ Affiner la sélection à l'aide de balises.

Balises VMware utilisant le AWS CLI

AWS Backup utilise l'appel d'API PutHypervisorPropertyMappingspour mapper les propriétés des entités de l'hyperviseur sur site aux propriétés de. AWS

Dans le AWS CLI, utilisez l'opération `put-hypervisor-property-mappings` :

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \
--vmware-to-aws-tag-mappings list of VMware to AWS tag mappings \
--iam-role-arn arn:aws:iam::account:role/roleName \
--region AWSRegion
--endpoint-url URL
```

Voici un exemple :

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-
Windows,AwsTagValue=Windows \
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \
--region us-east-1
```

Vous pouvez également utiliser GetHypervisorPropertyMappings pour vous aider à obtenir des informations de mappage de propriétés. Dans le AWS CLI, utilisez l'opérationget-hypervisor-property-mappings. Voici un exemple de modèle :

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

Voici un exemple :

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Synchroniser les métadonnées des machines virtuelles découvertes par l'hyperviseur à l' AWS aide d'une API, d'une CLI ou d'un SDK

Vous pouvez synchroniser les métadonnées des machines virtuelles. Dans ce cas, les balises VMware présentes sur la machine virtuelle qui font partie des mappages seront synchronisées. En outre, les balises AWS mappées aux balises VMware présentes sur la machine virtuelle seront appliquées à la ressource de machine virtuelle AWS .

AWS Backup utilise l'appel `StartVirtualMachinesMetadataSync`d'API pour synchroniser les métadonnées des machines virtuelles découvertes par l'hyperviseur. Pour synchroniser les métadonnées des machines virtuelles découvertes par l'hyperviseur avec AWS CLI, utilisez l'opération `start-virtual-machines-metadata-sync`.

Exemple de modèle :

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Exemple :

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Vous pouvez également utiliser `GetHypervisor` pour obtenir des informations sur l'hyperviseur, telles que l'hôte, l'état, le statut de la dernière synchronisation des métadonnées et également pour récupérer l'heure de la dernière synchronisation de métadonnées réussie. Dans le AWS CLI, utilisez l'opération`get-hypervisor`.

Exemple de modèle :

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
```

```
--region AWSRegion
```

Exemple :

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Pour plus d'informations, consultez la documentation de l'API VmwareTaget VmwareToAwsTagMapping.

Cette fonctionnalité sera disponible sur les nouvelles passerelles déployées après le 15 décembre 2022. Pour les passerelles existantes, cette nouvelle fonctionnalité sera disponible via une mise à jour logicielle automatique au plus tard le 30 janvier 2023. Pour mettre à jour manuellement la passerelle vers la dernière version, utilisez AWS CLI la commande UpdateGatewaySoftwareNow.

Exemple :

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

Attribution de machines virtuelles à l'aide de balises

Vous pouvez attribuer à vos machines virtuelles actuellement découvertes AWS Backup, ainsi qu'à d'autres AWS Backup ressources, une étiquette que vous avez déjà attribuée à l'un de vos plans de sauvegarde existants. Vous pouvez également créer un nouveau plan de sauvegarde et une nouvelle attribution de ressource basée sur des balises. Les plans de sauvegarde vérifient les ressources nouvellement attribuées chaque fois qu'ils exécutent une tâche de sauvegarde.

Pour baliser plusieurs machines virtuelles avec la même balise :

1. Dans le volet de navigation de gauche, choisissez Machines virtuelles.
2. Cochez la case à côté du Nom de la machine virtuelle pour choisir toutes vos machines virtuelles. Vous pouvez également cocher la case à côté des noms de machines virtuelles que vous souhaitez baliser.
3. Sélectionnez Add Tags (Ajouter des balises).
4. Tapez une Clé de balise.

5. Recommandé : saisissez une Valeur de balise.
6. Choisissez Confirmer.

Attribution de machines virtuelles à l'aide de la fonctionnalité Affecter des ressources au plan

Vous pouvez affecter les machines virtuelles actuellement découvertes par AWS Backup à un plan de sauvegarde existant ou nouveau à l'aide de la fonctionnalité Affecter des ressources au plan.

Pour attribuer des machines virtuelles à l'aide de la fonctionnalité Affecter des ressources au plan :

1. Dans le volet de navigation de gauche, choisissez Machines virtuelles.
2. Cochez la case à côté du Nom de la machine virtuelle pour choisir toutes vos machines virtuelles. Vous pouvez également cocher la case à côté des noms de plusieurs machines virtuelles pour les attribuer au même plan de sauvegarde.
3. Choisissez Affectations, puis Affecter des ressources au plan.
4. Saisissez un Nom d'attribution de ressource.
5. Choisissez un rôle IAM d'attribution de ressources pour créer des sauvegardes et gérer les points de récupération. Si vous n'avez pas de rôle IAM spécifique à utiliser, nous vous recommandons le Rôle par défaut qui dispose des autorisations appropriées.
6. Dans la section Plan de sauvegarde, choisissez un Plan de sauvegarde existant dans la liste déroulante. Vous pouvez également choisir Créer un plan de sauvegarde pour créer un nouveau plan de sauvegarde.
7. Choisissez Attribuer des ressources.
8. Facultatif : vérifiez que vos machines virtuelles sont attribuées à un plan de sauvegarde en choisissant Afficher le plan de sauvegarde. Ensuite, dans la section Attributions de ressources, choisissez le Nom de l'attribution de ressources.

Attribution de machines virtuelles à l'aide de la fonctionnalité Créer une affectation de groupe

Contrairement aux deux fonctionnalités d'attribution de ressources précédentes pour les machines virtuelles, la fonctionnalité Créer une attribution de groupe affecte non seulement les machines virtuelles actuellement découvertes par AWS Backup, mais également les machines virtuelles découvertes à l'avenir dans un dossier ou un hyperviseur que vous définissez.

De plus, vous n'avez pas besoin de cocher de case pour utiliser la fonctionnalité Créer une affectation de groupe.

Pour attribuer des machines virtuelles à l'aide de la fonctionnalité Affecter des ressources au plan :

1. Dans le volet de navigation de gauche, choisissez Machines virtuelles.
2. Choisissez Affectations, puis choisissez Créer une affectation de groupe.
3. Saisissez un Nom d'attribution de ressource.
4. Choisissez un rôle IAM d'attribution de ressources pour créer des sauvegardes et gérer les points de récupération. Si vous n'avez pas de rôle IAM spécifique à utiliser, nous vous recommandons le Rôle par défaut qui dispose des autorisations appropriées.
5. Dans la section Groupe de ressources, sélectionnez le menu déroulant Type de groupe. Vos options sont Dossier ou Hyperviseur.

    a. Choisissez Dossier pour attribuer toutes les machines virtuelles d'un dossier sur un hyperviseur. Sélectionnez un Nom de groupe de dossiers, par exemple `datacenter/vm`, à l'aide du menu déroulant. Vous pouvez également choisir d'inclure des Sous-dossiers.

    > **Note**
    >
    > Pour effectuer des attributions basées sur des dossiers, pendant le processus de découverte, balisez AWS Backup les machines virtuelles avec le dossier dans lequel elles les ont trouvées pendant le processus de découverte. Si vous déplacez ultérieurement une machine virtuelle vers un autre dossier, vous AWS Backup ne pourrez pas mettre à jour la balise pour vous en raison des meilleures pratiques en matière de AWS balisage. Cette méthode d'attribution peut entraîner la poursuite des sauvegardes des machines virtuelles que vous avez déplacées hors du dossier qui vous a été attribué.

    b. Choisissez Hyperviseur pour attribuer toutes les machines virtuelles gérées par un hyperviseur. Sélectionnez le Nom de groupe d'un ID d'hyperviseur à l'aide du menu déroulant.
6. Dans la section Plan de sauvegarde, choisissez un Plan de sauvegarde existant dans la liste déroulante. Vous pouvez également choisir Créer un plan de sauvegarde pour créer un nouveau plan de sauvegarde.
7. Choisissez Créer une affectation de groupe.
8. Facultatif : vérifiez que vos machines virtuelles sont attribuées à un plan de sauvegarde en choisissant Afficher le plan de sauvegarde. Dans la section Attributions de ressources, choisissez le Nom de l'attribution de ressources.

Étapes suivantes

Pour restaurer une machine virtuelle, consultez Restauration d'une machine virtuelle à l'aide de AWS Backup.

Informations sur les composants source tiers pour Backup gateway

Dans cette section, vous pouvez trouver des informations sur les outils et licences tiers dont nous dépendons pour fournir les fonctionnalités Backup gateway.

Le code source de certains composants de logiciels source tiers qui sont inclus dans le logiciel Backup gateway est disponible en téléchargement aux emplacements suivants :

- Pour les passerelles déployées sur VMware ESXi, téléchargez sources.tgz.

Ce produit inclut un logiciel développé par le projet OpenSSL pour être utilisé dans le kit d'outils OpenSSL (https://www.openssl.org/).

Ce produit inclut un logiciel développé par le kit de développement logiciel VMware® vSphere (https://www.vmware.com).

Pour connaître les licences pertinentes pour tous les outils tiers dépendants, consultez Licences tierces.

Composants open source pour AWS Appliance

Plusieurs outils et licences tiers sont utilisés pour fournir des fonctionnalités pour Backup gateway.

Utilisez les liens suivants pour télécharger le code source de certains composants logiciels open source inclus dans le logiciel AWS Appliance :

- Pour les passerelles déployées sur VMware ESXi, téléchargez sources.tar

Ce produit inclut un logiciel développé par le projet OpenSSL pour être utilisé dans le kit d'outils OpenSSL (https://www.openssl.org/). Pour connaître les licences pertinentes pour tous les outils tiers dépendants, consultez Licences tierces.

Résolution des problèmes de machines virtuelles

Sauvegardes incrémentielles/problèmes et messages CBT

Message d'échec : **`"The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."`**

Si ce message persiste, réinitialisez le CBT comme indiqué par VMware.

Le message indique que le CBT n'était pas activé ou n'était pas disponible : « VMware Change Block Tracking (CBT) n'était pas disponible pour cette machine virtuelle, mais la sauvegarde incrémentielle a été effectuée grâce à notre mécanisme de modification propriétaire. »

Vérifiez que le CBT est activé. Pour vérifier si le CBT est activé sur un disque virtuel, procédez comme suit :

1. Ouvrez le client vSphere et sélectionnez une machine virtuelle hors tension.
2. Cliquez avec le bouton droit sur la machine virtuelle et accédez à Modifier les paramètres > Options > Avancé/Général > Paramètres de configuration.
3. L'option `ctkEnabled` doit être égale à `True`.

S'il est activé, assurez-vous d'utiliser les fonctionnalités de up-to-date VMware. L'hôte doit être ESXi version 4.0 ou ultérieure et la machine virtuelle propriétaire des disques à suivre doit être dotée de matériel version 7 ou ultérieure.

Si le CBT est activé et que le logiciel et le matériel sont à jour, éteignez la machine virtuelle, puis réactivez-la. Assurez-vous que le CBT est activé. Effectuez ensuite à nouveau la sauvegarde.

Sauvegarde DynamoDB avancée

AWS Backup prend en charge des fonctionnalités avancées supplémentaires pour répondre à vos besoins en matière de protection des données Amazon DynamoDB. Après avoir activé AWS Backup les fonctionnalités avancées dans votre Région AWS, vous débloquez les fonctionnalités suivantes pour toutes les nouvelles sauvegardes de tables DynamoDB que vous créez :

- Réduction des coûts et optimisation :
  - Hiérarchisation des sauvegardes vers le stockage à froid pour réduire les coûts de stockage
  - Balisage de répartition des coûts à utiliser avec Cost Explorer

- Continuité de l'activité :
  - Copie entre régions
  - Copie entre comptes
- Sécurité:
  - Stockez les sauvegardes dans des coffres-forts AWS Backup chiffrés, que vous pouvez sécuriser à l'aide d'AWS Backup Vault Lock, de politiques AWS Backup et de clés de chiffrement.
  - Les sauvegardes héritent des balises de leurs tables DynamoDB source, ce qui vous permet de les utiliser pour définir des autorisations et des politiques de contrôle des services (SCP).

Les fonctionnalités avancées de sauvegarde DynamoDB sont activées par défaut pour les nouveaux clients qui s'inscrivent AWS Backup après novembre 2021. Plus précisément, les fonctionnalités avancées de sauvegarde DynamoDB sont activées par défaut pour les clients qui n'ont pas créé de coffre-fort de sauvegarde avant le 21 novembre 2021.

Nous recommandons à tous les AWS Backup clients existants d'activer les fonctionnalités avancées de DynamoDB. Il n'y a aucune différence dans le prix du stockage de sauvegarde à chaud une fois que vous avez activé les fonctionnalités avancées. Vous pouvez économiser de l'argent en hiérarchisant les sauvegardes vers le stockage à froid et optimiser vos coûts en utilisant des balises de répartition des coûts. Vous pouvez également commencer à tirer parti des fonctionnalités AWS Backup de continuité des activités et de sécurité de l'établissement.

> **Note**
>
> Si vous utilisez un rôle ou une politique personnalisé au lieu AWS Backup du rôle de service par défaut, vous devez ajouter ou utiliser les politiques d'autorisation suivantes (ou ajouter leurs autorisations équivalentes) à votre rôle personnalisé :
>
> - `AWSBackupServiceRolePolicyForBackup` pour effectuer une sauvegarde DynamoDB avancée.
> - `AWSBackupServiceRolePolicyForRestores` pour restaurer des sauvegardes DynamoDB avancées.
>
> Pour en savoir plus sur les politiques AWS gérées et consulter des exemples de politiques gérées par le client, consultez. Politiques gérées pour AWS Backup

Rubriques

Activation de la sauvegarde DynamoDB avancée à l'aide de la console

Vous pouvez activer les fonctionnalités AWS Backup avancées pour les sauvegardes DynamoDB à l'aide de la console DynamoDB AWS Backup ou de DynamoDB.

Pour activer les fonctionnalités avancées de sauvegarde DynamoDB depuis la console : AWS Backup

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le menu de navigation de gauche, choisissez Paramètres.
3. Dans la section Services pris en charge, vérifiez que DynamoDB est Activé.

   Si ce n'est pas le cas, choisissez Activation et activez DynamoDB en tant que service pris en charge par AWS Backup .
4. Dans la section Fonctionnalités avancées pour les sauvegardes DynamoDB, choisissez Activer.
5. Choisissez Activer les fonctions.

Pour savoir comment activer les fonctionnalités AWS Backup avancées à l'aide de la console DynamoDB, consultez la section AWS Backup Activation des fonctionnalités dans le guide de l'utilisateur d'Amazon DynamoDB.

Activation de la sauvegarde DynamoDB avancée par programmation

Vous pouvez également activer les fonctionnalités AWS Backup avancées pour les sauvegardes DynamoDB à l'aide de la AWS Command Line Interface (CLI). Vous activez les sauvegardes DynamoDB avancées lorsque vous définissez les deux valeurs suivantes sur `true` :

Pour activer par programmation les fonctionnalités AWS Backup avancées pour les sauvegardes DynamoDB :

1. Vérifiez si vous avez déjà activé les fonctionnalités AWS Backup avancées de DynamoDB à l'aide de la commande suivante :

   ```
   $ aws backup describe-region-settings
   ```

   Si `"DynamoDB":true` sous les options `"ResourceTypeManagementPreference"` et `"ResourceTypeOptInPreference"`,vous avez déjà activé la sauvegarde DynamoDB avancée.

   Si, comme dans le résultat suivant, vous possédez au moins une instance de `"DynamoDB":false`, vous n'avez pas encore activé la sauvegarde DynamoDB avancée. Passez à l'étape suivante.

   ```
   {
     "ResourceTypeManagementPreference":{
       "DynamoDB":false,
       "EFS":true
     }
     "ResourceTypeOptInPreference":{
       "Aurora":true,
       "DocumentDB":false,
       "DynamoDB":false,
       "EBS":true,
       "EC2":true,
       "EFS":true,
       "FSx":true,
       "Neptune":false,
       "RDS":true,
       "Storage Gateway":true
     }
   }
   ```

2. Utilisez l'opération UpdateRegionSettings suivante pour définir `"ResourceTypeManagementPreference"` et `"ResourceTypeOptInPreference"` sur `"DynamoDB":true` :

   ```
   aws backup update-region-settings \
                --resource-type-opt-in-preference DynamoDB=true \
   ```

```
    --resource-type-management-preference DynamoDB=true
```

Modification d'une sauvegarde DynamoDB avancée

Lorsque vous créez une sauvegarde DynamoDB après avoir activé les fonctionnalités avancées, vous pouvez l'utiliser AWS Backup pour : AWS Backup

- Copier une sauvegarde dans plusieurs régions
- Copier une sauvegarde dans plusieurs comptes
- Modifier le moment AWS Backup où une sauvegarde est transférée en stockage à froid
- Balisage de la sauvegarde

Pour utiliser ces fonctionnalités avancées sur une sauvegarde existante, consultez Modification d'une sauvegarde.

Si vous désactivez ultérieurement les fonctionnalités AWS Backup avancées de DynamoDB, vous pouvez continuer à effectuer ces opérations sur les sauvegardes DynamoDB que vous avez créées pendant la période pendant laquelle vous avez activé les fonctionnalités avancées.

Restauration d'une sauvegarde DynamoDB avancée

Vous pouvez restaurer les sauvegardes DynamoDB effectuées AWS Backup avec les fonctionnalités avancées activées de la même manière que vous restaurez les sauvegardes DynamoDB effectuées avant l'activation des fonctionnalités avancées. AWS Backup Vous pouvez effectuer une restauration à l'aide de l'un ou de l'autre AWS Backup ou de DynamoDB.

Vous pouvez définir le mode de chiffrement de votre table récemment restaurée à l'aide des options suivantes :

- Lorsque vous effectuez une restauration dans la même région que votre table d'origine, vous pouvez éventuellement spécifier une clé de chiffrement pour la table restaurée. Si vous ne spécifiez pas de clé de chiffrement, la table restaurée AWS Backup sera automatiquement chiffrée à l'aide de la même clé que celle utilisée pour chiffrer la table d'origine.
- Lorsque vous effectuez une restauration dans une région différente de celle de votre table d'origine, vous devez spécifier une clé de chiffrement.

Pour rétablir l'utilisation AWS Backup, voirRestauration d'une table Amazon DynamoDB.

Pour effectuer une restauration à l'aide de DynamoDB, consultez Restauration d'une table DynamoDB à partir d'une sauvegarde dans le Guide de l'utilisateur Amazon DynamoDB.

Suppression d'une sauvegarde DynamoDB avancée

Vous ne pouvez pas supprimer les sauvegardes créées à l'aide de ces fonctionnalités avancées dans DynamoDB. Vous devez utiliser AWS Backup pour supprimer des sauvegardes afin de maintenir la cohérence globale dans l'ensemble de votre environnement AWS .

Pour supprimer une sauvegarde DynamoDB, consultez Suppression de sauvegardes.

Autres avantages de la gestion complète d' AWS Backup lorsque vous activez la sauvegarde DynamoDB avancée

Lorsque vous activez les fonctionnalités AWS Backup avancées de DynamoDB, vous déléguez la gestion complète de vos sauvegardes DynamoDB à. AWS Backup Cela vous donne les avantages supplémentaires suivants :

Chiffrement

AWS Backup chiffre automatiquement les sauvegardes avec la clé KMS de votre AWS Backup coffre-fort de destination. Auparavant, elles étaient chiffrées à l'aide de la même méthode de chiffrement que votre table DynamoDB source. Cela augmente le nombre de défenses que vous pouvez utiliser pour protéger vos données. Pour plus d'informations, consultez Chiffrement pour les sauvegardes dans AWS Backup.

Amazon Resource Name (ARN)

L'espace de noms de service de chaque ARN de sauvegarde est `awsbackup`. Auparavant, l'espace de noms du service était `dynamodb`. Autrement dit, le début de chaque ARN passera de `arn:aws:dynamodb` à `arn:aws:backup`. Consultez ARN pour AWS Backup dans la Référence de l'autorisation de service.

Grâce à cette modification, vous ou votre administrateur de sauvegarde pouvez créer des stratégies d'accès pour les sauvegardes à l'aide de l'espace de noms de service `awsbackup` qui s'appliquent désormais aux sauvegardes DynamoDB créées après l'activation des fonctionnalités avancées. En utilisant l'espace de noms du service `awsbackup`, vous pouvez également appliquer des politiques aux autres sauvegardes effectuées par AWS Backup. Pour plus d'informations, consultez Contrôle d'accès.

Emplacement des frais sur le relevé de facturation

Les frais relatifs aux sauvegardes (y compris le stockage, les transferts de données, les restaurations et les suppressions anticipées) figurent dans la section « Sauvegarde » de votre AWS facture. Auparavant, les frais apparaissaient sous « DynamoDB » sur votre facture.

Cette modification garantit que vous pouvez utiliser la AWS Backup facturation pour surveiller de manière centralisée vos coûts de sauvegarde. Pour plus d'informations, consultez Mesure, coûts et facturation.

Sauvegardes Amazon Timestream

Amazon Timestream est une base de données de séries temporelles évolutive qui permet de stocker et d'analyser plusieurs milliards de points de données de séries temporelles par jour. Timestream est optimisé pour économiser du temps et des coûts en conservant les données récentes en mémoire et en stockant les données historiques dans un niveau de stockage optimisé en termes de coûts conformément à vos politiques.

Une base de données Timestream contient des tables. Ces tables contiennent des enregistrements et chaque enregistrement est un point de données unique dans une série temporelle. Une série chronologique est une séquence d'enregistrements enregistrés sur un intervalle de temps, tel que le cours d'une action, le niveau d'utilisation de la mémoire d'une instance Amazon EC2 ou un relevé de température. AWS Backup peut sauvegarder et restaurer de manière centralisée les tables Timestream. Vous pouvez copier ces sauvegardes de tables sur d'autres comptes et sur plusieurs autres comptes Régions AWS au sein de la même organisation.

Timestream ne propose pas actuellement de services de sauvegarde et de restauration natifs. Le fait de AWS Backup créer des copies sécurisées de vos tables Timestream peut donc ajouter une couche supplémentaire de sécurité et de résilience à vos ressources.

Sauvegarde des tables Timestream

Vous pouvez sauvegarder les tables Timestream via la AWS Backup console ou à l'aide du. AWS CLI

Il existe deux manières d'utiliser la AWS Backup console pour sauvegarder une table Timestream : à la demande ou dans le cadre d'un plan de sauvegarde.

Création de sauvegardes Timestream à la demande

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.

2. À l'aide du volet de navigation, choisissez Ressources protégées, puis Créer une sauvegarde à la demande.
3. Sur la page Créer une sauvegarde à la demande, choisissez Amazon Timestream.
4. Choisissez le Type de ressource Timestream, puis le nom de la table que vous souhaitez sauvegarder.
5. Dans la fenêtre Sauvegarde, assurez-vous que Créer le backup maintenant est sélectionné. Une sauvegarde est immédiatement lancée et votre cluster s'affiche plus tôt sur la page Ressources protégées.
6. Dans le menu déroulant Transition vers le stockage à froid, vous pouvez définir vos paramètres de transition.
7. Dans Période de rétention, vous pouvez choisir la durée de rétention de votre sauvegarde.
8. Choisissez un coffre-fort de sauvegarde existant ou créez-en un. Si vous choisissez Créer un coffre de sauvegarde, une nouvelle page s'ouvre afin que vous puissiez créer un coffre. Une fois que vous avez terminé, vous revenez à la page Créer une sauvegarde à la demande.
9. Sous Rôle IAM, choisissez Rôle par défaut (si le rôle AWS Backup par défaut n'est pas présent dans votre compte, il sera créé pour vous avec les autorisations appropriées).
10. (Facultatif) Des balises peuvent être ajoutées à votre point de récupération. Si vous souhaitez affecter une ou plusieurs balises à votre sauvegarde à la demande, entrez une clé et une valeur facultative, puis choisissez Add tag (Ajouter une balise).
11. Choisissez Create on-demand backup (Créer une sauvegarde à la demande). Vous accédez ainsi à la page Jobs (Tâches), où vous pouvez consulter une liste des tâches.
12. Choisissez l'ID de tâche de backup du cluster pour voir les détails de cette tâche. Il affichera un statut `Completed`, `In Progress` ou `Failed`. Vous pouvez cliquer sur le bouton Actualiser pour mettre à jour le statut.

Création de sauvegardes Timestream planifiées dans un plan de sauvegarde

Vos sauvegardes planifiées peuvent inclure des tables Timestream s'il s'agit d'une ressource protégée. Pour activer la protection des tables Amazon Timestream :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées.
3. Activez Amazon Timestream.

4. Consultez Attribution de ressources à la console pour inclure des tables Timestream dans un plan existant ou nouveau.

Sous Gérer les plans de backup, vous pouvez choisir de créer un plan de sauvegarde et d'inclure des tables Timestream, ou vous pouvez mettre à jour un plan existant pour inclure des tables Timestream. Lorsque vous ajoutez le type de ressource Timestream, vous pouvez choisir d'ajouter Toutes les tables Timestream ou de cocher les cases à côté des tables que vous souhaitez ajouter sous Sélectionner des types de ressources spécifiques.

La première sauvegarde des tables Timestream sera une sauvegarde complète. Les sauvegardes suivantes seront des sauvegardes incrémentielles.

Une fois que vous avez créé ou modifié votre plan de sauvegarde, accédez à Plans de sauvegarde dans le volet de navigation de gauche. Le plan de sauvegarde que vous avez spécifié doit afficher vos clusters sous Attributions de ressources.

Sauvegarde par programmation

Vous pouvez utiliser le nom d'opération `start-backup-job`. Incluez les paramètres suivants :

```
aws backup start-backup-job \
--backup-vault-name backup-vault-name \
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-
name \
--iam-role-arn arn:aws:iam::account:role/role-name \
--region Région AWS \
--endpoint-url URL
```

Affichage des sauvegardes des tables Timestream

Pour afficher et modifier les sauvegardes de vos tables Timestream dans la console, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Choisissez Coffres-forts de sauvegarde. Cliquez ensuite sur le nom du coffre-fort de sauvegarde qui contient vos tables Timestream.
3. Le coffre-fort de sauvegarde affichera un résumé et une liste des sauvegardes.

    a. Vous pouvez cliquer sur le lien dans la colonne ID du point de récupération, ou

b. Vous pouvez cocher la case située à gauche de l'ID du point de récupération et cliquer sur Actions pour supprimer les points de récupération dont vous n'avez plus besoin.

Restauration d'une table Timestream

Découvrez comment restaurer une table Timestream.

Sauvegarde de bases de données SAP HANA sur des instances Amazon EC2

> **Note**
>
> Services pris en charge par Région AWScontient les régions actuellement prises en charge dans lesquelles les sauvegardes de base de données SAP HANA sur les instances Amazon EC2 sont disponibles.

AWS Backup prend en charge les sauvegardes et les restaurations des bases de données SAP HANA sur les instances Amazon EC2.

Rubriques

- Présentation des bases de données SAP HANA avec AWS Backup
- Conditions préalables à la sauvegarde des bases de données SAP HANA via AWS Backup
- Opérations de sauvegarde SAP HANA dans la console AWS Backup
- Afficher les sauvegardes de base de données SAP HANA
- Utilisation AWS CLI pour les bases de données SAP HANA avec AWS Backup
- Résolution des problèmes de sauvegarde des bases de données SAP HANA
- Glossaire des termes de SAP HANA lors de l'utilisation AWS Backup
- AWS Backup support des bases de données SAP HANA sur les instances EC2 : notes de version

Présentation des bases de données SAP HANA avec AWS Backup

Outre la possibilité de créer des sauvegardes et de restaurer des bases de données, l'intégration d' AWS Backup avec Amazon EC2 Systems Manager pour SAP permet aux clients d'identifier et de baliser les bases de données SAP HANA.

AWS Backup est intégré à AWS Backint Agent pour effectuer des sauvegardes et des restaurations SAP HANA. Pour plus d'informations, consultez AWS Backint.

Conditions préalables à la sauvegarde des bases de données SAP HANA via AWS Backup

Plusieurs conditions préalables doivent être remplies avant que les activités de sauvegarde et de restauration puissent être effectuées. Notez que vous aurez besoin d'un accès administratif à votre base de données SAP HANA et d'autorisations pour créer de nouveaux rôles et politiques IAM dans votre AWS compte afin d'effectuer ces étapes.

Remplissez ces conditions préalables sur Amazon EC2 Systems Manager.

1. Configurer les autorisations requises pour l'instance Amazon EC2 exécutant la base de données SAP HANA
2. Enregistrez vos informations d'identification dans AWS Secrets Manager
3. Installez AWS Backint et AWS Systems Manager pour les agents SAP
4. Vérifier l'agent SSM
5. Vérifier les paramètres
6. Enregistrer la base de données SAP HANA

Il est recommandé d'enregistrer chaque instance HANA une seule fois. Les enregistrements multiples peuvent donner lieu à plusieurs ARN pour la même base de données. Le maintien d'un ARN et d'un enregistrement uniques simplifie la création et la maintenance des plans de sauvegarde et peut également contribuer à réduire la duplication imprévue des sauvegardes.

Opérations de sauvegarde SAP HANA dans la console AWS Backup

Une fois les conditions préalables et le SSM pour les configurations SAP terminés, vous pouvez sauvegarder et restaurer vos bases de données SAP HANA sur EC2.

Activation de la protection des ressources SAP HANA

AWS Backup Pour protéger vos bases de données SAP HANA, SAP HANA doit être activé en tant que ressource protégée. Pour l'activer :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.

2. Dans le panneau de navigation de gauche, choisissez Paramètres.
3. Sous Activation du service, sélectionnez Configurer les ressources.
4. Activez SAP HANA sur Amazon EC2.
5. Cliquez sur Confirmer.

Le service SAP HANA sur Amazon EC2 sera désormais activé.

Création d'une sauvegarde planifiée des bases de données SAP HANA

Vous pouvez modifier un plan de sauvegarde existant et y ajouter des ressources SAP HANA, ou vous pouvez créer un nouveau plan de sauvegarde uniquement pour les ressources SAP HANA.

Si vous choisissez de créer un nouveau plan de sauvegarde, trois options s'offrent à vous :

1. Option 1 : démarrer avec un modèle
    1. Choisissez un modèle de plan de sauvegarde.
    2. Spécifiez un nom de plan de sauvegarde.
    3. Cliquez sur Créer un plan.
2. Option 2 : élaborer un nouveau plan
    1. Spécifiez un nom de plan de sauvegarde.
    2. (Facultatif) Spécifiez les balises à ajouter au plan de sauvegarde.
    3. Spécifiez la configuration des règles de sauvegarde.
        a. Spécifiez un nom de règle de sauvegarde.
        b. Sélectionnez un coffre-fort de sauvegarde existant ou créez-en un. C'est ici que vos sauvegardes sont stockées.
        c. Spécifiez une fréquence de sauvegarde.
        d. Spécifiez une fenêtre de sauvegarde.

            Notez que la transition vers le stockage à froid n'est actuellement pas prise en charge.
        e. Spécifiez la période de rétention.

            La copie vers la destination n'est actuellement pas prise en charge
        f. (Facultatif) Spécifiez les balises à ajouter aux points de récupération.
    4. Cliquez sur Créer un plan.

3. Option 3 : définir un plan à l'aide de JSON

    1. Spécifiez le JSON de votre plan de sauvegarde en modifiant l'expression JSON d'un plan de sauvegarde existant ou en créant une nouvelle expression.
    2. Spécifiez un nom de plan de sauvegarde.
    3. Cliquez sur Valider l'expression JSON.

    Une fois le plan de sauvegarde créé, vous pouvez attribuer des ressources au plan de sauvegarde à l'étape suivante.

Quel que soit le plan que vous utilisez, assurez-vous d'attribuer les ressources. Vous pouvez choisir les bases de données SAP HANA à attribuer, y compris les bases de données système et locataire. Vous avez également la possibilité d'exclure des ID de ressource spécifiques.

Créez une sauvegarde à la demande des bases de données SAP HANA

Vous pouvez créer une sauvegarde à la demande complète qui s'exécute immédiatement après sa création. Notez que les sauvegardes à la demande des bases de données SAP HANA sur les instances Amazon EC2 sont des sauvegardes complètes ; les sauvegardes incrémentielles ne sont pas prises en charge.

Votre sauvegarde à la demande est à présent créée. Elle commencera à sauvegarder les ressources que vous avez spécifiées. La console vous redirigera vers la page des Tâches de sauvegarde, où vous pouvez voir la progression des tâches. Notez l'ID de la tâche de sauvegarde indiqué dans la bannière bleue en haut de votre écran, car vous en aurez besoin pour trouver facilement le statut de votre tâche de sauvegarde. Lorsque la sauvegarde est terminée, le statut passe à `Completed`. Les sauvegardes peuvent prendre plusieurs heures.

Actualisez la Liste des tâches de sauvegarde pour voir le changement de statut. Vous pouvez également rechercher et cliquer sur votre ID de tâche de backup pour afficher le statut détaillé de la tâche.

Sauvegardes continues des bases de données SAP HANA

Vous pouvez effectuer des sauvegardes continues, qui peuvent être utilisées avec la point-in-time restauration (PITR) (notez que les sauvegardes à la demande préservent les ressources dans l'état dans lequel elles ont été prises, tandis que PITR utilise des sauvegardes continues qui enregistrent les modifications au fil du temps).

Avec les sauvegardes continues, vous pouvez restaurer votre base de données SAP HANA sur une instance EC2 en la rétablissant à l'heure précise de votre choix, avec une seconde de précision (en remontant au maximum 35 jours en arrière). La sauvegarde continue fonctionne en créant d'abord une sauvegarde complète de votre ressource, puis en sauvegardant constamment les journaux de transactions de votre ressource. La restauration PITR fonctionne en accédant à votre sauvegarde complète et en relisant le journal des transactions jusqu'à l'heure indiquée AWS Backup pour la restauration.

Vous pouvez opter pour les sauvegardes continues lorsque vous créez un plan de sauvegarde à AWS Backup l'aide de la AWS Backup console ou de l'API.

Pour activer les sauvegardes continues à l'aide de la console

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sous Règles de sauvegarde, choisissez Ajouter une règle de sauvegarde.
4. Dans la section Configuration de règle de backup, sélectionnez Activer les sauvegardes continues pour les ressources prises en charge.

Une fois que vous avez désactivé le PITR (point-in-timerestauration) pour les sauvegardes de base de données SAP HANA, les journaux continueront d'être envoyés AWS Backup jusqu'à expiration du point de restauration (statut égal à). `EXPIRED`) Vous pouvez passer à un autre emplacement de sauvegarde des journaux dans SAP HANA pour arrêter la transmission des journaux à AWS Backup.

Un point de restauration continue dont l'état est égal à `STOPPED` indique qu'un point de restauration continue a été interrompu ; en d'autres termes, les journaux transmis par SAP HANA à AWS Backup ce point et indiquant les modifications incrémentielles apportées à une base de données présentent une lacune. Les points de récupération qui se produisent pendant cet intervalle de temps ont un statut `STOPPED`..

Pour les problèmes que vous pouvez rencontrer lors des tâches de sauvegardes continues (points de récupération), consultez la section Dépannage de la restauration SAP HANA dans ce guide.

Afficher les sauvegardes de base de données SAP HANA

Affichage du statut de vos tâches de sauvegarde et de récupération :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.

2. Dans le volet de navigation, sélectionnez Tâches.
3. Choisissez des tâches de sauvegarde, des tâches de restauration ou des tâches de copie pour voir la liste de vos tâches.
4. Recherchez et cliquez sur votre ID de tâche pour afficher les statuts détaillés de la tâche.

Affichage de tous les points de récupération dans un coffre :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Recherchez et cliquez sur un coffre-fort de sauvegarde pour afficher tous les points de récupération qu'il contient.

Affichage des détails des ressources protégées :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Protected resources (Ressources protégées).
3. Vous pouvez également filtrer par type de ressource pour afficher toutes les sauvegardes de ce type de ressource.

Utilisation AWS CLI pour les bases de données SAP HANA avec AWS Backup

Chaque action dans la console Backup est associée à un appel d'API correspondant.

Pour configurer AWS Backup et gérer ses ressources par programmation, utilisez l'appel d'API `StartBackupJob`pour sauvegarder une base de données SAP HANA sur une instance EC2.

Utilisez `start-backup-job` comme commande de l'interface de ligne de commande.

Résolution des problèmes de sauvegarde des bases de données SAP HANA

Si vous rencontrez des erreurs au cours de votre flux de travail, consultez les exemples d'erreurs suivants et les solutions suggérées :

Prérequis pour Python

- Erreur : erreur Zypper liée à la version de Python depuis SSM pour SAP et nécessitant AWS Backup Python 3.6, mais SUSE 12 SP5 prend en charge Python 3.4 par défaut.

Résolution : installez plusieurs versions de Python sur SUSE12 SP5 en procédant comme suit :

1. Exécutez une commande update-alternatives pour créer un lien symbolique pour Python 3 dans « /usr/local/bin/ » au lieu d'utiliser directement « /usr/bin/python3 ». Cette commande définira Python 3.4 comme version par défaut. La commande est la suivante : `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.4 5`
2. Ajoutez Python 3.6 à la configuration alternative en exécutant la commande suivante : `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
3. Modifiez la configuration alternative en Python 3.6 en exécutant la commande suivante : `# sudo update-alternatives –config python3`

   Le résultat suivant doit être affiché :

   ```
   There are 2 choices for the alternative python3 (providing /usr/local/bin/python3).
    Selection Path Priority Status
   * 0 /usr/bin/python3.4 5 auto mode
    1 /usr/bin/python3.4 5 manual mode
    2 /usr/bin/python3.6 2 manual mode
   Press enter to keep the current choice[*], or type selection number:
   ```
4. Entrez le numéro correspondant à Python 3.6.
5. Vérifiez la version de Python et confirmez que Python 3.6 est utilisé.
6. (Facultatif, mais recommandé) Vérifiez que les commandes Zypper fonctionnent comme prévu.

Amazon EC2 Systems Manager pour la découverte et l'enregistrement de SAP

- Erreur : SSM pour SAP n'a pas réussi à découvrir la charge de travail en raison du blocage de l'accès au point de terminaison public pour AWS Secrets Manager et SSM.

  Solution : testez si les points de terminaison sont accessibles depuis votre base de données SAP HANA. S'ils ne peuvent pas être atteints, vous pouvez créer des points de terminaison Amazon VPC AWS Secrets Manager et SSM pour SAP.

  1. Testez l'accès à Secrets Manager depuis l'hôte Amazon EC2 pour HANA DB en exécutant la commande suivante :. `aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp` Si la commande ne renvoie aucune valeur, le pare-

feu bloque l'accès au point de terminaison du service Secrets Manager. Le journal s'arrêtera à l'étape « Récupération des secrets depuis Secrets Manager ».

2. Testez la connectivité au SSM pour le point de terminaison SAP en exécutant la commande`aws ssm-sap list-registration`. Si la commande ne renvoie aucune valeur, le pare-feu bloque l'accès au point de terminaison SSM pour SAP.

   Exemple d'erreur :`Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`.

Deux options s'offrent à vous si les points de terminaison ne sont pas accessibles.

- Ouvrez des ports de pare-feu pour autoriser l'accès au point de terminaison de service public pour Secrets Manager et SSM pour SAP ; ou,
- Créez des points de terminaison VPC pour Secrets Manager et SSM pour SAP, puis :
  - Assurez-vous qu'Amazon VPC est activé pour DNSSupport et DNSHostname.
  - Assurez-vous que votre point de terminaison VPC a activé l'option Autoriser le nom DNS privé.
  - Si le SSM pour SAP Discovery s'est terminé avec succès, le journal indiquera que l'hôte a été découvert.

- Erreur : AWS Backup et la connexion Backint échoue en raison d'un accès bloqué aux points de terminaison publics du AWS Backup service. `aws-backint-agent.log`peut afficher des erreurs similaires à celles-ci : `time="2024-01-03T11:39:15-08:00" level=error msg="Storage configuration validation failed: missing backup data plane Id" oulevel=fatal msg="Error performing backup missing backup data plane Id`. En outre, la AWS Backup console peut afficher `Fatal Error: An internal error occured.`

  Résolution : deux options s'offrent à vous si les points de terminaison ne sont pas accessibles :

  - Ouvrez les ports de pare-feu pour autoriser l'accès aux points de terminaison de service public (HTTPS). Une fois cette option utilisée, le DNS résoudra les demandes adressées aux AWS services via des adresses IP publiques.
  - Créez des points de terminaison VPC pour acheminer de manière privée le trafic vers et depuis les AWS services requis pour. AWS Backup Une fois cette option utilisée, le DNS résoudra les demandes relatives à ces services via des adresses IP privées. Cette option peut nécessiter des mises à jour du serveur DNS afin d'ajouter des règles permettant de transférer les demandes vers des points de terminaison privés.

- Erreur : L'enregistrement de SSM pour SAP échoue car le mot de passe HANA contient des caractères spéciaux. Les erreurs peuvent inclure `Error connecting to database HBX/HBX when validating its credentials.` ou `Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.` après avoir testé une connexion à l'aide de hdbsql for `systemdb` et `tenantdb` qui a été testée à partir de l'instance Amazon EC2 de la base de données HANA.

  Dans la AWS Backup console de la page Tâches, les détails de la tâche de sauvegarde peuvent indiquer un état `FAILED` d'erreur`Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’`.

  Résolution : Assurez-vous que votre mot de passe ne contient pas de caractères spéciaux, tels que $.

- Erreur : **`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  Résolution : L'installation de l' AWS BackInt agent pour SAP HANA ne s'est peut-être pas terminée correctement. Réessayez le processus pour déployer le AWS Backint Agent et l'agent Amazon EC2 Systems Manager sur votre serveur d'applications SAP.

- Erreur : la console ne correspond pas aux fichiers journaux après l'enregistrement.

  Le journal de découverte indique l'échec de l'enregistrement lors de la tentative de connexion à HANA DB en raison de la présence de caractères spéciaux dans le mot de passe, bien que la console SSM for SAP Application Manager for SAP indique que l'enregistrement a bien été effectué. Il ne confirme pas que l'enregistrement a bien été effectué. Si la console indique un enregistrement réussi, mais pas les journaux, les sauvegardes échoueront.

  Confirmez le statut de l'enregistrement :

  1. Connectez-vous à la console SSM
  2. Sélectionnez Exécuter la commande dans le menu de navigation de gauche.
  3. Dans le champ de texte Historique des commandes, entrez`Instance ID:Equal:`, avec la valeur égale à l'instance que vous avez utilisée pour l'enregistrement. Cela filtrera l'historique des commandes.
  4. Utilisez la colonne command id pour rechercher les commandes dont le statut est défini`Failed`. Recherchez ensuite le nom du document AWSSystemsManagerSAP-Discovery.
  5. Dans le AWS CLI, exécutez la commande`aws ssm-sap register-application status`. Si la valeur renvoyée s'affiche`Error`, l'enregistrement a échoué.

Solution : Assurez-vous que votre mot de passe HANA ne comporte pas de caractères spéciaux (tels que « $ »).

Création d'une sauvegarde d'une base de données SAP HANA

- Erreur : AWS Backup la console affiche le message « Erreur fatale » lorsqu'une sauvegarde à la demande pour SystemDB ou TenantDB est créée. Cela se produit car le point de terminaison public cell-1.prod.us-west-2.storage.cryo.aws.a2z.com n'est pas accessible. Cela est dû à un pare-feu côté client qui bloque l'accès à ce point de terminaison.

  `aws-backint-agent.log`peut afficher des erreurs telles que `level=error msg="Storage configuration validation failed: missing backup data plane Id"` ou `level=fatal msg="Error performing backup missing backup data plane Id."`

  Résolution : accès par pare-feu ouvert au point de terminaison public cell-1.prod.us-west-2.storage.cryo.aws.a2z.com.
- Erreur :`Database cannot be backed up while it is stopped`.

  Résolution : assurez-vous que la base de données à sauvegarder est active. Les données et journaux de base de données ne peuvent être sauvegardés que tant que la base de données est en ligne.
- Erreur : `Getting backup metadata failed. Check the SSM document execution for more details.`

  Résolution : assurez-vous que la base de données à sauvegarder est active. Les données et journaux de base de données ne peuvent être sauvegardés que tant que la base de données est en ligne.

Surveillance des journaux de sauvegarde

- Erreur : `Encountered an issue with log backups, please check SAP HANA for details.`

  Solution : Vérifiez SAP HANA pour vous assurer que les sauvegardes des journaux sont envoyées AWS Backup depuis SAP HANA.
- Erreur : `One or more log backup attempts failed for recovery point.`

Résolution : vérifiez SAP HANA pour plus de détails. Assurez-vous que les sauvegardes des journaux sont envoyées AWS Backup depuis SAP HANA.

- Erreur : `Unable to determine the status of log backups for recovery point.`

  Résolution : vérifiez SAP HANA pour plus de détails. Assurez-vous que les sauvegardes des journaux sont envoyées AWS Backup depuis SAP HANA.

- Erreur : `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  Résolution : attendez que la tâche de restauration soit terminée. Les sauvegardes du journal devraient reprendre.

Glossaire des termes de SAP HANA lors de l'utilisation AWS Backup

Types de sauvegarde des données : SAP HANA prend en charge deux types de sauvegardes de données : les sauvegardes complètes et les sauvegardes INC (incrémentielles). AWS Backup optimise le type utilisé lors de chaque opération de sauvegarde.

Sauvegardes de catalogue : SAP HANA gère son propre manifeste appelé catalogue. AWS Backup interagit avec ce catalogue. Chaque nouvelle sauvegarde créera une entrée dans le catalogue.

Sauvegarde continue des journaux (journaux des transactions) : pour les fonctions de récupération ponctuelle (PITR), SAP HANA suit toutes les transactions depuis la dernière sauvegarde.

Copie système : tâche de restauration dans laquelle la base de données cible de restauration est différente de la base de données source à partir de laquelle le point de récupération a été créé.

Restauration destructive : une restauration destructive est un type de tâche de restauration au cours de laquelle une base de données restaurée supprime ou remplace la base de données source ou existante.

FULL : une sauvegarde d'une base de données complète.

INC : une sauvegarde incrémentielle est une sauvegarde de toutes les modifications apportées à une base de données SAP HANA depuis la sauvegarde précédente.

Pour plus de détails, consultez le Glossaire AWS.

AWS Backup support des bases de données SAP HANA sur les instances EC2 : notes de version

Certaines fonctionnalités ne sont pas prises en charge pour le moment :

- La copie entre comptes et entre régions n'est pas prise en charge.
- Backup Audit Manager et les rapports ne sont actuellement pas pris en charge.
- Services pris en charge par Région AWScontient les régions actuellement prises en charge pour les sauvegardes de base de données SAP HANA sur les instances Amazon EC2.

Sauvegardes Amazon Redshift

Amazon Redshift est un entrepôt des données cloud évolutif et entièrement géré qui vous permet d'obtenir plus rapidement des informations grâce à des analyses rapides, simples et sécurisées. Vous pouvez l'utiliser AWS Backup pour protéger vos entrepôts de données grâce à des sauvegardes immuables, à des politiques d'accès distinctes et à une gouvernance organisationnelle centralisée des tâches de sauvegarde et de restauration.

Un entrepôt de données Amazon Redshift est un ensemble de ressources informatiques appelées nœuds, qui sont organisées en un groupe appelé cluster. AWS Backup peut sauvegarder ces clusters.

Pour en savoir plus sur Amazon Redshift, consultez le Guide de démarrage Amazon Redshift, le Manuel du développeur de base de données Amazon Redshift et le Guide de la gestion du cluster Amazon Redshift.

Sauvegarde des clusters Amazon Redshift provisionnés

Vous pouvez protéger vos clusters Amazon Redshift à l'aide de la AWS Backup console ou par programmation à l'aide d'une API ou d'une CLI. Ces clusters peuvent être sauvegardés selon une planification régulière dans le cadre d'un plan de sauvegarde, ou ils peuvent être sauvegardés selon les besoins via une sauvegarde à la demande.

Vous pouvez restaurer une seule table (également appelée restauration au niveau des éléments) ou un cluster entier. Notez que les tables ne peuvent pas être sauvegardées seules ; les tables sont sauvegardées dans le cadre d'un cluster lors de la sauvegarde du cluster.

L'utilisation vous AWS Backup permet de visualiser vos ressources de manière centralisée ; toutefois, si Amazon Redshift est la seule ressource que vous utilisez, vous pouvez continuer à utiliser le

planificateur de snapshots automatique dans Amazon Redshift. Notez que vous ne pouvez pas continuer à gérer les paramètres manuels des instantanés à l'aide d'Amazon Redshift si vous choisissez de les gérer via. AWS Backup

Vous pouvez sauvegarder des clusters Amazon Redshift via la AWS Backup console ou à l'aide du. AWS CLI

Il existe deux manières d'utiliser la AWS Backup console pour sauvegarder un cluster Amazon Redshift : à la demande ou dans le cadre d'un plan de sauvegarde.

Création de sauvegardes Amazon Redshift à la demande

Consultez la page Création d'une sauvegarde à la demande pour plus d'informations.

Pour créer un instantané manuel, laissez la case Sauvegarde continue décochée lorsque vous créez un plan de sauvegarde incluant les ressources Amazon Redshift.

Création de sauvegardes Amazon Redshift planifiées dans un plan de sauvegarde

Vos sauvegardes planifiées peuvent inclure des clusters Amazon Redshift s'il s'agit d'une ressource protégée. Pour activer la protection des tables Amazon Redshift :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées.
3. Activez Amazon Redshift.
4. Consultez Attribution de ressources à la console pour inclure des clusters Amazon Redshift dans un plan existant ou nouveau.

Sous Gérer les plans de backup, vous pouvez choisir de créer un plan de sauvegarde et d'inclure des clusters Amazon Redshift ou vous pouvez mettre à jour un plan existant pour inclure des clusters Amazon Redshift. Lorsque vous ajoutez le type de ressource Amazon Redshift, vous pouvez choisir d'ajouter Tous les clusters Amazon Redshift ou de cocher les cases à côté des clusters.

Sauvegarde par programmation

Vous pouvez également définir votre plan de sauvegarde dans un document JSON et le fournir à l'aide de la AWS Backup console ou AWS CLI. Voir Création de plans de sauvegarde à l'aide d'un document JSON et de la AWS Backup CLI pour savoir comment créer un plan de sauvegarde par programmation.

Vous pouvez effectuer les opérations suivantes avec l'API :

- Arrêter une tâche de sauvegarde.
- Décrire une tâche de sauvegarde
- Obtenir les métadonnées du point de récupération
- Répertorier les points de récupération par ressource
- Répertorier les balises pour le point de récupération

Affichage des sauvegardes de cluster Amazon Redshift

Pour afficher et modifier les sauvegardes de vos tables Amazon Redshift dans la console, procédez comme suit :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Choisissez Coffres-forts de sauvegarde. Cliquez ensuite sur le nom du coffre-fort de sauvegarde qui contient vos clusters Amazon Redshift.
3. Le coffre-fort de sauvegarde affichera un résumé et une liste des sauvegardes. Vous pouvez cliquer sur le lien dans la colonne ID de point de récupération.
4. Pour supprimer un ou plusieurs points de récupération, cochez la ou les cases que vous souhaitez supprimer. Sous le bouton Actions, vous pouvez sélectionner Supprimer.

Restauration d'un cluster Amazon Redshift

Pour plus d'informations, consultez Restauration d'un cluster Amazon Redshift.

Sauvegardes Amazon Relational Database Service

Amazon RDS et AWS Backup

Lorsque vous envisagez les options de sauvegarde de vos instances et clusters Amazon RDS, il est important de préciser le type de sauvegarde que vous souhaitez créer et utiliser. Plusieurs AWS ressources, dont Amazon RDS, proposent leurs propres solutions de sauvegarde natives.

Amazon RDS offre la possibilité d'effectuer des sauvegardes automatisées et des sauvegardes manuelles. Dans la terminologie d'Amazon RDS, tous les points de restauration créés par AWS Backup, y compris ceux d'un plan de sauvegarde, sont considérés comme des sauvegardes manuelles.

Lorsque vous créez une sauvegarde (point de restauration) d'une instance Amazon RDS, AWS Backup vérifie si vous avez déjà utilisé Amazon RDS pour créer une sauvegarde automatique. AWS

Backup S'il existe une sauvegarde automatique, AWS Backup crée une copie de cet instantané (`copy-db-snapshot`opération). S'il n'existe aucune sauvegarde existante, AWS Backup crée un instantané de l'instance que vous indiquez, au lieu d'une copie (`create-db-snapshot`opération).

Le premier instantané créé par AWS Backup, créé par l'une ou l'autre opération, produira un instantané complet. Toutes les copies suivantes seront des sauvegardes incrémentielles, à condition que la sauvegarde complète existe.

> **Important**
>
> Lorsqu'un plan de AWS Backup sauvegarde est planifié pour créer plusieurs instantanés quotidiens d'une instance Amazon RDS, et lorsque l'une de ces fenêtres de démarrage de AWS Backup sauvegarde coïncide avec la fenêtre de sauvegarde Amazon RDS, le lignage des données des sauvegardes peut être bifurqué vers des sauvegardes non identiques, créant ainsi des sauvegardes imprévues et contradictoires. Pour éviter cela, assurez-vous que votre plan AWS Backup de sauvegarde ou votre fenêtre Amazon RDS ne coïncident pas avec leur époque.

Sauvegardes continues et restauration ponctuelle d'Amazon RDS

Les sauvegardes continues impliquent AWS Backup de créer une sauvegarde complète de votre ressource Amazon RDS, puis de capturer toutes les modifications via un journal des transactions. Vous pouvez obtenir une meilleure granularité en revenant au moment où vous souhaitez effectuer la restauration au lieu de choisir un instantané précédent pris à intervalles de temps fixes.

Consultez les sauvegardes continues et les services pris en charge par le PITR et la gestion des paramètres de sauvegarde continue pour plus d'informations.

Sauvegardes à plusieurs zones de disponibilité Amazon RDS

AWS Backup sauvegarde et prend en charge les options de déploiement Amazon RDS pour MySQL et pour PostgreSQL Multi-AZ (zone de disponibilité) avec une instance de base de données principale et deux instances de base de données de secours lisibles.

Les sauvegardes à plusieurs zones de disponibilité sont disponibles dans les régions suivantes : région Asie-Pacifique (Sydney), région Asie-Pacifique (Tokyo), région Europe (Irlande), région USA Est (Ohio), région USA Ouest (Oregon), région Europe (Stockholm), région Asie-Pacifique (Singapour), région USA Est (Virginie du Nord) et région Europe (Francfort).

L'option de déploiement multi-AZ optimise les transactions d'écriture et est idéale lorsque vos charges de travail nécessitent une capacité de lecture supplémentaire, une latence des transactions d'écriture plus faible, une meilleure résilience face à l'instabilité du réseau (qui a un impact sur la cohérence de la latence des transactions d'écriture), ainsi qu'une disponibilité et une durabilité élevées.

Pour créer un cluster multi-AZ, vous pouvez choisir MySQL ou PostgreSQL comme type de moteur.

Dans la AWS Backup console, il existe trois options de déploiement :

- Cluster de base de données multi-AZ : crée un cluster de bases de données avec une instance de base de données principale et deux instances de base de données de secours lisibles, chaque instance de base de données se trouvant dans une zone de disponibilité différente. Assure une haute disponibilité, une redondance des données et augmente la capacité des charges de travail prêtes à être installées sur les serveurs.
- Instance de base de données multi-AZ : crée une instance de base de données primaire avec une instance de base de données de secours dans une zone de disponibilité différente. Cela garantit une haute disponibilité et une redondance des données, mais l'instance de base de données de secours ne prend pas en charge les connexions pour les charges de travail de lecture.
- Instance de base de données unique : crée une instance de base de données unique sans instance de base de données de secours.

Pour créer une sauvegarde pour Amazon RDS, consultez Création d'une sauvegarde pour planifier une sauvegarde dans le cadre de vos plans de sauvegarde ou création d'une sauvegarde à la demande.

> **Note**
>
> La récupération ponctuelle (PITR) peut prendre en charge les instances, mais pas les clusters.
> La copie d'un instantané de cluster de bases de données multi-AZ n'est pas prise en charge.

Différences entre un cluster multi-AZ et une instance RDS

Une sauvegarde dans une seule zone de disponibilité ou dans deux zones de disponibilité est une instance RDS ; un déploiement et une sauvegarde avec trois instances ou plus constituent un cluster, comme les clusters Amazon Aurora, Amazon Neptune et Amazon DocumentDB.

L'ARN (Amazon Resource Name) est rendu différemment selon que l'instance ou le cluster est utilisé :

Un ARN d'instance RDS : `arn:aws:rds:region: account:db:name`

Un cluster à plusieurs zones de disponibilité RDS : `arn:aws:rds:region:account :cluster:name`

Pour plus d'informations, consultez Déploiements de clusters de base de données Multi-AZ dans le Guide de l'utilisateur Amazon RDS.

Pour plus d'informations sur Création d'un instantané de cluster de bases de données multi-AZ, consultez le Guide de l'utilisateur Amazon RDS.

AWS CloudFormation empiler des sauvegardes

Une CloudFormation pile est composée de plusieurs ressources dynamiques et apatrides que vous pouvez sauvegarder en tant qu'unité unique. En d'autres termes, vous pouvez sauvegarder et restaurer une application contenant plusieurs ressources en sauvegardant une pile et en restaurant les ressources qu'elle contient. Toutes les ressources d'une pile sont définies par son modèle AWS CloudFormation .

Lorsqu'une CloudFormation pile est sauvegardée, des points de récupération sont créés pour le CloudFormation modèle et pour chaque ressource supplémentaire prise AWS Backup en charge par la pile. Ces points de récupération sont regroupés au sein d'un point de récupération global appelé composite.

Ce point de récupération composite ne peut pas être restauré, mais les points de récupération imbriqués peuvent être restaurés. Vous pouvez restaurer une ou toutes les sauvegardes imbriquées au sein d'une sauvegarde composite à l'aide de la console ou de l' AWS CLI.

CloudFormation terminologie de la pile d'applications

- Point de récupération composite : point de récupération utilisé pour regrouper les points de récupération imbriqués, ainsi que d'autres métadonnées.
- Point de restauration imbriqué : point de récupération d'une ressource faisant partie d'une CloudFormation pile et sauvegardée dans le cadre du point de récupération composite. Chaque point de récupération imbriqué appartient à la pile d'un point de récupération composite.
- Tâche composite : tâche de sauvegarde, de copie ou de restauration pour une CloudFormation pile qui peut déclencher d'autres tâches de sauvegarde pour des ressources individuelles de la pile.

- Tâche imbriquée : tâche de sauvegarde, de copie ou de restauration d'une ressource au sein d'une AWS CloudFormation pile.

CloudFormation empiler les tâches de sauvegarde

Le processus de création d'une sauvegarde est appelé tâche de sauvegarde. Une tâche de sauvegarde de CloudFormation pile possède un statut. Lorsqu'une tâche de sauvegarde est terminée, elle a le statut `Completed`. Cela signifie qu'un AWS CloudFormation point de récupération (une sauvegarde) a été créée.

CloudFormation les piles peuvent être sauvegardées à l'aide de la console ou sauvegardées par programme. Pour sauvegarder n'importe quelle ressource, y compris une CloudFormation pile, voir Création d'une sauvegarde ailleurs dans ce guide AWS Backup du développeur.

CloudFormation les piles peuvent être sauvegardées à l'aide de la commande `StartBackupJob` API. Notez que la documentation et la console font référence à des points de récupération composites et imbriqués ; le langage de l'API utilise la terminologie « points de récupération parent/enfant » dans la même relation contextuelle.

CloudFormation les piles contenant toutes les AWS ressources sont indiquées par votre CloudFormation modèle. Notez que votre modèle peut contenir des ressources qui ne sont pas encore prises en charge par AWS Backup. Si votre modèle contient une combinaison de ressources AWS prises en charge et de ressources non prises en charge, AWS Backup vous sauvegarderez toujours le modèle dans une pile composite, mais Backup créera uniquement des points de restauration pour les services pris en charge par Backup. Tous les types de ressources contenus dans le CloudFormation modèle seront inclus dans une sauvegarde, même si vous n'avez pas opté pour un service en particulier (en faisant passer un service sur « Activé » dans les paramètres de la console). Les sauvegardes imbriquées (points de récupération) prises en charge par AWS Backup peuvent être restaurées, mais les piles imbriquées ne peuvent pas être sauvegardées ou restaurées.

AWS CloudFormation point de récupération

Statut du point de récupération

Lorsque la tâche de sauvegarde d'une pile est terminée (le statut de la tâche est `Completed`), une sauvegarde de la pile est créée. Cette sauvegarde est également connue sous le nom de point de récupération composite. Un point de récupération composite peut avoir l'un des statuts suivants : `Completed`, `Failed` ou `Partial`. Notez qu'une tâche de sauvegarde possède un statut et qu'un point de récupération (également appelé sauvegarde) possède également un statut distinct.

Une tâche de sauvegarde terminée signifie que l'ensemble de votre pile et les ressources qu'elle contient sont protégées par AWS Backup. Un statut d'échec indique que la tâche de sauvegarde a échoué ; vous devez créer à nouveau la sauvegarde une fois le problème à l'origine de l'échec résolu.

Un statut `Partial` signifie que toutes les ressources de la pile n'ont pas été sauvegardées. Cela peut se produire si le CloudFormation modèle contient des ressources qui ne sont pas actuellement prises en charge par AWS Backup, ou si une ou plusieurs tâches de sauvegarde appartenant aux ressources de la pile (ressources imbriquées) ont un statut autre que. `Completed` Vous pouvez créer manuellement une sauvegarde à la demande pour exécuter à nouveau toutes les ressources dont le statut n'est pas `Completed`. Si vous vous attendiez à ce que la pile ait le statut `Completed` mais qu'il est plutôt `Partial`, vérifiez laquelle des conditions ci-dessus pourrait être vraie pour votre pile.

Chaque ressource imbriquée au sein du point de récupération composite possède son propre point de récupération individuel, chacun ayant son propre statut (`Completed` ou `Failed`). Les points de récupération imbriqués dont le statut est `Completed` peuvent être restaurés.

Gestion des points de récupération

Les points de récupération composite (sauvegardes) peuvent être copiés ; les points de récupération imbriqués peuvent être copiés, supprimés, dissociés ou restaurés. Un point de récupération composite contenant des sauvegardes imbriquées ne peut pas être supprimé. Une fois que les points de récupération imbriqués au sein d'un point de récupération composite ont été supprimés ou dissociés, vous pouvez supprimer manuellement le point de récupération composite ou le laisser subsister jusqu'à ce que le cycle de vie du plan de sauvegarde le supprime.

Suppression d'un point de récupération

Vous pouvez supprimer un point de récupération à l'aide de la AWS Backup console ou du AWS CLI.

Pour supprimer des points de récupération à l'aide de la AWS Backup console,

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Cliquez sur Ressources protégées dans la navigation de gauche. Dans la zone de texte, tapez `CloudFormation` pour afficher uniquement vos CloudFormation piles.
3. Les points de récupération composite seront affichés dans le volet Points de récupération. Vous pouvez cliquer sur le signe plus (+) situé à gauche de l'ID de chaque point de récupération pour

développer chaque point de récupération composite, en affichant tous les points de récupération imbriqués contenus dans le composite. Vous pouvez cocher la case située à gauche de chaque point de récupération pour l'inclure dans votre sélection de points de récupération que vous souhaitez supprimer.

4. Cliquez sur le bouton Supprimer.

Lorsque vous utilisez la console pour supprimer un ou plusieurs points de récupération composite, un message d'avertissement apparaît. Cette boîte d'avertissement vous demande de confirmer votre intention de supprimer les points de récupération composite, y compris les points de récupération imbriqués dans les piles composites.

Pour supprimer des points de récupération à l'aide de l'API, utilisez la commande `DeleteRecoveryPoint`.

Lorsque vous utilisez l'API avec le, AWS Command Line Interface vous devez supprimer tous les points de récupération imbriqués avant de supprimer un point composite. Si vous envoyez une demande d'API pour supprimer une sauvegarde de pile composite (point de récupération) qui contient encore des points de récupération imbriqués, la demande renvoie une erreur.

Dissociation d'un point de récupération imbriqué d'un point de récupération composite

Vous pouvez dissocier un point de récupération imbriqué d'un point de récupération composite (par exemple, vous souhaitez conserver le point de récupération imbriqué mais supprimer le point de récupération composite). Les deux points de récupération resteront, mais ils ne seront plus connectés ; en d'autres termes, les actions effectuées sur le point de récupération composite ne s'appliqueront plus au point de récupération imbriqué une fois celui-ci dissocié.

Vous pouvez dissocier le point de récupération à l'aide de la console ou appeler l'API `DisassociateRecoveryPointFromParent`. [Notez que les appels d'API utilisent le terme « parent » pour désigner les points de récupération composite.]

Copie d'un point de récupération

Vous pouvez copier un point de récupération composite ou un point de récupération imbriqué si la ressource prend en charge la copie entre comptes et entre régions.

Pour copier des points de restauration à l'aide de la AWS Backup console :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.

2. Cliquez sur Ressources protégées dans la navigation de gauche. Dans la zone de texte, tapez `CloudFormation` pour afficher uniquement vos CloudFormation piles.
3. Les points de récupération composite seront affichés dans le volet Points de récupération. Vous pouvez cliquer sur le signe plus (+) situé à gauche de l'ID de chaque point de récupération pour développer chaque point de récupération composite, en affichant tous les points de récupération imbriqués contenus dans le composite. Vous pouvez cliquer sur le bouton circulaire situé à gauche de n'importe quel point de récupération pour le copier.
4. Une fois sélectionné, cliquez sur le bouton Copier dans le coin supérieur droit du volet.

Lorsque vous copiez un point de récupération composite, les points de récupération imbriqués qui ne prennent pas en charge la fonctionnalité de copie ne se retrouveront pas dans la pile copiée. Le point de récupération composite aura le statut `Partial`.

Questions fréquentes (FAQ)

1. « Qu'est-ce qui est inclus dans la sauvegarde de l'application ? »

   Dans le cadre de chaque sauvegarde d'une application définie à l'aide CloudFormation, le modèle, la valeur traitée de chaque paramètre du modèle et les ressources imbriquées prises en charge par AWS Backup sont sauvegardés. Une ressource imbriquée est sauvegardée de la même manière qu'une ressource individuelle ne faisant pas partie d'une CloudFormation pile est sauvegardée. Notez que les valeurs des paramètres marqués comme `no-echo` ne seront pas sauvegardées.

2. « Puis-je sauvegarder ma AWS CloudFormation pile contenant des piles imbriquées ? »

   Oui. Vos CloudFormation piles contenant des piles imbriquées peuvent se trouver dans votre sauvegarde.

3. « Un statut *`Partial`* signifie-t-il que la création de ma sauvegarde a échoué ? »

   Non. Un statut partiel indique que certains points de récupération ont été sauvegardés, tandis que d'autres ne l'ont pas été. Trois conditions permettent de vérifier si vous attendiez un résultat de sauvegarde `Completed` :

   a. Votre CloudFormation pile contient-elle des ressources qui ne sont actuellement pas prises en charge par ? AWS Backup Pour obtenir la liste des ressources prises en charge, consultez

la section AWS Ressources prises en charge et applications tierces dans notre guide du développeur.

b. Une ou plusieurs tâches de sauvegarde appartenant aux ressources de la pile n'ont pas abouti et la tâche doit être à nouveau exécutée.

c. Un point de récupération imbriqué a été supprimé ou dissocié d'un point de récupération composite.

4. « Comment exclure des ressources de ma CloudFormation pile de sauvegarde ? »

   Lorsque vous sauvegardez votre CloudFormation pile, vous pouvez exclure des ressources de la sauvegarde. Dans la console, lors des processus de création d'un plan de sauvegarde et de mise à jour d'un plan de sauvegarde, il existe une étape d'attribution de ressources. Dans cette étape, il existe une section Sélection des ressources. Si vous choisissez d'inclure des types de ressources spécifiques et que vous les avez incluses CloudFormation en tant que ressource à sauvegarder, vous pouvez exclure des identifiants de ressources spécifiques des types de ressources sélectionnés. Vous pouvez également utiliser des balises pour exclure des ressources de la pile.

   Avec l'interface de ligne de commande, vous pouvez utiliser

   - `NotResources`dans votre plan de sauvegarde pour exclure une ressource spécifique de vos CloudFormation piles.
   - `StringNotLike` pour exclure des éléments via des balises.

5. « Quels types de sauvegardes sont pris en charge pour les ressources imbriquées ? »

   Les sauvegardes de ressources imbriquées peuvent être complètes ou incrémentielles, selon le type de sauvegarde pris en charge AWS Backup pour ces ressources. Pour plus d'informations, consultez Fonctionnement des sauvegardes incrémentielles. Notez toutefois que le PITR (point-in-time restauration) n'est pas pris en charge pour les ressources imbriquées Amazon S3 et Amazon RDS.

6. « Les ensembles de modifications qui font partie de la CloudFormation pile sont-ils sauvegardés ? »

   Non Les ensembles de modifications ne sont pas sauvegardés dans le cadre de la sauvegarde par CloudFormation pile.

7. « Quel est l'impact de l'état de la AWS CloudFormation pile sur la sauvegarde ? »

L'état de la CloudFormation pile peut avoir un impact sur la sauvegarde. Une pile avec les statuts suivants peut être sauvegardée : `COMPLETE`, `CREATE_COMPLETE`, `ROLLBACK_COMPLETE`, `UPDATE_COMPLETE`, `UPDATE_ROLLBACK_COMPLETE`, `IMPORT_COMPLETE` ou `IMPORT_ROLLBACK_COMPLETE`.

Si le téléchargement d'un nouveau modèle échoue et que la pile passe au statut `ROLLBACK_COMPLETE`, le nouveau modèle sera sauvegardé, mais les sauvegardes des ressources imbriquées seront basées sur les ressources annulées.

8. « En quoi les cycles de vie des piles d'applications diffèrent-ils des autres cycles de vie des points de récupération ? »

   Les cycles de vie des points de récupération imbriqués sont déterminés par le plan de sauvegarde auquel ils appartiennent. Le point de récupération composite est déterminé par le cycle de vie le plus long de tous les points de récupération imbriqués. Lorsque le dernier point de récupération imbriqué restant dans un point de récupération composite est supprimé ou dissocié, le point de récupération composite est également supprimé.

9. « Comment sont CloudFormation copiées les balises d'un point de récupération ? »

   Oui. Ces balises seront copiées sur chaque point de récupération imbriqué correspondant.

10. « Existe-t-il un ordre pour supprimer les points de restauration composite et imbriqués (sauvegardes) ? »

    Oui. Certaines sauvegardes doivent être supprimées avant que d'autres puissent être supprimées. Les sauvegardes composite contenant des points de récupération imbriqués ne peuvent pas être supprimées tant que tous les points de récupération composite n'ont pas été supprimés. Une fois qu'un point de récupération composite ne contient plus de points de récupération imbriqués, vous pouvez le supprimer manuellement. Dans le cas contraire, il sera supprimé conformément au cycle de vie de son plan de sauvegarde.

Restauration d'applications au sein d'une pile

Consultez Comment restaurer des sauvegardes de pile d'applications pour en savoir plus sur la restauration de points de récupération imbriqués.

Création de sauvegardes Windows VSS

Vous pouvez ainsi sauvegarder et restaurer les applications Windows compatibles VSS (Volume Shadow Copy Service) exécutées sur des instances Amazon EC2. AWS Backup Si l'application possède un enregistreur VSS enregistré auprès de Windows VSS, il AWS Backup crée un instantané qui sera cohérent pour cette application.

Vous pouvez effectuer des restaurations cohérentes, tout en utilisant le même service de sauvegarde géré que celui utilisé pour protéger les autres AWS ressources. Avec les sauvegardes Windows cohérentes par rapport aux applications sur EC2, vous bénéficiez des mêmes paramètres de cohérence et de la même connaissance des applications que les outils de sauvegarde traditionnels.

> **Note**
>
> AWS Backup ne prend actuellement en charge que les sauvegardes cohérentes des ressources exécutées sur Amazon EC2, en particulier 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 Windows.

Pour plus d'informations, consultez la section Création d'un instantané compatible avec les applications VSS dans le guide de l'utilisateur Amazon EC2.

Pour sauvegarder et restaurer des ressources Windows compatibles avec VSS exécutant Amazon EC2, suivez ces étapes pour effectuer les tâches préalables requises. Pour obtenir des instructions, consultez Avant de commencer dans le Guide de l'utilisateur Amazon EC2 pour les instances Windows.

1. Téléchargez, installez et configurez l'agent SSM dans AWS Systems Manager. Cette étape est obligatoire. Pour obtenir des instructions, consultez la section Utilisation de l'agent SSM sur les instances Amazon EC2 pour Windows Server dans le Guide de l'utilisateur de Systems AWS Manager.
2. Ajoutez une politique IAM au rôle IAM et attachez le rôle à l'instance Amazon EC2 avant d'effectuer la sauvegarde Windows VSS (Volume Shadow Copy Service). Pour obtenir des instructions, consultez la section Créer un rôle IAM pour les instantanés compatibles VSS dans le guide de l'utilisateur Amazon EC2. Pour un exemple de politique IAM, consultez Politiques gérées pour AWS Backup.

3. Téléchargez et installez des composants VSS sur l'instance Windows sur Amazon EC2
4. Activez VSS dans AWS Backup :
    1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
    2. Sur le tableau de bord, choisissez le type de sauvegarde que vous souhaitez créer, soit Créer un backup à la demande, soit Gérer les plans de backup. Fournissez les informations nécessaires pour votre type de sauvegarde.
    3. Lorsque vous attribuez des ressources, choisissez EC2. La sauvegarde Windows VSS est actuellement prise en charge uniquement pour les instances EC2.
    4. Dans la section Paramètres avancés, choisissez Windows VSS. Cela vous permet d'effectuer des sauvegardes Windows VSS cohérentes avec les applications.
    5. Créez votre sauvegarde.

Une tâche de sauvegarde dont le statut est `Completed` ne garantit pas la réussite de la partie VSS ; l'inclusion de VSS se fait dans la mesure du possible. Procédez comme suit pour déterminer si une sauvegarde est cohérente avec les applications, si elle résiste aux pannes ou si elle a échoué :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Sous Mon compte dans le menu de navigation de gauche, cliquez sur Tâches.
3. Un statut `Completed` indique une tâche réussie cohérente par rapport aux applications (VSS).

    Un statut `Completed with issues` indique que l'opération VSS a échoué, de sorte que seule une sauvegarde en cas de panne a réussi. Ce statut comportera également un message contextuel `"Windows VSS Backup Job Error encountered, trying for regular backup"`.

    En cas d'échec de la sauvegarde, le statut sera `Failed`.
4. Pour afficher des informations supplémentaires sur la tâche de sauvegarde, cliquez sur la tâche individuelle. Par exemple, les détails peuvent être `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`.

Les sauvegardes compatibles VSS avec une cible autre que Windows ou un composant Windows non VSS dont la tâche est réussie seront cohérentes en cas de crash sans VSS.

Instances Amazon EC2 non prises en charge

Les types d'instances Amazon EC2 suivants ne sont pas pris en charge pour les sauvegardes Windows compatibles avec VSS, car il s'agit de petites instances susceptibles de ne pas effectuer la sauvegarde correctement.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Amazon EBS et AWS Backup

Le processus de sauvegarde des ressources Amazon EBS est similaire aux étapes utilisées pour sauvegarder d'autres types de ressources :

- Création d'une sauvegarde à la demande
- Création d'une sauvegarde planifiée

Des informations spécifiques aux ressources sont indiquées dans les sections suivantes.

Niveau d’archive Amazon EBS pour le stockage à froid

EBS est l’une des ressources qui prend en charge la transition des sauvegardes vers le stockage à froid. Pour plus d’informations, consultez Cycle de vie et niveaux de stockage.

> **Note**
>
> Cette fonctionnalité n'est pas disponible dans les régions Chine (Pékin), Chine (Ningxia), AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest).

Sauvegardes multi-volumes en cas de panne sur Amazon EBS

Par défaut, AWS Backup crée des sauvegardes cohérentes en cas de crash des volumes Amazon EBS attachés à une instance Amazon EC2. La cohérence en cas de panne signifie que les instantanés de chaque volume Amazon EBS attaché à la même instance Amazon EC2 sont pris exactement au même moment. Vous n'avez plus besoin d'arrêter vos instances ou de coordonner plusieurs volumes Amazon EBS pour garantir l'état de votre application en cas de panne.

Les instantanés multivolumes compatibles avec les crashs étant une AWS Backup fonctionnalité par défaut, vous n'avez rien de différent à faire pour utiliser cette fonctionnalité. Vous pouvez sauvegarder des volumes Amazon EBS avec l'une des procédures suivantes :

Le rôle utilisé pour créer un point de restauration d'un instantané EBS sera associé à ce cliché. Ce même rôle doit être utilisé pour supprimer les points de récupération qu'il a créés ou pour transférer ses points de restauration vers un niveau d'archivage.

Amazon EBS Snapshot Lock et AWS Backup

AWS Backup les instantanés Amazon EBS gérés et les instantanés associés à une AMI AWS Backup Amazon EC2 gérée sur laquelle Amazon EBS Snapshot Lock est appliqué ne peuvent pas être supprimés dans le cadre du cycle de vie du point de restauration si la durée du verrouillage des instantanés dépasse le cycle de vie de sauvegarde. Ces points de récupération auront plutôt le statut `EXPIRED`. Ces points de récupération peuvent être supprimés manuellement si vous choisissez de supprimer d’abord le verrouillage d’instantané Amazon EBS.

Restauration des ressources Amazon EBS

Pour restaurer vos volumes Amazon EBS, suivez les étapes décrites dans Restauration d'un volume Amazon EBS.

Copie de balises sur des sauvegardes

En général, AWS Backup copie les balises des ressources qu'il protège vers vos points de récupération. Pour plus d'informations sur la copie des balises lors d'une restauration, consultez Copie de balises lors d'une restauration.

Par exemple, lorsque vous sauvegardez un volume Amazon EC2, vous copiez ses balises AWS Backup de ressources de groupe et individuelles dans l'instantané obtenu, sous réserve des conditions suivantes :

- Pour obtenir la liste des autorisations spécifiques aux ressources requises pour enregistrer les balises de métadonnées sur les sauvegardes, consultez Autorisations requises pour affecter des balises aux sauvegardes.
- Les balises initialement associées à une ressource et les balises attribuées lors de la sauvegarde sont attribuées aux points de restauration stockés dans un coffre de sauvegarde, jusqu'à un maximum de 50 (il s'agit d'une AWS limitation). Les balises attribuées lors de la sauvegarde sont prioritaires et les deux jeux de balises sont copiés par ordre alphabétique.
- DynamoDB ne prend pas en charge l'attribution de balises aux sauvegardes, sauf si vous activez d'abord Sauvegarde DynamoDB avancée.
- Les volumes Amazon EBS attachés aux instances Amazon EC2 sont des ressources imbriquées. Les balises des volumes Amazon EBS attachés aux instances Amazon EC2 sont des balises imbriquées. AWS Backup fait de son mieux pour copier les balises imbriquées, mais en cas d'échec, il crée une sauvegarde sans elles et indique le statut terminé.
- Lorsqu'une sauvegarde Amazon EC2 crée un point de restauration d'image et un ensemble de snapshots, elle AWS Backup copie les balises dans l'AMI qui en résulte. AWS Backup fait également de son mieux pour copier les balises des volumes associés à l'instance Amazon EC2 vers les instantanés qui en résultent.

Si vous copiez votre sauvegarde vers une autre sauvegarde Région AWS, AWS Backup copie toutes les balises de la sauvegarde d'origine vers la destination Région AWS.

Arrêt d'une tâche de sauvegarde

Vous pouvez arrêter une tâche de sauvegarde une AWS Backup fois qu'elle a été lancée. Dans ce cas, la sauvegarde n'est pas créée et l'enregistrement de la tâche de sauvegarde est conservé avec l'état aborted (abandonnée).

Pour arrêter une tâche de sauvegarde à l'aide de la AWS Backup console

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation de gauche, choisissez Jobs (Tâches).
3. Choisissez la tâche de sauvegarde que vous souhaitez arrêter.
4. Dans le panneau des détails de la tâche de sauvegarde, choisissez Stop (Arrêter).

Copie d'une sauvegarde

Vous pouvez copier des sauvegardes Régions AWS sur plusieurs sites Comptes AWS , à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié pour la plupart des types de ressources. Pour plus de détails, voirthe section called “Disponibilité des fonctionnalités par ressource”.

Vous pouvez également automatiser une séquence de copies entre comptes et entre régions pour la plupart des ressources prises en charge, à l'exception d'Amazon RDS et Aurora. Pour les instantanés Amazon RDS et Aurora, l'automatisation des copies entre comptes ou entre régions est AWS Backup uniquement prise en charge en fonction de la manière dont ces services créent leurs clés de chiffrement (la copie d'un instantané de cluster de bases de données multi-AZ n'est pas prise en charge).

Certains types de ressources disposent à la fois d'une fonctionnalité de sauvegarde continue et d'une copie entre régions et entre comptes. Lorsqu'une copie entre régions ou entre comptes d'une sauvegarde continue est réalisée, le point de récupération copié (sauvegarde) devient une sauvegarde instantanée (périodique). Selon le type de ressource, les instantanés peuvent être une copie incrémentielle ou une copie complète. La restauration à un instant dans le passé (PITR) n'est pas disponible pour ces copies.

Les copies conservent leur configuration source, y compris les dates de création et la période de conservation. La date de création fait référence à la date de création de la source, et non à la date de création de la copie.

REMARQUE : la configuration source remplace le paramètre d'expiration de sa copie, même si la copie est configurée pour ne jamais expirer ; une copie définie pour ne jamais expirer conservera toujours la date d'expiration de sa source.

Si vous souhaitez que la copie de votre sauvegarde n'expire jamais, définissez vos sauvegardes source pour qu'elles n'expirent jamais ou spécifiez que votre copie expire 100 ans après sa création.

Table des matières

Création de copies de sauvegarde sur Régions AWS

Vous pouvez ainsi copier des sauvegardes Régions AWS sur plusieurs à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié. AWS Backup La réplication entre régions est particulièrement utile en cas d'exigences de continuité d'activité ou de conformité pour stocker les sauvegardes à une distance minimale de vos données de production. Pour un didacticiel vidéo, consultez Managing cross-Region copies of backups.

Lorsque vous copiez une sauvegarde vers un nouveau Région AWS pour la première fois, AWS Backup copie la sauvegarde dans son intégralité. En général, si un service prend en charge les sauvegardes incrémentielles, les copies suivantes de cette sauvegarde Région AWS seront incrémentielles. AWS Backup chiffrera à nouveau votre copie à l'aide de la clé gérée par le client de votre coffre-fort de destination.

Amazon EBS fait exception. Selon lui, la modification de l'état de chiffrement d'un instantané au cours d'une opération de copie aboutit à une copie complète (et non incrémentielle).

Prérequis

- La plupart des ressources AWS Backup prises en charge prennent en charge la sauvegarde entre régions. Pour plus de détails, reportez-vous à la section Disponibilité des fonctionnalités par ressource.
- La plupart des AWS régions prennent en charge la sauvegarde interrégionale. Pour plus de détails, reportez-vous à la section Disponibilité des fonctionnalités par Région AWS.
- AWS Backup ne prend pas en charge les copies interrégionales destinées au stockage dans des niveaux froids.

Considérations relatives à la copie entre régions avec des ressources spécifiques

Amazon RDS

Vous ne pouvez pas copier un groupe d'options dans un autre Région AWS. En cas de tentative, vous pouvez obtenir un message d'erreur, tel que « Le cliché nécessite un groupe d'options cible avec les options suivantes :... »

Vous devez saisir les mêmes groupes d'options dans la cible Région AWS lorsque vous créez une nouvelle copie interrégionale d'un instantané Amazon RDS.

Exécution d'une sauvegarde entre régions à la demande

Pour copier une sauvegarde existante à la demande

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Choisissez Coffres-forts de sauvegarde.
3. Choisissez le coffre-fort qui contient le point de récupération à copier.
4. Dans la section Sauvegardes, sélectionnez un point de récupération à copier.
5. À l'aide du bouton déroulant Actions, choisissez Copier.
6. Entrez les valeurs suivantes :

   Copier vers la destination

   Choisissez la destination Région AWS de la copie. Vous pouvez ajouter une nouvelle règle de copie par copie à une nouvelle destination.

   Coffre-fort de sauvegarde de destination

   Choisissez le coffre-fort de sauvegarde de destination pour la copie.

   Transition vers le stockage à froid

   Choisissez le moment où vous souhaitez transférer la copie de sauvegarde vers le stockage à froid. Les sauvegardes transférées vers un stockage à froid doivent y être stockées pendant un minimum de 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

   Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau Disponibilité des fonctionnalités par ressource. L'expression de stockage à froid est ignorée pour les autres ressources.

   Période de conservation

   Spécifiez le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid. La période de rétention Toujours permet de conserver votre copie indéfiniment.

   Rôle IAM

   Choisissez le rôle IAM à utiliser lors de la création de la copie. AWS Backup Le rôle doit également être AWS Backup répertorié comme une entité de confiance, ce qui AWS

Backup permet d'assumer le rôle. Si vous choisissez Par défaut et que le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle sera créé pour vous avec les autorisations appropriées.

7. Choisissez Copier.

Planification de la sauvegarde entre régions

Vous pouvez utiliser un plan de sauvegarde planifié pour copier des sauvegardes entre Régions AWS.

Pour copier une sauvegarde à l'aide d'un plan de sauvegarde planifié

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans Mon compte, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sur la page Créer un plan de sauvegarde, choisissez Créer un nouveau plan.
4. Pour Nom du plan de sauvegarde, entrez le nom de votre plan de sauvegarde.
5. Dans la section Configuration de règle de backup, ajoutez une règle de sauvegarde qui définit un calendrier de sauvegarde, une fenêtre de sauvegarde et des règles de cycle de vie. Vous pourrez ajouter d'autres règles de sauvegarde ultérieurement.

   a. Pour Nom de la règle de sauvegarde, entrez un nom pour votre règle.

   b. Pour Coffre de sauvegarde, choisissez un coffre-fort dans la liste. Les points de récupération pour cette sauvegarde seront enregistrés dans ce coffre-fort. Vous pouvez créer un nouveau coffre-fort de sauvegarde.

   c. Pour Fréquence de sauvegarde, choisissez la fréquence à laquelle vous souhaitez effectuer des sauvegardes.

   d. Pour les services prenant en charge le PITR, si vous souhaitez bénéficier de cette fonctionnalité, choisissez Activer les sauvegardes continues pour la point-in-time restauration (PITR). Pour obtenir une liste des services qui prennent en charge la PITR, consultez cette section du tableau Disponibilité des fonctionnalités par ressource.

   e. Pour Fenêtre de sauvegarde, choisissez Utiliser la fenêtre de sauvegarde par défaut – recommandé. Vous pouvez personnaliser la fenêtre de sauvegarde.

   f. Pour Copier vers la destination, choisissez la Région AWS de destination de votre copie de sauvegarde. Votre sauvegarde sera copiée dans cette région. Vous pouvez ajouter une

nouvelle règle de copie par copie à une nouvelle destination. Entrez ensuite les valeurs suivantes :

Copier dans le coffre-fort d'un autre compte

Ne désactivez pas cette option. Pour en savoir plus sur la copie entre comptes, voir Création de copies de sauvegarde sur Comptes AWS

Coffre-fort de sauvegarde de destination

Choisissez le coffre-fort de sauvegarde dans la région de destination où AWS Backup vous copierez votre sauvegarde.

Si vous souhaitez créer un nouveau coffre-fort de sauvegarde pour une copie entre régions, choisissez Créer un coffre de backup. Entrez les informations dans l'assistant. Choisissez ensuite Créer un coffre de sauvegarde.

6. Choisissez Créer un plan.

Création de copies de sauvegarde sur Comptes AWS

Vous pouvez en AWS Backup sauvegarder plusieurs Comptes AWS à la demande ou automatiquement dans le cadre d'un plan de sauvegarde planifié. Utilisez une sauvegarde entre comptes si vous souhaitez copier en toute sécurité vos sauvegardes sur un ou plusieurs Comptes AWS sites de votre organisation pour des raisons opérationnelles ou de sécurité. Si votre sauvegarde d'origine est supprimée par inadvertance, vous pouvez copier la sauvegarde de son compte de destination vers son compte source, puis démarrer la restauration. Pour ce faire, vous devez disposer de deux comptes appartenant à la même organisation dans le service AWS Organizations . Pour plus d'informations, consultez Didacticiel : Création et configuration d'une organisation dans le Guide de l'utilisateur Organizations.

Dans votre compte de destination, vous devez créer un coffre-fort de sauvegarde. Vous attribuez ensuite une clé gérée par le client pour chiffrer les sauvegardes dans le compte de destination, ainsi qu'une politique d'accès basée sur les ressources pour autoriser l'accès AWS Backup aux ressources que vous souhaitez copier. Dans le compte source, si vos ressources sont chiffrées à l'aide d'une clé gérée par le client, vous devez partager cette clé gérée par le client avec le compte de destination. Vous pouvez ensuite créer un plan de sauvegarde et choisir un compte de destination faisant partie de votre unité organisationnelle dans AWS Organizations.

Lorsque vous copiez une sauvegarde sur plusieurs comptes pour la première fois, AWS Backup copie la sauvegarde dans son intégralité. En général, si un service prend en charge les sauvegardes incrémentielles, les copies suivantes de cette sauvegarde dans le même compte sont incrémentielles. AWS Backup chiffre à nouveau votre copie à l'aide de la clé gérée par le client de votre coffre-fort de destination.

Prérequis

- Avant de gérer les ressources sur plusieurs Comptes AWS AWS Backup entrées, vos comptes doivent appartenir à la même organisation dans le AWS Organizations service.
- La plupart des ressources prises en charge par AWS Backup prennent en charge la sauvegarde entre comptes. Pour plus de détails, reportez-vous à la section Disponibilité des fonctionnalités par ressource.
- La plupart des AWS régions prennent en charge la sauvegarde entre comptes. Pour plus de détails, reportez-vous à la section Disponibilité des fonctionnalités par Région AWS.
- AWS Backup ne prend pas en charge les copies entre comptes pour le stockage dans des niveaux froids.

Configuration de la sauvegarde entre comptes

De quoi avez-vous besoin pour créer des sauvegardes entre comptes ?

- Un compte source

  Le compte source est le compte où résident vos AWS ressources de production et vos sauvegardes principales.

  L'utilisateur du compte source lance l'opération de sauvegarde entre comptes. L'utilisateur ou le rôle du compte source doit disposer des autorisations d'API appropriées pour lancer l'opération. Les autorisations appropriées peuvent être la politique AWS géréeAWSBackupFullAccess, qui permet un accès complet aux AWS Backup opérations, ou une politique gérée par le client qui autorise des actions telles queec2:ModifySnapshotAttribute. Pour plus d'informations sur les types de politiques, consultez Politiques gérées par AWS Backup.
- Un compte de destination

  Le compte de destination est le compte sur lequel vous souhaitez conserver une copie de votre sauvegarde. Vous pouvez choisir plusieurs comptes de destination. Le compte de destination doit se trouver dans la même organisation que le compte source dans AWS Organizations.

Vous devez « Autoriser » la stratégie d'accès `backup:CopyIntoBackupVault` à votre coffre-fort de sauvegarde de destination. L'absence de cette politique empêchera toute tentative de copie sur le compte de destination.

- Un compte de gestion dans AWS Organizations

  Le compte de gestion est le compte principal de votre organisation, tel que défini par AWS Organizations, que vous utilisez pour gérer la sauvegarde entre comptes sur l'ensemble de vos Comptes AWS. Pour utiliser la sauvegarde entre comptes, vous devez également activer l'approbation de service. Après avoir activé l'approbation de service, vous pouvez utiliser n'importe quel compte de l'organisation comme compte de destination. Depuis votre compte de destination, vous pouvez choisir les coffres-forts à utiliser pour la sauvegarde entre comptes.
- Activation de la sauvegarde entre comptes dans la console AWS Backup

Pour plus d'informations sur la sécurité, consultez Remarques de sécurité pour la sauvegarde entre comptes.

Pour utiliser la sauvegarde entre comptes, vous devez activer la fonctionnalité de sauvegarde entre comptes. Vous devez ensuite « Autoriser » la stratégie d'accès `backup:CopyIntoBackupVault` dans votre coffre-fort de sauvegarde de destination.

Activer la sauvegarde entre comptes

1. Connectez-vous à l'aide des informations d'identification AWS Organizations de votre compte de gestion. La sauvegarde entre comptes ne peut être activée ou désactivée qu'à l'aide de ces informations d'identification.
2. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
3. Dans Mon compte, choisissez Paramètres.
4. Pour Backup entre comptes, choisissez Activer.
5. Dans Coffres de sauvegarde, choisissez votre coffre-fort de destination.

   Pour la copie entre comptes, le coffre source et le coffre de destination se trouvent dans des comptes différents. Passez au compte auquel appartient le compte de destination, si nécessaire.
6. Dans la section Stratégie d'accès, « Autorisez » `backup:CopyIntoBackupVault`. Par exemple, choisissez Ajouter des autorisations, puis Autoriser l'accès à un coffre de sauvegarde depuis l'organisation. Toute action entre comptes autre que `backup:CopyIntoBackupVault` sera rejetée.

7. Désormais, n'importe quel compte de votre organisation peut partager le contenu de son coffre-fort de sauvegarde avec n'importe quel autre compte de votre organisation. Pour plus d'informations, consultez Partage d'un coffre-fort de sauvegarde avec un autre compte AWS. Pour limiter les comptes autorisés à recevoir le contenu des coffres-forts de sauvegarde d'autres comptes, consultez Configuration de votre compte en tant que compte de destination.

Planification d'une sauvegarde entre comptes

Vous pouvez utiliser un plan de sauvegarde planifié pour copier des sauvegardes entre Comptes AWS.

Pour copier une sauvegarde à l'aide d'un plan de sauvegarde planifié

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans Mon compte, choisissez Plans de sauvegarde, puis Créer un plan de sauvegarde.
3. Sur la page Créer un plan de sauvegarde, choisissez Créer un nouveau plan.
4. Pour Nom du plan de sauvegarde, entrez le nom de votre plan de sauvegarde.
5. Dans la section Configuration de règle de backup, ajoutez une règle de sauvegarde qui définit un calendrier de sauvegarde, une fenêtre de sauvegarde et des règles de cycle de vie. Vous pourrez ajouter d'autres règles de sauvegarde ultérieurement.

   Pour Nom de la règle, entrez un nom pour votre règle.
6. Dans la section Planification, sous Fréquence, choisissez la fréquence à laquelle vous souhaitez que la sauvegarde soit effectuée.
7. Pour Fenêtre de sauvegarde, choisissez Utiliser la fenêtre de sauvegarde par défaut (recommandé). Vous pouvez personnaliser la fenêtre de sauvegarde.
8. Pour Coffre de sauvegarde, choisissez un coffre-fort dans la liste. Les points de récupération pour cette sauvegarde seront enregistrés dans ce coffre-fort. Vous pouvez créer un nouveau coffre-fort de sauvegarde.
9. Dans la section Générer une copie – facultatif, entrez les valeurs suivantes :

   Région de destination

   Choisissez la destination Région AWS de votre copie de sauvegarde. Votre sauvegarde sera copiée dans cette région. Vous pouvez ajouter une nouvelle règle de copie par copie à une nouvelle destination.

Copier dans le coffre-fort d'un autre compte

Basculez pour choisir cette option. L'option devient bleue lorsqu'elle est sélectionnée. L'option ARN du coffre externe apparaît.

ARN du coffre-fort externe

Entrez l'Amazon Resource Name (ARN) du compte de destination. L'ARN est une chaîne qui contient l'identifiant du compte et son Région AWS. AWS Backup copiera la sauvegarde dans le coffre-fort du compte de destination. La liste Région de destination est automatiquement mise à jour en fonction de la région dans l'ARN du coffre-fort externe.

Pour Autoriser l'accès au coffre de sauvegarde, choisissez Autoriser. Choisissez ensuite Autoriser dans l'assistant qui s'ouvre.

AWS Backup a besoin d'autorisations pour accéder au compte externe afin de copier la sauvegarde à la valeur spécifiée. L'assistant présente l'exemple de politique suivant qui fournit cet accès.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
}
```

Transition vers le stockage à froid

Choisissez le moment pour effectuer la transition de la copie de sauvegarde vers le stockage à froid et le moment d’expiration (suppression) de la copie. Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau Disponibilité des fonctionnalités par ressource. L'expression de stockage à froid est ignorée pour les autres ressources.

Expiration indique le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid.

> **Note**
>
> Lorsque les sauvegardes expirent et sont marquées pour suppression dans le cadre de votre politique de cycle de vie, AWS Backup supprime les sauvegardes à un moment choisi au hasard au cours des 8 heures suivantes. Cette fenêtre permet de garantir des performances constantes.

10. Choisissez Balises ajoutées à des points de récupération pour ajouter des balises à vos points de récupération.
11. Pour Paramètres de sauvegarde avancés, choisissez Windows VSS pour activer les instantanés compatibles avec les applications pour les logiciels tiers sélectionnés exécutés sur EC2.
12. Choisissez Créer un plan.

Exécution d'une sauvegarde entre comptes à la demande

Vous pouvez copier une sauvegarde Compte AWS sur un autre à la demande.

Pour copier une sauvegarde à la demande

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Pour Mon compte, choisissez Coffre de sauvegarde pour voir tous vos coffres-forts de sauvegarde répertoriés. Vous pouvez filtrer en fonction du nom ou de la balise du coffre-fort de sauvegarde.
3. Choisissez l'ID de point de récupération de la sauvegarde que vous souhaitez copier.
4. Choisissez Copier.
5. Développez Détails de la sauvegarde pour voir les informations relatives au point de récupération que vous copiez.
6. Dans la section Copier la configuration, choisissez une option dans la liste Région de destination.

7. Choisissez Copier dans le coffre d'un autre compte. L'option devient bleue lorsqu'elle est sélectionnée.
8. Entrez l'Amazon Resource Name (ARN) du compte de destination. L'ARN est une chaîne qui contient l'identifiant du compte et son Région AWS. AWS Backup copiera la sauvegarde dans le coffre-fort du compte de destination. La liste Région de destination est automatiquement mise à jour en fonction de la région dans l'ARN du coffre-fort externe.
9. Pour Autoriser l'accès au coffre de sauvegarde, choisissez Autoriser. Choisissez ensuite Autoriser dans l'assistant qui s'ouvre.

   Pour créer la copie, il AWS Backup faut des autorisations pour accéder au compte source. L'assistant affiche un exemple de politique qui fournit cet accès. Cette politique est présentée ci-après.

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "Allow account to copy into backup vault",
         "Effect": "Allow",
         "Action": "backup:CopyIntoBackupVault",
         "Resource": "*",
         "Principal": {
           "AWS": "arn:aws:iam::account-id:root"
         }
       }
     ]
   }
   ```

10. Pour Transition vers le stockage à froid, choisissez le moment pour effectuer la transition de la copie de sauvegarde vers le stockage à froid et le moment d'expiration (suppression) de la copie. Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Vous ne pouvez pas modifier cette valeur après la transition d'une copie vers le stockage à froid.

    Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau Disponibilité des fonctionnalités par ressource. L'expression de stockage à froid est ignorée pour les autres ressources.

Expiration indique le nombre de jours après la création pour la suppression de la copie. Cette valeur doit être supérieure de 90 jours à la valeur de Transition vers le stockage à froid.

11. Pour Rôle IAM, spécifiez le rôle IAM (tel que le rôle par défaut) autorisé à rendre votre sauvegarde disponible pour une copie. L'acte de copie est effectué par le rôle lié au service de votre compte de destination.
12. Choisissez Copier. Selon la taille de la ressource que vous copiez, ce processus peut prendre plusieurs heures. Une fois la tâche de copie terminée, vous verrez la copie dans l'onglet Tâches de copie du menu Tâches.

Clés de chiffrement et copies entre comptes

La clé de chiffrement des copies entre comptes dépend du type de ressource. Ressources qui ont AWS Backup Gestion complète utilisé la clé de chiffrement du coffre de sauvegarde source. Les clés KMS gérées par le client peuvent être utilisées pour le chiffrement des copies entre comptes de ces types de ressources.

Les types de ressources qui ne sont pas entièrement gérés par AWS Backup ont la même clé KMS source et la même clé KMS de ressource. La copie entre comptes avec des clés KMS AWS gérées n'est pas prise en charge pour ces types de ressources qui ne sont pas entièrement gérées par AWS Backup.

Pour obtenir de l'aide supplémentaire pour résoudre les problèmes de copie entre comptes, consultez le centre de AWS connaissances.

Lors d'une copie entre comptes, la politique de clé KMS du compte source doit autoriser le compte de destination à utiliser la politique de clé KMS.

Restaurer une sauvegarde de l'un Compte AWS à l'autre

AWS Backup ne prend pas en charge la récupération de ressources de l'un Compte AWS à l'autre. Toutefois, vous pouvez copier une sauvegarde d'un compte vers un autre, puis la restaurer dans ce compte. Par exemple, vous ne pouvez pas restaurer une sauvegarde du compte A vers le compte B, mais vous pouvez copier une sauvegarde du compte A vers le compte B, puis la restaurer dans le compte B.

La restauration d'une sauvegarde d'un compte à un autre est un processus en deux étapes.

Pour restaurer une sauvegarde d'un compte à un autre

1. Copiez la sauvegarde de la source Compte AWS vers le compte sur lequel vous souhaitez effectuer la restauration. Pour obtenir des instructions, consultez Configuration de la sauvegarde entre comptes.
2. Suivez les instructions appropriées à votre ressource pour restaurer la sauvegarde.

Partage d'un coffre-fort de sauvegarde avec un autre compte AWS

AWS Backup vous permet de partager un coffre-fort de sauvegarde avec un ou plusieurs comptes, ou avec l'ensemble de votre organisation AWS Organizations. Vous pouvez partager un coffre-fort de sauvegarde de destination avec un compte AWS source, un utilisateur ou un rôle IAM source.

Pour partager un coffre-fort de sauvegarde de destination

1. Choisissez AWS Backup, puis Coffres de sauvegarde.
2. Choisissez le nom du coffre-fort de sauvegarde que vous souhaitez partager.
3. Dans le volet Stratégie d'accès, choisissez le menu déroulant Ajouter des autorisations.
4. Choisissez Autoriser l'accès au niveau du compte à un coffre de sauvegarde. Vous pouvez également choisir d'autoriser l'accès au niveau de l'organisation ou au niveau du rôle.
5. Entrez l'AccountID du compte que vous souhaitez partager avec ce coffre-fort de sauvegarde de destination.
6. Choisissez Enregistrer la stratégie.

Vous pouvez utiliser les politiques IAM pour partager votre coffre-fort de sauvegarde.

Partage d'un coffre-fort de sauvegarde de destination avec un Compte AWS ou un rôle IAM

La politique suivante partage un coffre-fort de sauvegarde avec un compte numéro `4444555566666` et le rôle IAM `SomeRole` dans le compte numéro `111122223333`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
```

```
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
}
```

Partagez un coffre-fort de sauvegarde de destination dans lequel une unité organisationnelle AWS Organizations

La politique suivante partage un coffre-fort de sauvegarde avec les unités organisationnelles qui utilisent leur `PrincipalOrgPaths`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

Partagez un coffre-fort de sauvegarde de destination avec une organisation dans AWS Organizations

La politique suivante partage un coffre-fort de sauvegarde avec l'organisation portant l'`PrincipalOrgID` « o-a1b2c3d4e5 ».

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

```
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

Configuration de votre compte en tant que compte de destination

Lorsque vous activez pour la première fois les sauvegardes entre comptes à l'aide de votre compte de AWS Organizations gestion, tout utilisateur d'un compte membre peut configurer son compte comme compte de destination. Nous vous recommandons de définir une ou plusieurs des politiques de contrôle des services (SCP) suivantes dans AWS Organizations afin de limiter vos comptes de destination. Pour en savoir plus sur l'attachement de politiques de contrôle des services aux AWS Organizations nœuds, consultez la section Attacher et détacher des politiques de contrôle des services.

Limitation des comptes de destination à l'aide de balises

Lorsqu'elles sont associées à une AWS Organizations racine, une unité d'organisation ou un compte individuel, cette politique limite les destinations de copies de cette racine, de cette unité d'organisation ou de ce compte aux seuls comptes dotés de coffres-forts de sauvegarde que vous avez marqués`DestinationBackupVault`. L'autorisation `"backup:CopyIntoBackupVault"` contrôle le comportement d'un coffre-fort de sauvegarde et, dans ce cas, les coffres-forts de sauvegarde de destination valides. Utilisez cette politique, ainsi que la balise correspondante appliquée aux coffres-forts de destination approuvés, pour contrôler les destinations des copies entre comptes uniquement vers les comptes approuvés et les coffres-forts de sauvegarde.

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

```
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

Limitation des comptes de destination à l'aide de numéros de compte et de noms de coffres

Lorsqu'elles sont associées à une AWS Organizations racine, une unité d'organisation ou un compte individuel, cette politique limite les copies provenant de cette racine, de cette unité d'organisation ou de ce compte à deux comptes de destination uniquement. L'autorisation `"backup:CopyFromBackupVault"` contrôle le comportement d'un point de récupération dans le coffre-fort de sauvegarde et, dans ce cas, les destinations vers lesquelles vous pouvez copier ce point de récupération. Le coffre-fort source n'autorisera les copies vers le premier compte de destination (112233445566) que si un ou plusieurs noms de coffre-fort de sauvegarde de destination commencent par `cab-`. Le coffre-fort source n'autorisera les copies vers le deuxième compte de destination (123456789012) que si la destination est le seul coffre-fort de sauvegarde nommé `fort-knox`.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"arn:aws:ec2:*:snapshot/*",
      "Condition":{
        "ForAllValues:ArnNotLike":{
          "backup:CopyTargets":[
            "arn:aws:backup:*:112233445566:backup-vault:cab-*",
            "arn:aws:backup:us-west-1:123456789012:backup-vault:fort-knox"
          ]
        }
      }
    }
```

```
  ]
}
```

Limitez les comptes de destination à l'aide d'unités organisationnelles dans AWS Organizations

Lorsque vous êtes attaché à une AWS Organizations racine ou à une unité d'organisation qui contient votre compte source, ou lorsqu'il est attaché à votre compte source, la politique suivante limite les comptes de destination à ces comptes au sein des deux unités d'organisation spécifiées.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringNotLike":{
          "backup:CopyTargetOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

Remarques de sécurité pour la sauvegarde entre comptes

Tenez compte des éléments suivants lors de l'exécution de sauvegardes entre comptes dans AWS Backup :

- Le coffre-fort de destination ne peut pas être le coffre-fort par défaut. Cela est dû au fait que le coffre-fort par défaut est chiffré avec une clé qui ne peut pas être partagée avec d'autres comptes.
- Les sauvegardes entre comptes peuvent continuer à s'exécuter pendant 15 minutes au maximum après avoir désactivé la sauvegarde entre comptes. Cela est dû à une cohérence à terme et peut entraîner le démarrage ou la fin de certaines tâches entre comptes, même après avoir désactivé la sauvegarde entre comptes.
- Si le compte de destination quitte l'organisation ultérieurement, ce compte conservera les sauvegardes. Pour éviter toute fuite de données potentielle, ajoutez une autorisation de refus

à l'autorisation `organizations:LeaveOrganization` dans une politique de contrôle des services (SCP) attachée au compte de destination. Pour des informations détaillées sur les SCP, consultez Suppression d'un compte membre de votre organisation dans le Guide de l'utilisateur Organizations.

- Si vous supprimez un rôle de copie lors d'une copie entre comptes, vous ne AWS Backup pouvez pas annuler le partage des instantanés du compte source une fois la tâche de copie terminée. Dans ce cas, la tâche de sauvegarde se termine, mais le statut de la tâche de copie indique Impossible d'annuler le partage de l'instantané.

Suppression de sauvegardes

Nous vous recommandons de l'utiliser AWS Backup pour supprimer automatiquement les sauvegardes dont vous n'avez plus besoin en configurant votre cycle de vie lors de la création de votre plan de sauvegarde. Par exemple, si vous définissez le cycle de vie de votre plan de sauvegarde de manière à conserver vos points de restauration pendant un an, AWS Backup vous supprimerez automatiquement le 1er janvier 2022 les points de récupération créés le 1er janvier 2021 ou dans les heures qui ont suivi. (AWS Backup répartit ses suppressions de manière aléatoire dans les 8 heures suivant l'expiration du point de récupération afin de maintenir les performances.) Pour en savoir plus sur la configuration de votre politique de rétention du cycle de vie, consultez Création d'un plan de sauvegarde.

Toutefois, vous pouvez souhaiter supprimer manuellement un ou plusieurs points de récupération. Par exemple :

- Vous avez des points de récupération `EXPIRED`. Ces points de restauration n'ont pas AWS Backup pu être supprimés automatiquement car vous avez supprimé ou modifié la politique IAM d'origine que vous avez utilisée pour créer votre plan de sauvegarde. Lorsqu'il AWS Backup a tenté de les supprimer, il n'était pas autorisé à le faire.

  Des points de récupération expirés peuvent également être créés si un point de récupération Amazon EBS ou Amazon EC2 AWS géré est doté d'un Amazon EBS Snapshot Lock AWS Backup et n'est pas en mesure de terminer le processus de cycle de vie qui entraînerait normalement la suppression du point de récupération. Notez que ces points de récupération expirés peuvent être restaurés à partir de la console et de l'API Amazon EC2 ou de la console et de l'API Amazon EBS.

> **Warning**
>
> Vous continuerez à enregistrer les points de récupération expirés sur votre compte. Cela peut augmenter vos coûts de stockage.

Après le 6 août 2021, le point de restauration cible AWS Backup sera affiché comme expiré dans son coffre-fort de sauvegarde. Vous pouvez passer votre souris sur le statut Expiré rouge pour afficher un message de statut contextuel expliquant pourquoi il n'a pas été possible de supprimer la sauvegarde. Vous pouvez également choisir Actualiser pour recevoir les informations les plus récentes.

- Vous ne souhaitez plus qu'un plan de sauvegarde fonctionne comme vous l'avez configuré. La mise à jour du plan de sauvegarde affecte les futurs points de récupération qu'il créera, mais n'affecte pas le point de récupération déjà créé. Pour en savoir plus, consultez Mise à jour d'un plan de sauvegarde.
- Vous devez effectuer un nettoyage après avoir terminé un test ou un didacticiel.

Suppression manuelle de sauvegardes

Pour supprimer manuellement des points de récupération

1. Dans le volet de navigation de la AWS Backup console, sélectionnez Backup vaults.
2. Sur la page Backup vaults (Coffres-forts de sauvegarde), choisissez le coffre-fort de sauvegarde dans lequel vous avez stocké les sauvegardes.
3. Choisissez un point de récupération, choisissez le menu déroulant Actions, puis Supprimer.
4. 1. Si votre liste contient une sauvegarde continue, choisissez l'une des options suivantes. Chaque sauvegarde continue possède un point de récupération unique.
     - Supprimer définitivement mes données de sauvegarde ou Supprimer le point de récupération. En sélectionnant l'une de ces options, vous arrêtez les futures sauvegardes continues et supprimez également vos données de sauvegarde continue existantes.

> **Note**
>
> Consultez Sauvegardes et point-in-time restaurations continues (PITR) les considérations relatives à la sauvegarde continue sur Amazon S3, Amazon RDS et Aurora.

- Conservez mes données de sauvegarde en continu ou dissociez le point de restauration. En sélectionnant l'une de ces options, vous arrêtez les futures sauvegardes continues, mais vous conservez vos données de sauvegarde continues existantes jusqu'à leur expiration, conformément à votre période de rétention.

  Un point de restauration continue (sauvegarde) Amazon S3 dissocié restera dans son coffre de sauvegarde, mais son état passera à`STOPPED`.

2. Pour supprimer tous les points de récupération répertoriés, tapez Supprimer, puis choisissez Supprimer le point de restauration.
3. AWS Backup commence à soumettre vos points de récupération pour suppression et affiche une barre de progression. Gardez l'onglet de votre navigateur ouvert et ne quittez pas cette page pendant le processus de soumission.
4. À la fin du processus de soumission, vous AWS Backup présente un statut dans la bannière. Le statut peut être :
   - Soumis avec succès. Vous pouvez choisir Afficher la progression du statut de suppression de chaque point de récupération.
   - Échec de l'envoi. Vous pouvez choisir Afficher la progression du statut de suppression de chaque point de récupération ou Réessayer votre soumission.
   - Un résultat mitigé : certains points de récupération ont été soumis avec succès alors que d'autres points de récupération n'ont pas été soumis.
5. Si vous choisissez Afficher la progression, vous pouvez consulter l'État de la suppression de chaque sauvegarde. Si un statut de suppression est Échec ou Expiré, vous pouvez cliquer sur ce statut pour en connaître la raison. Vous pouvez également choisir de Réessayer les suppressions qui ont échoué.

Résolution des problèmes liés aux suppressions manuelles

Dans de rares cas, il AWS Backup se peut que votre demande de suppression ne soit pas traitée. AWS Backup utilise le rôle lié au service `AWSServiceRoleForBackup` pour effectuer des suppressions.

Si votre demande de suppression échoue, vérifiez que votre rôle IAM est autorisé à créer des rôles liés à un service. Plus précisément, vérifiez que votre rôle IAM possède l'action `iam:CreateServiceLinkedRole`. Si ce n'est pas le cas, ajoutez cette autorisation au rôle utilisé pour créer une sauvegarde. L'ajout de cette autorisation permet AWS Backup d'effectuer des suppressions manuelles.

Si, une fois que vous avez confirmé l'action `iam:CreateServiceLinkedRole` pour votre rôle IAM, vos points de récupération sont toujours bloqués avec le statut `DELETING`, nous étudierons probablement votre problème. Terminez votre suppression manuelle avec les étapes suivantes :

1. Configurez un rappel pour revenir dans 2 à 3 jours.
2. Après 2 à 3 jours, vérifiez les points de suppression `EXPIRED` récents résultant de votre première opération de suppression manuelle.
3. Supprimez manuellement ces points de récupération `EXPIRED`.

Pour plus d'informations sur les rôles, consultez Utilisation des rôles liés à un service et Ajout et suppression d'autorisations basées sur l'identité IAM.

Modification d'une sauvegarde

Après avoir créé une sauvegarde à l'aide de AWS Backup, vous pouvez modifier le cycle de vie ou les balises de la sauvegarde. Le cycle de vie définit à quel moment une sauvegarde est transférée vers un stockage à froid et quand elle expire. AWS Backup effectue la transition et valide l'expiration des sauvegardes automatiquement, conformément au cycle de vie que vous définissez.

Pour consulter la liste des ressources que vous pouvez transférer vers le stockage à froid, consultez la section « Cycle de vie vers le stockage à froid » du tableau Disponibilité des fonctionnalités par ressource. L'expression de stockage à froid est ignorée pour les autres ressources.

> **Note**
>
> La modification des balises d'une sauvegarde à l'aide de la AWS Backup console n'est prise en charge que pour les sauvegardes des systèmes de fichiers Amazon Elastic File System (Amazon EFS) et Amazon DynamoDB Advanced.
> Les balises qui ont été ajoutées au point de récupération lors de la création d'autres ressources apparaîtront toujours, mais elles seront grisées et ne seront pas modifiables. Même si ces balises ne sont pas modifiables dans la AWS Backup console, vous pouvez modifier les balises des sauvegardes de ces autres services à l'aide de la console ou de l'API du service.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Lorsque vous mettez à jour le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) », la valeur doit être au minimum l'âge de la sauvegarde plus une journée. Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Voici un exemple de mise à jour du cycle de vie d'une sauvegarde.

Pour modifier le cycle de vie d'une sauvegarde

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Dans la section Backups (Sauvegardes), choisissez une sauvegarde.
4. Sur la page des détails de la sauvegarde, choisissez Edit (Modifier).
5. Configurez les paramètres du cycle de vie, puis choisissez Save (Enregistrer).

Restauration d'une sauvegarde

Comment restaurer

Pour les instructions de restauration de la console et les liens vers la documentation pour chaque type de ressource AWS Backup pris en charge, consultez les liens au bas de cette page.

Pour restaurer une sauvegarde par programmation, utilisez l'opération d'API StartRestoreJob.

Les valeurs de configuration (« restaurer des métadonnées ») dont vous avez besoin pour restaurer votre ressource varient en fonction de la ressource que vous souhaitez restaurer. Pour obtenir les métadonnées de configuration avec lesquelles votre sauvegarde a été créée, vous pouvez appeler GetRecoveryPointRestoreMetadata. Les exemples de restauration de métadonnées sont également disponibles dans les liens au bas de cette page.

La restauration depuis le stockage à froid prend généralement 4 heures de plus que la restauration depuis un stockage à chaud.

Pour chaque restauration, une tâche de restauration est créée avec un ID de tâche unique, par exemple `1323657E-2AA4-1D94-2C48-5D7A423E7394`.

> **Note**
>
> AWS Backup ne prévoit aucun accord de niveau de service (SLA) concernant la durée de restauration. Les temps de restauration peuvent varier en fonction de la charge et de la capacité du système, même pour les restaurations contenant les mêmes ressources.

Restaurations non destructives

Lorsque vous AWS Backup restaurez une sauvegarde, une nouvelle ressource est créée avec la sauvegarde que vous restaurez. Cela permet d'empêcher votre activité de restauration de détruire vos ressources existantes.

Tests de restauration

Vous pouvez effectuer des tests sur vos ressources pour simuler une expérience de restauration. Cela permet de déterminer si vous atteignez l’objectif de durée de récupération (RTO) de votre organisation et de vous préparer aux futurs besoins de restauration.

Pour plus d’informations, consultez Tests de restauration.

Copie de balises lors d'une restauration

> **Note**
>
> Cette fonctionnalité n'est actuellement pas disponible pour les restaurations d'Amazon DynamoDB, Amazon S3, SAP HANA sur des instances Amazon EC2, des machines virtuelles et des ressources Amazon Timestream.

Introduction

Vous pouvez copier des balises lorsque vous restaurez une ressource si les balises appartenaient à la ressource protégée au moment de la sauvegarde. Les balises, qui sont des étiquettes contenant une paire clé-valeur, peuvent vous aider à identifier et à rechercher des ressources. Lorsque vous lancez une tâche de restauration, des balises appartenant aux ressources sauvegardées d'origine peuvent être ajoutées à la ressource en cours de restauration.

Le fait de choisir d'inclure des balises lors d'une tâche de restauration permet de réduire les frais et le travail liés à l'application manuelle de balises aux ressources une fois la tâche de restauration terminée. Notez que cela est différent de l'ajout de nouvelles balises aux ressources restaurées.

Lorsque vous restaurez une sauvegarde dans le flux de console, vos balises source sont copiées par défaut. Dans la console, décochez la case si vous ne souhaitez pas copier les balises vers une ressource restaurée.

Dans l'opération d'API `StartRestoreJob`, le paramètre `CopySourceTagsToRestoredResource` est défini sur `false` par défaut, ce qui exclut les balises source d'origine de la ressource que vous restaurez. Si vous souhaitez inclure des balises provenant de la source d'origine, définissez ce paramètre sur `True`.

Considérations

- Une ressource peut avoir jusqu'à 50 balises, y compris les ressources restaurées. Consultez la section Marquage de vos AWS ressources pour plus d'informations sur les limites de balises.
- Assurez-vous que les autorisations appropriées sont présentes dans le rôle utilisé pour les restaurations afin de copier des balises. Le rôle par défaut pour les restaurations contient les autorisations nécessaires. Un rôle personnalisé doit inclure des autorisations supplémentaires pour baliser les ressources.

- Les ressources suivantes ne sont actuellement pas prises en charge pour l'inclusion de balises de restauration : VMware Cloud™ AWS activé, VMware Cloud™ activé AWS Outposts, systèmes sur site, instances SAP HANA sur Amazon EC2, Timestream, DynamoDB, Advanced DynamoDB et Amazon S3.
- Pour les sauvegardes continues, les balises de la ressource d'origine telles que celles de la sauvegarde la plus récente seront copiées sur la ressource restaurée.
- Les balises ne seront pas copiées pour les restaurations au niveau des éléments.
- Les balises qui ont été ajoutées à une sauvegarde une fois la tâche de sauvegarde terminée mais qui n'étaient pas présentes sur la ressource d'origine avant la sauvegarde ne seront pas copiées sur la ressource restaurée. Seules les sauvegardes créées après le 22 mai 2023 sont éligibles à la copie de balises lors de la restauration.

Interaction de balises avec des ressources spécifiques

- Amazon EC2
  - Les balises appliquées aux instances Amazon EC2 restaurées sont également appliquées aux volumes Amazon EBS restaurés attachés.
  - Les balises appliquées aux volumes EBS attachés aux instances source ne sont pas copiées sur les volumes attachés aux instances restaurées. Si vous avez des politiques IAM qui autorisent ou refusent aux utilisateurs l'accès aux volumes EBS en fonction de leurs balises, vous devez réattribuer manuellement les balises requises aux volumes restaurés pour garantir que vos politiques restent en vigueur.
- Lorsque vous restaurez une ressource Amazon EFS, elle doit être copiée dans un nouveau système de fichiers. Les restaurations d'un système de fichiers existant ne peuvent pas contenir de balises copiées sur celui-ci.
- Amazon RDS
  - Si le cluster RDS qui a été sauvegardé est toujours actif, les balises de ce cluster seront copiées.
  - Si le cluster d'origine n'est plus actif, les balises de l'instantané du cluster seront copiées à la place.
  - Les balises présentes sur la ressource au moment de la sauvegarde seront copiées lors de la restauration, que le paramètre booléen pour `CopySourceTagsToRestoredResource` soit défini sur `True` ou `False`. Toutefois, si l'instantané ne contient pas de balises, le paramètre booléen ci-dessus sera utilisé.

- Par défaut, les clusters Amazon Redshift incluent toujours des balises lors d'une tâche de restauration.

Copie des balises via la console

1. Ouvrez la console AWS Backup.
2. Dans le volet de navigation, choisissez Ressources protégées et sélectionnez l'ID de ressource Amazon S3 que vous voulez restaurer.
3. Sur la page Détails de la ressource, vous verrez une liste des points de récupération pour l'ID de ressource sélectionné. Pour restaurer une ressource :

   a. Dans le volet Sauvegarde, choisissez l'ID du point de récupération de la ressource.

   b. Dans le coin supérieur droit du volet, choisissez Restaurer (vous pouvez également accéder au coffre-fort de sauvegarde, rechercher le point de récupération, puis cliquer sur Actions, puis sur Restaurer).
4. Sur la page Restaurer la sauvegarde, recherchez le panneau intitulé Restaurer avec des balises. Pour inclure toutes les balises de la ressource d'origine, maintenez la case cochée (notez que cette case est cochée par défaut dans la console).
5. Cliquez sur Restaurer la sauvegarde après avoir sélectionné tous vos paramètres et rôles préférés.

Pour inclure des balises par programmation

Utilisez l'opération d'API `StartRestoreJob`. Assurez-vous que le paramètre booléen suivant est défini sur `True` :

```
CopySourceTagsToRestoredResource = true
```

Si le paramètre booléen est `CopySourceTagsToRestoredResource` = `True`, la tâche de restauration copiera les balises de la ou des ressources d'origine vers le matériel restauré.

> **Important**
>
> La tâche de restauration échouera si ce paramètre est inclus pour une ressource non prise en charge (VMware, systèmes sur site AWS Outposts, instances SAP HANA sur EC2, Timestream, DynamoDB, Advanced DynamoDB et Amazon S3).

```
{
    "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
    "Metadata": {
        "InstanceInitiatedShutdownBehavior": "stop",
        "DisableApiTermination": "false",
        "EbsOptimized": "false",
        "InstanceType": "t1.micro",
        "SubnetId": "subnet-123ab456cd7efgh89",
        "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
        "Placement": "{\"GroupName\":null,\"Tenancy\":\"default\"}",
        "HibernationOptions": "{\"Configured\":false}",
        "IamInstanceProfileName": "UseBackedUpValue",
        "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
    },
    "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
    "ResourceType": "EC2",
    "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
    "CopySourceTagsToRestoredResource": true
}
```

Résolution des problèmes de restauration des balises

ERREUR : autorisations insuffisantes

SOLUTION : assurez-vous de disposer des autorisations nécessaires dans votre rôle de restauration afin de pouvoir inclure des balises sur votre ressource restaurée. La politique de rôle de service AWS géré par défaut pour AWSBackupServiceRolePolicyForRestoresles restaurations contient les autorisations nécessaires pour cette tâche.

Si vous choisissez d'utiliser un rôle personnalisé, assurez-vous que les autorisations suivantes sont présentes :

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

Pour plus d'informations, consultez Autorisations d'API.

Statuts de la tâche de restauration

Vous pouvez afficher le statut d'une tâche de restauration sur la page Tâches de la console AWS Backup . Les statuts d'une tâche de restauration peuvent être en attente, en cours d'exécution, terminée, abandonnée et échec.

Rubriques

Restauration des données S3

Vous pouvez restaurer les données S3 que vous avez sauvegardées AWS Backup à l'aide de la classe de stockage S3 Standard. Vous pouvez restaurer tous les objets d'un compartiment ou des objets spécifiques. Vous pouvez les restaurer dans un compartiment existant ou nouveau.

Autorisations de restauration Amazon S3

Avant de commencer à restaurer les ressources, assurez-vous que le rôle que vous utilisez dispose des autorisations suffisantes.

Pour plus d'informations, consultez les entrées suivantes sur les politiques :

1. AWSBackupServiceRolePolicyForS3Restore
2. AWSBackupServiceRolePolicyForRestores
3. Politiques gérées pour AWS Backup

Considérations relatives à la restauration sur Amazon S3

- AWS Backup crée une sauvegarde de toutes vos versions de S3, mais restaure uniquement la dernière version de la pile de versions à tout moment.
- Les listes de contrôle d'accès (ACL) doivent être activées dans le compartiment de destination, sinon la tâche échouera. Pour activer les listes ACL, suivez les instructions de la page Configuration des listes ACL.
- Les restaurations d'objets sont ignorées si le compartiment source contient un objet portant le même nom ou le même ID de version.
- Si vous restaurez des objets spécifiques, vous pouvez restaurer la version actuelle d'un objet.
- Lorsque vous effectuez une restauration dans le compartiment S3 d'origine,
  - AWS Backup n'effectue pas de restauration destructive, c'est-à-dire qu' AWS Backup il ne place pas un objet dans un bucket à la place d'un objet qui existe déjà, quelle que soit sa version.
  - Dans la version actuelle, un marqueur de suppression est considéré comme un objet inexistant, de sorte qu'une restauration peut avoir lieu.
  - AWS Backup ne supprime pas d'objets (sans marqueurs de suppression) d'un bucket lors d'une restauration (exemple : les clés actuellement présentes dans le bucket qui n'étaient pas présentes lors de la sauvegarde seront conservées).
- Restauration de copies interrégionales
  - Bien que les sauvegardes S3 puissent être copiées d'une région à l'autre, les tâches de restauration ne sont effectuées que dans la même région dans laquelle se trouve la sauvegarde ou la copie d'origine.

    Example

    Exemple : un compartiment S3 créé dans la région USA Est (Virginie du Nord) peut être copié dans la région Canada (Centre). La tâche de restauration peut être lancée à l'aide du compartiment d'origine dans la région USA Est (Virginie du Nord) et restaurée dans cette région,

ou la tâche de restauration peut être lancée à l'aide de la copie dans la région du Canada (centre) et restaurée dans cette région.

- La méthode de chiffrement d'origine ne peut pas être utilisée pour restaurer un point de restauration (sauvegarde) copié depuis une autre région. AWS KMS Le chiffrement des copies entre régions n'est pas disponible pour les ressources Amazon S3 ; utilisez plutôt un type de chiffrement différent pour une tâche de restauration.

Utiliser la AWS Backup console pour restaurer les points de récupération Amazon S3

Pour restaurer vos données Amazon S3 à l'aide de la AWS Backup console :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées et sélectionnez l'ID de ressource Amazon S3 que vous voulez restaurer.
3. Sur la page Détails de la ressource, vous verrez une liste des points de récupération pour l'ID de ressource sélectionné. Pour restaurer une ressource :

   a. Dans le volet Sauvegarde, choisissez l'ID du point de récupération de la ressource.

   b. Dans le coin supérieur droit du volet, choisissez Restaurer.

      (Vous pouvez également accéder au coffre-fort de sauvegarde, trouver le point de récupération, puis cliquer sur Actions, puis sur Restaurer.)
4. Si vous restaurez une sauvegarde continue, dans le volet Heure de restauration, sélectionnez l'une des options suivantes :

   a. Acceptez la valeur par défaut pour restaurer la Dernière heure de restauration.

   b. Spécifiez la date et l'heure de restauration.
5. Dans le volet Paramètres, indiquez si vous souhaitez Restaurer le compartiment entier ou effectuer une Restauration au niveau des éléments.

   a. Si vous choisissez la restauration au niveau de l'élément, vous restaurez jusqu'à 5 éléments (objets ou dossiers dans un compartiment) par tâche de restauration en spécifiant l'URI S3 de chaque élément qui identifie de manière unique cet objet.

      (Pour plus d'informations sur les URI de compartiments S3, consultez Méthodes d'accès à un compartiment dans le Guide de l'utilisateur Amazon Simple Storage Service.)

   b. Choisissez Ajouter un élément pour spécifier un autre élément à restaurer.

6. Choisissez votre Destination de restauration. Vous pouvez Restaurer vers le compartiment source, Utiliser un compartiment existant ou Créer un compartiment.

   > **Note**
   >
   > La gestion des versions doit être activée dans votre compartiment de destination de restauration. AWS Backup vous avertit si le bucket que vous sélectionnez ne répond pas à cette exigence.

   a. Si vous choisissez Utiliser un compartiment existant, sélectionnez le compartiment S3 de destination dans le menu déroulant qui affiche tous les compartiments existants dans votre région actuelle AWS .

   b. Si vous choisissez Créer un compartiment, saisissez le Nouveau nom de compartiment. La gestion des versions S3 est activée par défaut dans le nouveau compartiment. Les paramètres Bloquer l'accès public (BPA) seront désactivés par défaut. Vous pouvez modifier ces paramètres après avoir créé le compartiment dans S3.

7. Pour le chiffrement des objets de votre compartiment S3, vous pouvez choisir le chiffrement des objets restauré. Utilisez les clés de chiffrement d'origine (par défaut), la Clé Amazon S3 (SSE-S3) ou la CléAWS Key Management Service (SSE-KMS).

   Ces paramètres s'appliquent uniquement au chiffrement des objets du compartiment S3. Cela n'affecte pas le chiffrement du compartiment lui-même.

   a. Utiliser les clés de chiffrement d'origine (par défaut) restaure les objets avec les mêmes clés de chiffrement que celles utilisées par l'objet source. Si un objet source n'a pas été chiffré, cette méthode le restaure sans chiffrement.

      Cette option de restauration vous permet de choisir éventuellement une clé de chiffrement de remplacement pour chiffrer le ou les objets de restauration si la clé d'origine n'est pas disponible.

   b. Si vous choisissez la Clé Amazon S3 (SSE-S3), vous n'avez pas besoin de spécifier d'autres options.

   c. Si vous choisissez la AWS Key Management Service clé (SSE-KMS), vous pouvez effectuer les choix suivants : Clé gérée par AWS (aws/s3), Choisissez parmi vos AWS KMS clés ou Entrez l'ARN de la clé. AWS KMS

i. Si vous choisissez Clé gérée par AWS (aws/s3), vous n'avez pas besoin de spécifier d'autres options.

ii. Si vous choisissez parmi vos AWS KMS clés, sélectionnez une AWS KMS clé dans le menu déroulant. Vous pouvez également choisir Créer une clé.

iii. Si vous entrez l'ARN de la AWS KMS clé, saisissez l'ARN dans la zone de texte. Vous pouvez également choisir Créer une clé.

8. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
9. Choisissez Restore backup. Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon S3

Utilisez `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon S3 :

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
 required for item-level restore.
NewBucket // Boolean to indicate whether to create a new bucket.
Encrypted // Boolean to indicate whether to encrypt the restored data.
CreationToken // An idempotency token.
EncryptionType // The type of encryption to encrypt your restored objects. Options
 are original (same encryption as the original object), SSE-S3, or SSE-KMS).
RestoreTime // The restore time (only valid for continuous recovery points where it is
 required, in format 2021-11-27T03:30:27Z).

// Optional metadata:
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
aws:backup:request-id
```

Statut du point de récupération

Les points de récupération auront un statut indiquant leur état.

`PARTIAL`le statut indique qu' AWS Backup il n'a pas été possible de créer le point de restauration avant la fermeture de la fenêtre de sauvegarde. Pour augmenter la fenêtre de votre plan de sauvegarde à l'aide de l'API, consultez UpdateBackupPlan. Vous pouvez également augmenter la fenêtre de votre plan de sauvegarde à l'aide de la console en choisissant et en modifiant votre plan de sauvegarde.

`EXPIRED`le statut indique que le point de restauration a dépassé sa période de rétention, mais qu'il n'est AWS Backup pas autorisé ou qu'il est incapable de le supprimer pour une autre raison. Pour supprimer manuellement ces points de récupération, voir Étape 3 : Supprimer les points de récupération dans la section Nettoyage des ressources du guide Mise en route.

Le statut `STOPPED` apparaît lors d'une sauvegarde continue lorsqu'un utilisateur a effectué une action qui entraîne la désactivation de la sauvegarde continue. Cela peut être dû à la suppression des autorisations, à la désactivation de la gestion des versions, à la désactivation des événements envoyés à Amazon EventBridge ou à la désactivation des EventBridge règles mises en place par. AWS Backup

Pour résoudre le statut `STOPPED`, assurez-vous que toutes les autorisations demandées sont en place et que la gestion des versions est activée sur le compartiment S3. Une fois ces conditions remplies, la prochaine instance d'une règle de sauvegarde exécutée entraînera la création d'un nouveau point de récupération continue. Les points de récupération ayant le statut ARRÊTÉ n'ont pas besoin d'être supprimés.

Restauration d'une machine virtuelle à l'aide de AWS Backup

Vous pouvez restaurer une machine virtuelle sur VMware, VMware Cloud on AWS, VMware Cloud on AWS Outposts, un volume Amazon EBS ou une instance Amazon EC2. La restauration (ou la migration) d'une machine virtuelle vers EC2 nécessite une licence. Par défaut, AWS inclura une licence (des frais s'appliquent). Pour plus d'informations, consultez la section Options de licence dans le guide de l'utilisateur de VM Import/Export.

Vous pouvez restaurer une machine virtuelle VMware à l'aide de la AWS Backup console ou via le AWS CLI. Lorsqu'une machine virtuelle est restaurée, le dossier VMware Tools n'est pas inclus. Consultez la documentation VMware pour réinstaller VMware Tools.

AWS Backup les restaurations de machines virtuelles ne sont pas destructives, ce qui signifie AWS Backup qu'elles ne remplacent pas les machines virtuelles existantes lors d'une restauration. La tâche de restauration déploie plutôt une nouvelle machine virtuelle.

Tâches

Considérations relatives à la restauration d'une machine virtuelle sur une instance Amazon EC2

- La restauration (ou la migration) d'une machine virtuelle vers EC2 nécessite une licence. Par défaut, AWS inclut une licence (des frais s'appliquent). Pour plus d'informations, consultez la section Options de licence dans le guide de l'utilisateur de VM Import/Export.
- Il existe une limite maximale de 5 To (téraoctets) pour chaque disque de machine virtuelle.
- Vous ne pouvez pas spécifier de paire de clés lorsque vous restaurez la machine virtuelle sur une instance. Vous pouvez ajouter une paire de clés `authorized_keys` pendant le lancement (via les données utilisateur de l'instance) ou après le lancement (comme décrit dans cette section de résolution des problèmes du guide de l'utilisateur Amazon EC2).
- Vérifiez que votre système d'exploitation est compatible pour l'importation vers et l'exportation depuis Amazon EC2 dans le guide de l'utilisateur de VM Import/Export.
- Consultez les limites liées à l'importation de machines virtuelles vers Amazon EC2 dans le guide de l'utilisateur VM Import/Export.
- Lorsque vous effectuez une restauration sur une instance Amazon EC2 à l'aide de AWS CLI, vous devez spécifier. `"RestoreTo":"EC2Instance"` Tous les autres attributs ont des valeurs par défaut.

Utiliser la AWS Backup console pour restaurer les points de restauration des machines virtuelles

Vous pouvez restaurer une machine virtuelle à partir de plusieurs emplacements dans le volet de navigation gauche de la AWS Backup console :

- Choisissez Hyperviseurs pour afficher les points de récupération des machines virtuelles gérées par un hyperviseur connecté à AWS Backup.
- Choisissez Machines virtuelles pour afficher les points de récupération des machines virtuelles sur tous les hyperviseurs connectés à AWS Backup.

- Choisissez Backup vaults pour afficher les points de restauration stockés dans un AWS Backup coffre-fort spécifique.
- Choisissez Ressources protégées pour afficher les points de restauration de toutes vos ressources AWS Backup protégées.

Si vous devez restaurer une machine virtuelle qui n'est plus connectée à Backup gateway, choisissez Coffres de sauvegarde ou Ressources protégées pour localiser votre point de récupération.

Options

- Restaurer sur VMware
- Restaurer sur un volume Amazon EBS
- Restaurer sur une instance Amazon EC2

Pour restaurer une machine virtuelle sur VMware, VMware Cloud on AWS et VMware Cloud on AWS Outposts

1. Dans les vues Hyperviseurs ou Machines virtuelles, choisissez le Nom de la machine virtuelle à restaurer. Dans la vue Ressources protégées, choisissez l'ID de ressource de la machine virtuelle à restaurer.
2. Cliquez sur le bouton circulaire situé à côté de l'ID du point de récupération à restaurer.
3. Choisissez Restore (Restaurer).
4. Choisissez le Type de restauration.
    a. La Restauration complète restaure tous les disques de la machine virtuelle.
    b. La Restauration au niveau du disque restaure une sélection définie par l'utilisateur d'un ou de plusieurs disques. Utilisez le menu déroulant pour sélectionner les disques à restaurer.
5. Choisissez l'Emplacement de la restauration. Les options sont VMware, VMware Cloud on AWS et VMware Cloud on AWS Outposts.
6. Si vous effectuez une restauration complète, passez à la prochaine étape. Si vous effectuez une restauration au niveau du disque, un menu déroulant s'affichera sous Disques de machine virtuelle. Choisissez un ou plusieurs volumes de démarrage à restaurer.
7. Sélectionnez un hyperviseur dans le menu déroulant pour gérer la machine virtuelle restaurée

8. Pour la machine virtuelle restaurée, utilisez les bonnes pratiques de votre organisation en matière de machine virtuelle pour spécifier :

    a. Nom

    b. Chemin (tel que `/datacenter/vm`)

    c. Nom de la ressource de calcul (tel que VMHost ou Cluster)

    Si un hôte fait partie d'un cluster, vous ne pouvez pas effectuer de restauration sur l'hôte, mais uniquement sur le cluster donné.

    d. Entrepôt de données
9. Pour Restaurer le rôle, sélectionnez le Rôle par défaut (recommandé) ou Sélectionner un rôle IAM à l'aide du menu déroulant.
10. Choisissez Restore backup.
11. Facultatif : vérifiez que votre tâche de restauration a le statut `Completed`. Dans le menu de navigation de gauche, choisissez Tâches.

Pour restaurer une machine virtuelle sur un volume Amazon EBS

1. Dans les vues Hyperviseurs ou Machines virtuelles, choisissez le Nom de la machine virtuelle à restaurer. Dans la vue Ressources protégées, choisissez l'ID de ressource de la machine virtuelle à restaurer.
2. Cliquez sur le bouton circulaire situé à côté de l'ID du point de récupération à restaurer.
3. Choisissez Restore (Restaurer).
4. Choisissez le Type de restauration.

    - La Restauration du disque restaure une sélection définie par l'utilisateur d'un disque. Utilisez le menu déroulant pour sélectionner le disque à restaurer.
5. Choisissez l'Emplacement de restauration comme Amazon EBS.
6. Dans le menu déroulant Disque de machine virtuelle, choisissez le volume de démarrage à restaurer.
7. Sous Type de volume EBS, choisissez le type de volume.
8. Choisissez votre Zone de disponibilité.
9. Chiffrement (facultatif). Cochez cette case si vous choisissez de chiffrer le volume EBS.
10. Sélectionnez votre clé KMS dans le menu.

11. Pour le rôle Restaurer, sélectionnez le rôle par défaut (recommandé) ou Choisissez un rôle IAM.
12. Choisissez Restore backup.
13. Facultatif : vérifiez que votre tâche de restauration a le statut `Completed`. Dans le menu de navigation de gauche, choisissez Tâches.
14. Facultatif : consultez Comment créer un volume logique LVM sur un volume EBS entier ? pour en savoir plus sur la façon de monter des volumes gérés et d'accéder aux données sur le volume Amazon EBS restauré.

Pour restaurer une machine virtuelle sur une instance Amazon EC2

1. Dans les vues Hyperviseurs ou Machines virtuelles, choisissez le Nom de la machine virtuelle à restaurer. Dans la vue Ressources protégées, choisissez l'ID de ressource de la machine virtuelle à restaurer.
2. Cliquez sur le bouton circulaire situé à côté de l'ID du point de récupération à restaurer.
3. Choisissez Restore (Restaurer).
4. Choisissez le Type de restauration.
   - La Restauration complète restaure complètement le système de fichiers, y compris le dossier et les fichiers au niveau racine.
5. Choisissez l'Emplacement de restauration comme Amazon EC2.
6. Pour Type d'instance, choisissez la combinaison de calcul et de mémoire requise pour exécuter votre application sur votre nouvelle instance.

   > **Tip**
   >
   > Choisissez un type d'instance qui correspond ou dépasse les spécifications de la machine virtuelle d'origine. Pour plus d'informations, consultez le guide des types d'instances Amazon EC2.

7. Pour Virtual Private Cloud (VPC), choisissez un cloud privé virtuel (VPC) qui définit l'environnement réseau de l'instance.
8. Pour Sous-réseau, choisissez l'un des sous-réseaux du VPC. Votre instance reçoit une adresse IP privée depuis la plage d'adresses de sous-réseau.
9. Pour les groupes de sécurité, choisissez un groupe de sécurité qui agit comme un pare-feu pour le trafic vers votre instance.

10. Pour le rôle Restaurer, sélectionnez le rôle par défaut (recommandé) ou Choisissez un rôle IAM.
11. Facultatif : pour exécuter un script sur votre instance au lancement, développez les paramètres avancés et entrez le script dans Données utilisateur.
12. Choisissez Restore backup.
13. Facultatif : vérifiez que votre tâche de restauration a le statut `Completed`. Dans le menu de navigation de gauche, choisissez Tâches.

AWS CLI À utiliser pour restaurer les points de restauration des machines virtuelles

Utilisez `StartRestoreJob`.

Vous pouvez spécifier les métadonnées suivantes pour restaurer une machine virtuelle sur Amazon EC2 et Amazon EBS :

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

Vous pouvez spécifier les métadonnées suivantes pour la restauration d'une machine virtuelle sur VMware, VMware Cloud on AWS et VMware Cloud on AWS Outpost :

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

L'exemple suivant décrit comment effectuer une restauration complète dans VMware :

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-
east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/
vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":"[{\"DiskId
\":\"2000\",\"Label\":\"Hard disk 1\"}]","vmId":"vm-101"}'
```

Restauration d'un système de fichiers FSX

Les options de restauration disponibles lorsque vous les utilisez AWS Backup pour restaurer les systèmes de fichiers Amazon FSx sont les mêmes que pour la sauvegarde native d'Amazon FSx. Vous pouvez utiliser le point de restauration d'une sauvegarde pour créer un nouveau système de fichiers et restaurer un point-in-time instantané d'un autre système de fichiers.

Lors de la restauration des systèmes de fichiers Amazon FSx, AWS Backup crée un nouveau système de fichiers et le remplit avec les données (Amazon FSx for NetApp ONTAP permet de restaurer un volume sur un système de fichiers existant). Cela est similaire à la façon dont Amazon FSx natif sauvegarde et restaure les systèmes de fichiers. La restauration d'une sauvegarde sur un nouveau système de fichiers prend le même temps que la création d'un nouveau système de fichiers. Les données restaurées à partir de la sauvegarde sont chargées de façon différée dans le système de fichiers. Il se peut donc que vous rencontriez une latence légèrement plus élevée au cours du processus.

> **Note**
>
> Vous ne pouvez pas effectuer de restauration sur un système de fichiers Amazon FSx existant, ni restaurer des fichiers ou des dossiers individuels.
> FSx pour ONTAP ne prend pas en charge la sauvegarde de certains types de volumes, notamment les volumes DP (protection des données), les volumes LS (partage de charge),

les volumes complets ou les volumes sur des systèmes de fichiers pleins. Pour plus d'informations, consultez Fonctionnement de FSx pour ONTAP avec les sauvegardes.
AWS Backup les coffres-forts contenant les points de restauration des systèmes de fichiers Amazon FSx sont visibles à l'extérieur de. AWS Backup Vous pouvez restaurer les points de récupération à l'aide d'Amazon FSx, mais vous ne pouvez pas les supprimer.

Vous pouvez consulter les sauvegardes créées par la fonctionnalité de sauvegarde automatique intégrée d'Amazon FSx depuis la AWS Backup console. Vous pouvez également récupérer ces sauvegardes à l'aide de AWS Backup. Toutefois, vous ne pouvez pas supprimer ces sauvegardes ni modifier les plannings de sauvegarde automatiques de vos systèmes de fichiers Amazon FSx à l'aide de. AWS Backup

Vous pouvez restaurer les sauvegardes créées à AWS Backup l'aide de la AWS Backup console, de l'API ou AWS CLI. Cette section explique comment utiliser la AWS Backup console pour restaurer les systèmes de fichiers Amazon FSx.

Utiliser la AWS Backup console pour restaurer les points de restauration Amazon FSx

Restauration d'un système de fichiers Amazon FSx for Windows File Server

Pour restaurer un système de fichiers Amazon FSx for Windows File Server

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de ressource Amazon FSx que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer la sauvegarde.
5. Dans la section Informations sur le système de fichiers, l'ID de votre sauvegarde est affiché sous ID de sauvegarde et le type de système de fichiers est affiché sous Type de système de fichiers. Vous pouvez restaurer à la fois les systèmes de fichiers FSx for Windows File Server et FSx pour Lustre.
6. Pour Type de déploiement, acceptez le choix par défaut. Vous ne pouvez pas modifier le type de déploiement d'un système de fichiers lors de la restauration.
7. Choisissez le Type de stockage à utiliser. Si la capacité de stockage de votre système de fichiers est inférieure à 2 000 GiO, vous ne pouvez pas utiliser le type de stockage HDD.

8. Pour Capacité de débit, choisissez Capacité de débit recommandée pour utiliser le débit recommandé de 16 Mo par seconde (Mo/s), ou choisissez Spécifier la capacité de débit et entrez un nouveau débit.
9. Dans la section Réseau et sécurité, fournissez les informations requises.
10. Si vous restaurez un système de fichiers FSx for Windows File Server, fournissez les informations d'authentification Windows utilisées pour accéder au système de fichiers, ou vous pouvez en créer un nouveau.

    > **Note**
    >
    > Lorsque vous restaurez une sauvegarde, vous ne pouvez pas modifier le type d'Active Directory sur le système de fichiers.

    Pour plus d'informations sur Microsoft Active Directory, consultez Utilisation d'Active Directory dans Amazon FSx for Windows File Server dans le Guide de l'utilisateur Amazon FSx for Windows File Server.
11. (Facultatif) Dans la section Sauvegarde et maintenance, fournissez les informations permettant de définir vos préférences de sauvegarde.
12. Dans la section Rôle de restauration, choisissez le rôle IAM qu' AWS Backup utilisera pour créer et gérer vos sauvegardes en votre nom. Nous vous recommandons de choisir le Rôle par défaut. S'il n'y a pas de rôle par défaut, il sera créé pour vous avec les autorisations appropriées. Vous pouvez également fournir votre propre rôle IAM.
13. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Restauration d'un système de fichiers Amazon FSx pour Lustre

AWS Backup prend en charge les systèmes de fichiers Amazon FSx for Lustre dotés d'un type de déploiement de stockage persistant et qui ne sont pas liés à un référentiel de données tel qu'Amazon S3.

Pour restaurer un système de fichiers Amazon FSx pour Lustre

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de ressource Amazon FSx que vous voulez restaurer.

3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer la sauvegarde vers un nouveau système de fichiers.
5. Dans la section Paramètres, l'ID de votre sauvegarde est affiché sous ID de sauvegarde et le type de système de fichiers est affiché sous Type de système de fichiers. Le Type de système de fichiers doit être Lustre.
6. (Facultatif) Entrez un nom pour votre système de fichiers.
7. Choisissez un type de déploiement. AWS Backup prend uniquement en charge le type de déploiement persistant. Vous ne pouvez pas modifier le type de déploiement d'un système de fichiers lors de la restauration.

   Le type de déploiement persistant est destiné au stockage à long terme. Pour obtenir des informations détaillées sur les options de déploiement de FSx pour Lustre, consultez Utilisation des options de déploiement disponibles pour les systèmes de fichiers Amazon FSx pour Lustre dans le Guide de l'utilisateur Amazon FSx pour Lustre.
8. Choisissez le Débit par unité de stockage que vous souhaitez utiliser.
9. Spécifiez la Capacité de stockage à utiliser. Entrez une capacité comprise entre 32 GiO et 64 436 GiO.
10. Dans la section Réseau et sécurité, fournissez les informations requises.
11. (Facultatif) Dans la section Sauvegarde et maintenance, fournissez les informations permettant de définir vos préférences de sauvegarde.
12. Dans la section Rôle de restauration, choisissez le rôle IAM qu' AWS Backup utilisera pour créer et gérer vos sauvegardes en votre nom. Nous vous recommandons de choisir le Rôle par défaut. S'il n'y a pas de rôle par défaut, il sera créé pour vous avec les autorisations appropriées. Vous pouvez également fournir votre rôle IAM.
13. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Restauration des volumes Amazon FSx pour NetApp ONTAP

Pour restaurer les volumes Amazon FSx pour NetApp ONTAP :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de ressource Amazon FSx que vous voulez restaurer.

3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer.

   La première section, Informations sur le système de fichiers, affiche l'ID du point de récupération, l'ID du système de fichiers et le type de système de fichiers.
5. Sous Options de restauration, plusieurs sections s'offrent à vous. Choisissez d'abord le Système de fichiers dans le menu déroulant.
6. Choisissez ensuite la Machine virtuelle de stockage préférée dans le menu déroulant.
7. Entrez un nom pour votre volume.
8. Spécifiez le Chemin de jonction, c'est-à-dire l'emplacement dans votre système de fichiers où votre volume sera monté.
9. Spécifiez la Taille du volume en mégaoctets (Mo) que vous créez.
10. (Facultatif) Vous pouvez choisir Activer l'efficacité de stockage en cochant la case. Cela permettra la déduplication, la compression et le compactage.
11. Dans le menu déroulant Politique de hiérarchisation des groupes de capacité, sélectionnez la préférence de hiérarchisation.
12. Dans les autorisations de restauration, choisissez le rôle IAM qui AWS Backup sera utilisé pour restaurer les sauvegardes.
13. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Restauration d'un système de fichiers Amazon FSx pour OpenZFS

Pour restaurer un système de fichiers FSx pour OpenZFS

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de ressource Amazon FSx que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Choisissez l'ID du point de récupération de la ressource.
4. En haut à droite du volet, choisissez Restaurer pour ouvrir la page Restaurer la sauvegarde.

   Dans la section Informations sur le système de fichiers, l'ID de votre sauvegarde est affiché sous ID de sauvegarde et le type de système de fichiers est affiché sous Type de système de fichiers. Le type de système de fichiers doit être FSx pour OpenZFS.

5. Sous Options de restauration, vous pouvez sélectionner Restauration rapide ou Restauration standard. La restauration rapide utilisera les paramètres par défaut du système de fichiers source. Si vous effectuez une restauration rapide, passez à l'étape 7.

   Si vous choisissez la restauration standard, spécifiez les configurations supplémentaires suivantes :

   a. IOPS SSD provisionnées : vous pouvez choisir la case d'option Automatique ou choisir l'option Provisionné par l'utilisateur si disponible.

   b. Capacité de débit : vous pouvez choisir la Capacité de débit recommandée de 64 Mo/sec ou vous pouvez choisir Spécifier la capacité de débit.

   c. (Facultatif) Groupes de sécurité VPC : vous pouvez spécifier des groupes de sécurité VPC à associer à l'interface réseau de votre système de fichiers.

   d. Clé de chiffrement : Spécifiez la AWS Key Management Service clé pour protéger les données du système de fichiers restaurées au repos.

   e. (Facultatif) Configuration du volume racine : cette configuration est réduite par défaut. Vous pouvez l'agrandir en cliquant sur le carat pointant vers le bas (flèche). La création d'un système de fichiers à partir d'une sauvegarde créera un nouveau système de fichiers ; les volumes et les instantanés conserveront leurs configurations source.

   f. (Facultatif) Sauvegarde et maintenance : pour définir une sauvegarde planifiée, cliquez sur le carat pointant vers le bas (flèche) pour développer la section. Vous pouvez choisir la fenêtre de sauvegarde, l'heure et les minutes, la période de rétention et la fenêtre de maintenance hebdomadaire.

6. (Facultatif) Vous pouvez entrer un nom pour votre volume.

7. La Capacité de stockage SDD affichera la capacité de stockage du système de fichiers.

8. Choisissez le Cloud privé virtuel (VPC) à partir duquel votre système de fichiers est accessible.

9. Dans le menu déroulant Sous-réseau, choisissez le sous-réseau dans lequel réside l'interface réseau de votre système de fichiers.

10. Dans la section Rôle de restauration, choisissez le rôle IAM qui AWS Backup sera utilisé pour créer et gérer vos sauvegardes en votre nom. Nous vous recommandons de choisir le Rôle par défaut. S'il n'y a pas de rôle par défaut, il sera créé pour vous avec les autorisations appropriées. Vous pouvez également choisir un rôle IAM.

11. Vérifiez toutes vos entrées, puis choisissez Restaurer la sauvegarde.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon FSx

Pour restaurer Amazon FSx à l'aide de l'API ou de l'interface de ligne de commande, utilisez `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon FSx :

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

Métadonnées de restauration FSx for Windows File Server

Vous pouvez spécifier les métadonnées suivantes lors des restaurations FSx for Windows File Server :

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

Métadonnées de restauration FSx pour Lustre

Vous pouvez spécifier les options `PerUnitStorageThroughput` et `DriveCacheType` suivantes pendant une restauration FSx pour Lustre.

Métadonnées de restauration FSx pour ONTAP

Vous pouvez spécifier les métadonnées suivantes lors d'une restauration FSx pour ONTAP :

- Nom #name du volume à créer
- OntapConfiguration: # configuration ontap
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

Métadonnées de restauration FSx pour OpenZFS

Vous pouvez spécifier les métadonnées suivantes lors d'une restauration FSx pour OpenZFS :

- `ThroughputCapacity`
- `DesklopsConfiguration`
- Si Iops est spécifié, vous devez inclure une valeur comprise entre 0 et 160 000, mais ne pas inclure Mode.

Exemple de commande de restauration d'une interface de ligne de commande :

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/
backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-
type "FSx" --region us-west-2 --metadata 'SubnetIds="[\"subnet-1234\",
\"subnet-5678\"]",StorageType=HDD,SecurityGroupIds="[\"sg-bb5efdc4\",
\"sg-0faa52\"]",WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\",
\"PreferredSubnetId\": \"subnet-1234\",\"ThroughputCapacity\": \"32\"}"'
```

Exemple de métadonnées de restauration :

```
"restoreMetadata":  "{\"StorageType\":\"SSD\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\",\"StorageCapacity
\":\"1200\",\"VpcId\":\"vpc-0ab0979fa431ad326\",\"FileSystemType\":\"LUSTRE\",
\"LustreConfiguration\":\"{\\\"WeeklyMaintenanceStartTime\\\":\\\"4:10:30\\\",\\
\"DeploymentType\\\":\\\"PERSISTENT_1\\\",\\\"PerUnitStorageThroughput\\\":50,\\
```

```
\"CopyTagsToBackups\\\":true}\",\"FileSystemId\":\"fs-0ca11fb3d218a35c2\",\"SubnetIds
\":\"[\\\"subnet-0e66e94eb43235351\\\"]\"}"
```

Restauration d'un volume Amazon EBS

Lorsque vous restaurez un instantané Amazon Elastic Block Store (Amazon EBS) AWS Backup , vous créez un nouveau volume Amazon EBS que vous pouvez associer à votre instance Amazon EC2.

Vous pouvez choisir de restaurer l'instantané en tant que volume EBS ou en tant que volume AWS Storage Gateway .

Utiliser la AWS Backup console pour restaurer les points de récupération Amazon EBS

Pour restaurer un volume Amazon EBS

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées, puis l'ID de ressource EBS que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Spécifiez les paramètres de restauration de votre ressource. Les paramètres de restauration que vous saisissez sont spécifiques au type de ressource sélectionné.

   Pour Type de ressource, choisissez la AWS ressource à créer lors de la restauration de cette sauvegarde.
5. Si vous choisissez Volume EBS, indiquez les valeurs Type de volume, Taille (Gio), et choisissez une Zone de disponibilité.

   - Après Débit, il y aura une case à cocher facultative Chiffrer ce volume. Cette option restera active si le point de récupération EBS est chiffré.

     Vous pouvez spécifier une clé KMS ou créer une AWS KMS clé.

   Si vous choisissez Volume Storage Gateway, choisissez une Passerelle accessible. Choisissez également votre Nom de cible iSCSI.

- Pour les passerelles Volume stocké, choisissez un ID de disque.
- Pour les passerelles Volume mis en cache, choisissez une capacité au moins égale à votre ressource protégée.

6. Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration.

> **Note**
>
> Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle par défaut est créé pour vous avec les autorisations appropriées. Vous pouvez supprimer ce rôle par défaut ou le rendre inutilisable.

7. Choisissez Restore backup.

   Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

La restauration d'un instantané EBS archivé le déplace temporairement d'un stockage à froid vers un stockage à chaud afin de créer un nouveau volume EBS. Ce type de restauration entraîne des frais de récupération uniques. Les frais de stockage pour le stockage à chaud et à froid sont facturés pendant cette période de restauration. Les volumes EBS stockés à froid ne peuvent pas être restaurés sur un volume de passerelle Backup.

Vous pouvez restaurer un instantané EBS archivé dans un stockage à froid à l'aide de la console AWS Backup ou de la ligne de commande. Une restauration à partir d'un stockage à froid peut prendre jusqu'à 72 heures. Pour plus d'informations, consultez Archiver des instantanés Amazon EBS dans le guide de l'utilisateur Amazon EBS.

Console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Accédez à Coffres de sauvegarde > *Coffre* > Restaurer un instantané EBS archivé.
3. Dans la section Paramètres, entrez une valeur comprise entre 0 et 180 inclus, qui indique le nombre de jours nécessaires pour restaurer temporairement un instantané archivé.
4. Entrez d'autres paramètres : type de volume, taille, IOPS, zone de disponibilité, débit et chiffrement.
5. Choisissez votre rôle de restauration.

6. Sélectionnez Restaurer la sauvegarde. Dans la fenêtre contextuelle de confirmation, confirmez les instantanés et le type de restauration. Sélectionnez ensuite Restaurer l'instantané.

AWS CLI

1. Utiliser `start-restore-job`
2. Incluez les paramètres.
3.
4.
5.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon EBS

Pour restaurer Amazon EBS à l'aide de l'API ou de l'interface de ligne de commande, utilisez `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon EBS :

```
availabilityZone
volumeType
volumeSize
iops
throughput
temporaryRestoreDays
encrypted // if set to true, encryption will be enabled as volume is restored
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
 of default KMS Key Id
aws:backup:request-id
```

Exemple :

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Restauration d'un système de fichiers Amazon EFS

Si vous restaurez une instance Amazon Elastic File System (Amazon EFS), vous pouvez effectuer une restauration complète ou une restauration au niveau des éléments.

Restauration complète

Lorsque vous effectuez une restauration complète, l'ensemble du système de fichiers est restauré.

AWS Backup ne prend pas en charge les restaurations destructives avec Amazon EFS. Une restauration destructive se produit lorsqu'un système de fichiers restauré supprime ou remplace le système de fichiers source ou existant. AWS Backup restaure plutôt votre système de fichiers dans un répertoire de restauration situé hors du répertoire racine.

Restauration au niveau des éléments

Lorsque vous effectuez une restauration au niveau de l'élément, elle AWS Backup restaure un fichier ou un répertoire spécifique. Vous devez spécifier le chemin relatif à la racine du système de fichiers. Par exemple, si le système de fichiers est monté sur `user/home/myname/efs/file1` et que le chemin d'accès à ce dernier est **`/file1`**, saisissez `/user/home/myname/efs`. Les chemins sont sensibles à la casse. Les caractères génériques et les chaînes regex ne sont pas pris en charge. Votre chemin peut être différent de celui de l'hôte si le système de fichiers est monté à l'aide d'un point d'accès.

Vous pouvez sélectionner jusqu'à 10 éléments lorsque vous utilisez la console pour exécuter une restauration EFS. Il n'y a aucune limite d'éléments lorsque vous utilisez l'interface de ligne de commande pour effectuer une restauration ; toutefois, la longueur des métadonnées de restauration pouvant être transmises est limitée à 200 Ko.

Vous pouvez restaurer ces éléments dans un système de fichiers nouveau ou existant. Dans tous les cas, AWS Backup crée un nouveau répertoire Amazon EFS (`aws-backup-restore_`*`datetime`*) à partir du répertoire racine pour contenir les éléments. La hiérarchie complète des éléments spécifiés est conservée dans le répertoire de récupération. Par exemple, si le répertoire A contient des sous-répertoires B, C et D, AWS Backup conserve la structure hiérarchique lorsque A, B, C et D sont restaurés. Vous pouvez effectuer une restauration Amazon EFS au niveau des éléments dans un système de fichiers existant ou sur un nouveau système de fichiers, mais chaque tentative de restauration crée un nouveau répertoire de récupération hors du répertoire racine pour contenir les fichiers restaurés. Si vous tentez plusieurs restaurations pour le même chemin d’accès, plusieurs répertoires contenant les éléments restaurés peuvent exister.

> **Note**
>
> Si vous ne conservez qu'une sauvegarde hebdomadaire, vous pouvez uniquement restaurer vers le statut du système de fichiers au moment où vous avez effectué cette sauvegarde. Vous ne pouvez pas restaurer vers des sauvegardes incrémentielles antérieures.

Utiliser la AWS Backup console pour restaurer un point de récupération Amazon EFS

Pour restaurer un système de fichiers Amazon EFS

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Votre coffre-fort de sauvegarde EFS reçoit la stratégie d'accès `Deny backup:StartRestoreJob` lors de sa création. Si vous restaurez votre coffre-fort de sauvegarde pour la première fois, vous devez modifier votre stratégie d'accès comme suit.
   a. Choisissez Coffres-forts de sauvegarde.
   b. Choisissez le coffre-fort de sauvegarde contenant le point de récupération que vous souhaitez restaurer.
   c. Faites défiler jusqu'à la Stratégie d'accès du coffre
   d. Le cas échéant, supprimez `backup:StartRestoreJob` de la `Statement`. Pour ce faire, choisissez Modifier, supprimez `backup:StartRestoreJob`, puis choisissez Enregistrer la stratégie.
3. Dans le volet de navigation, choisissez Ressources protégées et l'ID du système de fichiers EFS que vous voulez restaurer.
4. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID du système de fichiers sélectionné s'affiche. Pour restaurer un système de fichiers, dans le volet Sauvegardes, cliquez sur la case d'option en regard de l'ID du point de récupération du système de fichiers. Dans le coin supérieur droit du volet, choisissez Restaurer.
5. Spécifiez les paramètres de restauration de votre système de fichiers. Les paramètres de restauration que vous saisissez sont spécifiques au type de ressource sélectionné.

   Vous pouvez effectuer une Restauration complète, qui restaure l'ensemble du système de fichiers. Vous pouvez également restaurer des fichiers et des répertoires spécifiques à l'aide d'une Restauration au niveau des éléments.

- Choisissez l'option Restauration complète pour restaurer le système de fichiers dans son intégralité, y compris tous les dossiers et fichiers de niveau racine.
- Choisissez l'option de restauration au niveau des éléments pour restaurer un fichier ou un répertoire spécifique. Vous pouvez sélectionner et restaurer jusqu'à cinq éléments dans votre Amazon EFS.

  Pour restaurer un fichier ou un répertoire spécifique, vous devez spécifier le chemin relatif lié au point de montage. Par exemple, si le système de fichiers est monté sur **`/file1`** et que le chemin d'accès au fichier est `/user/home/myname/efs`, saisissez `user/home/myname/efs/file1`. Les chemins sont sensibles à la casse et ne peuvent pas contenir de caractères spéciaux, de caractères génériques et de chaînes regex.

  1. Dans la zone de texte Chemin d'accès de l'élément, saisissez le chemin d'accès de votre fichier ou dossier.
  2. Choisissez Ajouter un élément pour ajouter des fichiers ou des répertoires supplémentaires. Vous pouvez sélectionner et restaurer jusqu'à cinq éléments dans votre système de fichiers EFS.

6. Pour Emplacement de restauration

   - Choisissez Restaurer dans le répertoire du système de fichiers source si vous souhaitez restaurer dans le système de fichiers source.
   - Choisissez Restaurer dans un nouveau système de fichiers si vous souhaitez restaurer dans un autre système de fichiers.

7. Pour Type de système de fichiers

   - (Recommandé) Choisissez Régional si vous souhaitez restaurer votre système de fichiers dans plusieurs zones de AWS disponibilité.
   - Choisissez Unizone si vous souhaitez restaurer votre système de fichiers dans une seule zone de disponibilité. Ensuite, dans le menu déroulant Zone de disponibilité, choisissez la destination de votre restauration.

   Pour plus d'informations, consultez Gestion de classes de stockage Amazon EFS dans le Guide de l'utilisateur Amazon EFS.

8. Pour Performances

- Si vous avez choisi d'effectuer une restauration Régionale, choisissez Usage général (recommandé), ou E/S max..
- Si vous avez choisi d'effectuer une restauration Unizone, vous devez choisir Usage général (recommandé). Les restaurations Unizone ne prennent pas en charge E/S max.

9. Pour Activer le chiffrement

   - Choisissez Activer le chiffrement, si vous souhaitez chiffrer votre système de fichiers. Les identifiants et alias des clés KMS apparaissent dans la liste une fois qu'ils ont été créés à l'aide de la console AWS Key Management Service (AWS KMS).
   - Dans la zone de texte Clé KMS, choisissez la clé à utiliser dans la liste.

10. Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration.

    > **Note**
    >
    > Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle par défaut est créé pour vous avec les autorisations appropriées. Vous pouvez supprimer ce rôle par défaut ou le rendre inutilisable.

11. Choisissez Restore backup.

    Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

    > **Note**
    >
    > Si vous ne conservez qu'une sauvegarde hebdomadaire, vous pouvez uniquement restaurer vers le statut du système de fichiers au moment où vous avez effectué cette sauvegarde. Vous ne pouvez pas restaurer vers des sauvegardes incrémentielles antérieures.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon EFS

Utilisez `StartRestoreJob`. Lors de la restauration d'une instance Amazon EFS, vous pouvez restaurer un système de fichiers entier ou des fichiers ou répertoires spécifiques. Vous avez besoin des informations suivantes pour restaurer des ressources Amazon EFS :

- `file-system-id`— L'ID du système de fichiers Amazon EFS sauvegardé par AWS Backup. Renvoyé dans `GetRecoveryPointRestoreMetadata` Cela n'est pas obligatoire lors de la restauration d'un nouveau système de fichiers (cette valeur est ignorée si le paramètre `newFileSystem` est`True`).
- `Encrypted` : valeur booléenne qui, si la valeur est true, spécifie que le système de fichiers est chiffré. Si `KmsKeyId` est spécifié, `Encrypted` doit être défini sur `true`.
- `KmsKeyId`— Spécifie la AWS KMS clé utilisée pour chiffrer le système de fichiers restauré.
- `PerformanceMode` : spécifie le mode de débit du système de fichiers.
- `CreationToken` : valeur fournie par l'utilisateur qui garantit que le caractère unique (idempotence) de la demande.
- `newFileSystem` : valeur booléenne qui, si la valeur est true, spécifie que le point de récupération est restauré à un nouveau système de fichiers Amazon EFS.
- `ItemsToRestore` : tableau de cinq chaînes au maximum, chaque chaîne étant un chemin d'accès au fichier. Utilisez `ItemsToRestore` pour restaurer des fichiers ou des répertoires spécifiques, plutôt que la totalité du système de fichiers. Ce paramètre est facultatif.

Vous pouvez également inclure `aws:backup:request-id`.

Les restaurations One Zone peuvent être effectuées en incluant les paramètres suivants :

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Pour plus d'informations sur les valeurs de configuration Amazon EFS, consultez create-file-system.

Désactivation des sauvegardes automatiques dans Amazon EFS

Par défaut, Amazon EFS crée automatiquement des sauvegardes de données. Ces sauvegardes sont représentées sous forme de points de restauration dans AWS Backup. Les tentatives de suppression du point de récupération entraîneront un message d'erreur indiquant que les privilèges sont insuffisants pour effectuer l'action.

Il est recommandé de maintenir cette sauvegarde automatique active. Notamment en cas de suppression accidentelle de données, cette sauvegarde permet de restaurer le contenu du système de fichiers à la date du dernier point de récupération créé.

Dans le cas peu probable où vous souhaiteriez les désactiver, la stratégie d'accès doit être modifiée de `"Effect": "Deny"` à `"Effect": "Allow"`. Consultez le Guide de l'utilisateur Amazon EFS pour plus d'informations sur l'activation ou la désactivation des sauvegardes automatiques.

Restauration d'une table Amazon DynamoDB

Utiliser la AWS Backup console pour restaurer les points de restauration DynamoDB

Pour restaurer une table DynamoDB

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource DynamoDB que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Pour Paramètres, Nom nouvelle table, entrez un nouveau nom de table.
5. Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration.
6. Pour Paramètres de chiffrement :

   a. Si votre sauvegarde est gérée par DynamoDB (son ARN commence par) AWS Backup , chiffre votre table restaurée à l'`arn:aws:dynamo`dbaide d'une clé appartenant à DynamoDB. AWS

      Pour choisir une autre clé pour chiffrer votre table restaurée, vous pouvez soit utiliser l' AWS Backup StartRestoreJobopération, soit effectuer la restauration depuis la console DynamoDB.

   b. Si votre sauvegarde prend en charge AWS Backup la gestion complète (son ARN commence par`arn:aws:backup`), vous pouvez choisir l'une des options de chiffrement suivantes pour protéger votre table restaurée :

      - (Par défaut) Clé KMS appartenant à DynamoDB (sans frais supplémentaires pour le chiffrement)
      - Clé KMS gérée par DynamoDB (des frais KMS s'appliquent)
      - Clé KMS gérée par le client (des frais KMS s'appliquent)

Les clés « détenues par DynamoDB » et « gérées par DynamoDB » sont identiques aux clés « détenues par AWS » et « gérées par AWS », respectivement. Pour plus de précisions, consultez Fonctionnement du chiffrement au repos dans le Guide du développeur Amazon DynamoDB.

Pour plus d'informations sur AWS Backup la gestion complète, consultezSauvegarde DynamoDB avancée.

> **Note**
>
> Les instructions suivantes s'appliquent uniquement si vous restaurez une sauvegarde copiée ET que vous souhaitez chiffrer la table restaurée avec la même clé que celle que vous avez utilisée pour chiffrer votre table d'origine.
> Lors de la restauration d'une sauvegarde interrégionale, pour chiffrer votre table restaurée à l'aide de la même clé que celle que vous avez utilisée pour chiffrer votre table d'origine, votre clé doit être une clé multirégionale. AWS Les clés -owned et AWS-managed ne sont pas des clés multirégionales. Pour plus d'informations, consultez Clés multi-régions dans le Manuel du développeur AWS Key Management Service .
> Lorsque vous restaurez une sauvegarde entre comptes, pour chiffrer votre table restaurée à l'aide de la même clé que celle que vous avez utilisée pour chiffrer votre table d'origine, vous devez partager la clé de votre compte source avec votre compte de destination. AWS Les clés -owned et AWS-managed ne peuvent pas être partagées entre les comptes. Pour plus d'informations, consultez Autoriser des utilisateurs d'autres comptes à utiliser une clé KMS dans le Manuel du développeur AWS Key Management Service .

7. Choisissez Restore backup.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration DynamoDB

Utilisez `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations DynamoDB. Les métadonnées ne sont pas sensibles à la casse.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

Voici un exemple d'argument `restoreMetadata` pour une opération `StartRestoreJob` dans l'interface de ligne de commande :

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-
g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
--metadata
 'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,KMSMasterKeyId=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://cell-1.gamma.us-east-1.controller.cryo.aws.a2z.com
```

L'exemple précédent chiffre la table restaurée à l'aide d'une clé AWS appartenant à l'utilisateur. La partie des métadonnées de restauration qui spécifie le chiffrement à l'aide de la clé AWS-owned est :`\"encryptionType\":\"Default\",\"kmsMasterKeyArn\":\"Not Applicable\"`.

Pour chiffrer votre table restaurée à l'aide d'une clé AWS gérée, spécifiez les métadonnées de restauration suivantes :. `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"`

Pour chiffrer votre table restaurée à l'aide d'une clé gérée par le client, spécifiez les métadonnées de restauration suivantes : `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`.

Restauration d'une base de données RDS

La restauration d'une base de données Amazon RDS nécessite la spécification de plusieurs options de restauration. Pour plus d'informations sur ces options, consultez Sauvegarde et restauration d'une instance de base de données Amazon RDS dans le Guide de l'utilisateur Amazon RDS.

Utiliser la AWS Backup console pour restaurer les points de récupération Amazon RDS

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Amazon RDS que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Dans le volet Spécifications d'instance, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Moteur de base de données, Modèle de licence, Classe d'instance de base de données, Multi AZ et Type de stockage. Par exemple, si vous souhaitez une instance de base de données de secours, spécifiez Multi-AZ.
5. Dans le volet Paramètres, spécifiez un nom unique pour toutes les instances de base de données et les clusters que vous Compte AWS possédez dans la région actuelle. L'identifiant d'instance de base de données n'est pas sensible à la casse, mais il est stocké intégralement en minuscules, comme dans `mydbinstance`. Ce champ est obligatoire.
6. Dans le volet Network & Security, acceptez les valeurs par défaut ou spécifiez les options pour les paramètres du Virtual Private Cloud (VPC), du groupe de sous-réseaux, de l'accessibilité publique (généralement oui) et de la zone de disponibilité.
7. Dans le volet Options de base de données, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Port de base de données, Groupe de paramètres DB, Groupe d'options, Copier les balises dans les instantanés et Authentification IAM DB activée.
8. Dans le volet Chiffrement, utilisez les paramètres par défaut. Si l'instance de base de données source de l'instantané a été chiffrée, l'instance de base de données restaurée est également chiffrée. Ce chiffrement ne peut pas être supprimé.
9. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.

10. Dans le volet Maintenance, acceptez la valeur par défaut ou spécifiez la valeur du paramètre Mise à niveau automatique des versions mineures.
11. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
12. Une fois que tous les paramètres ont été spécifiés, choisissez Restaurer la sauvegarde.

    Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon RDS

Utilisez `StartRestoreJob`. Pour plus d'informations sur les métadonnées et les valeurs acceptées, consultez `RestoreDBInstanceFromDBSnapshot` dans la Référence d'API Amazon RDS. AWS Backup Accepte en outre les attributs informatifs suivants. Cependant, leur inclusion n'affectera pas la restauration :

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

Restauration d'un cluster Amazon Aurora

Utiliser la AWS Backup console pour restaurer les points de restauration Aurora

AWS Backup restaure votre cluster Aurora ; il ne crée ni n'attache d'instance Amazon RDS à votre cluster. Au cours des étapes suivantes, vous allez créer et associer une instance Amazon RDS à votre cluster Aurora restauré à l'aide de l'interface de ligne de commande.

Pour restaurer un cluster Aurora, vous devez spécifier plusieurs options de restauration. Pour plus d'informations sur ces options, consultez Présentation de la sauvegarde et de la restauration d'un cluster de bases de données Aurora dans le Guide de l'utilisateur Amazon Aurora. Les spécifications relatives aux options de restauration se trouvent dans le guide de l'API pour `RestoreDBClusterFromSnapshot`.

Pour restaurer un cluster Amazon Aurora

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.

2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Aurora que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Dans le volet Spécifications d'instance, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Moteur de base de données, Version du moteur de base de données et Type de capacité.

   > **Note**
   >
   > Si le type de capacité Sans serveur est sélectionné, un volet Paramètres de capacité apparaît. Spécifiez les valeurs des paramètres Unité de capacité Aurora minimale et Unité de capacité Aurora maximale ou choisissez des options différentes dans la section Configuration de dimensionnement supplémentaire.

5. Dans le volet Paramètres, spécifiez un nom unique pour toutes les instances de cluster de base de données que vous Compte AWS possédez dans la région actuelle.
6. Dans le volet Réseau et sécurité, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Cloud privé virtuel (VPC), Groupe de sous-réseaux et Zone de disponibilité.
7. Dans le volet Options de base de données, acceptez les valeurs par défaut ou spécifiez les valeurs des paramètres Port de base de données, Groupe de paramètres de cluster DB et Authentification IAM DB activée.
8. Dans le volet Sauvegarde, acceptez la valeur par défaut ou spécifiez la valeur du paramètre Copier les balises dans les instantanés.
9. Dans le volet Retour sur trace, acceptez la valeur par défaut ou spécifiez les valeurs des paramètres Activer le retour sur trace ou Désactiver le retour sur trace.
10. Dans le volet Chiffrement, acceptez la valeur par défaut ou spécifiez les valeurs des paramètres Activer le chiffrement ou Désactiver le chiffrement.
11. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.
12. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
13. Après avoir spécifié tous vos paramètres, choisissez Restaurer la sauvegarde.

Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

14. Une fois votre restauration terminée, attachez votre cluster Aurora restauré à une instance Amazon RDS.

    À l'aide de la AWS CLI :

    - Pour Linux, macOS ou Unix :

    ```
    aws rds create-db-instance --db-instance-identifier sample-instance \
                  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
    instance-class db.r4.large
    ```

    - Pour Windows :

    ```
    aws rds create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
    instance-class db.r4.large
    ```

Consultez la section Sauvegardes et point-in-time restaurations continues (PITR) pour obtenir des informations sur les sauvegardes continues et la restauration à un moment donné.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Aurora

Utilisez `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations Aurora :

```
List<String> availabilityZones;
Long backtrackWindow;
Boolean copyTagsToSnapshot;
String databaseName;
String dbClusterIdentifier;
String dbClusterParameterGroupName;
String dbSubnetGroupName;
List<String> enableCloudwatchLogsExports;
Boolean enableIAMDatabaseAuthentication;
String engine;
String engineMode;
```

```
String engineVersion;
String kmsKeyId;
Integer port;
String optionGroupName;
ScalingConfiguration scalingConfiguration;
List<String> vpcSecurityGroupIds;
```

Exemple :

```
"restoreMetadata":"{\"EngineVersion\":\"5.6.10a\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7\",\"EngineMode\":
\"serverless\",\"AvailabilityZones\":\"[\\\"us-east-1b\\\",\\\"us-east-1e\\\",\\
\"us-east-1c\\\"]\",\"Port\":\"3306\",\"DatabaseName\":\"\",\"DBSubnetGroupName\":
\"default-vpc-05a3b07cf6e193e1g\",\"VpcSecurityGroupIds\":\"[\\\"sg-012d52c68c6e88f00\
\\"]\",\"ScalingConfiguration\":\"{\\\"MinCapacity\\\":2,\\\"MaxCapacity\\\":64,
\\\"AutoPause\\\":true,\\\"SecondsUntilAutoPause\\\":300,\\\"TimeoutAction\\\":
\\\"RollbackCapacityChange\\\"}\",\"EnableIAMDatabaseAuthentication\":\"false\",
\"DBClusterParameterGroupName\":\"default.aurora5.6\",\"CopyTagsToSnapshot\":\"true\",
\"Engine\":\"aurora\",\"EnableCloudwatchLogsExports\":\"[]\"}"
```

Restauration d'une instance Amazon EC2

Lorsque vous restaurez une instance EC2, vous AWS Backup créez une Amazon Machine Image (AMI), une instance, le volume racine Amazon EBS, les volumes de données Amazon EBS (si la ressource protégée contenait des volumes de données) et les instantanés Amazon EBS. Vous pouvez personnaliser certains paramètres d'instance à l'aide de la AWS Backup console, ou un plus grand nombre de paramètres à l'aide du AWS CLI ou d'un AWS SDK.

Les considérations suivantes s'appliquent à la restauration des instances EC2 :

- AWS Backup configure l'instance restaurée pour utiliser la même paire de clés que celle utilisée à l'origine par la ressource protégée. Vous ne pouvez pas spécifier une paire de clés différente pour l'instance restaurée pendant le processus de restauration.
- AWS Backup ne sauvegarde ni ne restaure les données utilisateur utilisées lors du lancement d'une instance Amazon EC2.
- Lors de la configuration de l'instance restaurée, vous pouvez choisir d'utiliser le même profil d'instance que celui utilisé initialement par la ressource protégée ou de le lancer sans profil d'instance. Cela permet d'éviter une escalade possible des privilèges. Vous pouvez mettre à jour le profil d'instance pour l'instance restaurée à l'aide de la console Amazon EC2.

Si vous utilisez le profil d'instance d'origine, vous devez accorder AWS Backup les autorisations suivantes, l'ARN de la ressource étant l'ARN du rôle IAM associé au profil d'instance.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

- Lors d'une restauration, tous les quotas et restrictions de configuration Amazon EC2 s'appliquent.
- Si le coffre-fort contenant vos points de récupération Amazon EC2 est verrouillé, consultez Considérations supplémentaires en matière de sécurité pour plus d'informations.

Utiliser la AWS Backup console pour restaurer les points de restauration Amazon EC2

vous pouvez restaurer une instance Amazon EC2 complète à partir d'un point de récupération unique, y compris le volume racine, les volumes de données et certains paramètres de configuration de l'instance, tels que le type d'instance et la paire de clés.

Pour restaurer les ressources Amazon EC2 à l'aide de la console AWS Backup

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées, puis choisissez l'ID de la ressource Amazon EC2 pour ouvrir la page de détails de la ressource.
3. Dans le volet Points de restauration, cliquez sur le bouton radio à côté de l'ID du point de récupération à restaurer. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Dans le volet Paramètres réseau, nous utilisons les paramètres de l'instance protégée pour sélectionner les valeurs par défaut pour le type d'instance, le VPC, le sous-réseau, le groupe de sécurité et le rôle IAM de l'instance. Vous pouvez utiliser ces valeurs par défaut ou les modifier selon vos besoins.
5. Dans le volet Restaurer le rôle, utilisez le rôle par défaut ou choisissez un rôle IAM pour spécifier un rôle IAM qui AWS Backup autorise la restauration de la sauvegarde.
6. Dans le volet Balises de ressources protégées, nous sélectionnons par défaut Copier les balises de la ressource protégée vers la ressource restaurée. Si vous ne souhaitez pas copier ces balises, désactivez la case à cocher.

7. Dans le volet Paramètres avancés, acceptez les valeurs par défaut des paramètres de l'instance ou modifiez-les selon vos besoins. Pour plus d'informations sur ces paramètres, choisissez Info pour le paramètre afin d'ouvrir son volet d'aide.
8. Lorsque vous avez terminé de configurer l'instance, choisissez Restaurer la sauvegarde.

Restaurez Amazon EC2 avec AWS CLI

Dans l'interface de ligne de commande `start-restore-job`, vous pouvez effectuer une restauration avec un maximum de 32 paramètres (y compris certains paramètres qui ne sont pas personnalisables via la AWS Backup console).

Voici une liste des métadonnées acceptées que vous pouvez transmettre pour restaurer un point de récupération Amazon EC2.

```
InstanceType
KeyName
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
RamdiskId
KernelId
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
```

```
aws:backup:request-id
```

AWS Backup accepte les attributs suivants fournis uniquement à titre informatif. Cependant, leur inclusion n'affectera pas la restauration :

```
vpcId
```

Vous pouvez également restaurer une instance Amazon EC2 sans inclure de paramètres stockés. Cette option est disponible dans l'onglet Ressources protégées de la console AWS Backup .

Restauration d'un volume Storage Gateway

Si vous restaurez un instantané de AWS Storage Gateway volume, vous pouvez choisir de le restaurer en tant que volume Storage Gateway ou en tant que volume Amazon EBS. Cela est dû au fait qu'il AWS Backup s'intègre aux deux services et que tout instantané de Storage Gateway peut être restauré sur un volume Storage Gateway ou sur un volume Amazon EBS.

Restaurez Storage Gateway via la AWS Backup console

Pour restaurer un volume Storage Gateway

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées, puis l'ID de ressource Storage Gateway que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Spécifiez les paramètres de restauration de votre ressource. Les paramètres de restauration que vous saisissez sont spécifiques au type de ressource sélectionné.

   Pour Type de ressource, choisissez la AWS ressource à créer lors de la restauration de cette sauvegarde.
5. Si vous choisissez Volume Storage Gateway, choisissez une Passerelle accessible. Choisissez également votre Nom de cible iSCSI.

   1. Pour les passerelles « Volume stocké », choisissez un ID de disque.

2. Pour les passerelles « Volume mis en cache », choisissez une capacité au moins égale à votre ressource protégée.

   Si vous choisissez Volume EBS, indiquez les valeurs Type de volume, Taille (Gio), et choisissez une Zone de disponibilité.

6. Pour le rôle de restauration, choisissez le rôle IAM qui AWS Backup assumera cette restauration.

   > **Note**
   >
   > Si le rôle AWS Backup par défaut n'est pas présent dans votre compte, un rôle par défaut est créé pour vous avec les autorisations appropriées. Vous pouvez supprimer ce rôle par défaut ou le rendre inutilisable.

7. Choisissez Restore backup.

   Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.

Restaurez Storage Gateway avec AWS CLI

Dans l'interface de ligne de commande, `start-restore-job` vous permet de restaurer un volume Storage Gateway.

La liste suivante contient les métadonnées acceptées.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and Région AWS.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Restauration d'une table Amazon Timestream

Lorsque vous restaurez une table Amazon Timestream, plusieurs options doivent être configurées, notamment le nom de la nouvelle table, la base de données de destination, vos préférences

d'allocation de stockage (mémoire et stockage magnétique) et le rôle que vous utiliserez pour terminer la tâche de restauration. Vous pouvez également choisir un compartiment Amazon S3 dans lequel stocker les journaux d'erreurs. Les écritures sur stockage magnétique étant asynchrones, vous souhaiterez peut-être journaliser les erreurs.

Le stockage de données Timestream comporte deux niveaux : un stockage en mémoire et un stockage magnétique. Le stockage en mémoire est requis, mais vous avez la possibilité de transférer votre table restaurée vers un stockage magnétique une fois la durée de mémoire spécifiée écoulée. La mémoire est optimisée pour les écritures de données à haut débit et les point-in-time requêtes rapides. Le stockage magnétique est optimisé pour les écritures de données à faible débit et arrivée tardive, le stockage de données à long terme et les requêtes analytiques rapides.

Lorsque vous restaurez une table Timestream, vous déterminez combien de temps vous souhaitez que la table reste dans chaque niveau de stockage. À l'aide de la console ou de l'API, vous pouvez définir la durée de stockage pour les deux. Notez que le stockage est linéaire et séquentiel. Timestream stockera d'abord votre table restaurée dans un stockage en mémoire, puis la transmettra automatiquement en stockage magnétique lorsque le temps de stockage en mémoire sera atteint.

> **Note**
>
> La période de rétention de la mémoire magnétique doit être égale ou supérieure à la période de rétention initiale (indiquée en haut à droite de la console), sinon les données seront perdues.

Exemple : vous définissez l'allocation de stockage en mémoire pour conserver les données pendant une semaine et l'allocation de mémoire magnétique pour conserver les mêmes données pendant un an. Lorsque les données du stockage en mémoire datent d'une semaine, elles sont automatiquement déplacées vers le stockage magnétique. Elles sont ensuite conservées dans le stockage magnétique pendant un an. À la fin de cette période, elles sont supprimées de Timestream et d' AWS Backup.

Pour restaurer une table Amazon Timestream à l'aide de la console AWS Backup

Vous pouvez restaurer les tables Timestream dans la AWS Backup console qui ont été créées par. AWS Backup

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Amazon Timestream que vous voulez restaurer.

3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Spécifiez les nouveaux paramètres de configuration de votre table, notamment :
   a. Nom de la nouvelle table, composé de 2 à 256 caractères (lettres, chiffres, tirets, points et traits de soulignement).
   b. Base de données de destination, choisie dans le menu déroulant.
5. Allocation de stockage : définissez la durée pendant laquelle la table restaurée restera pour la première fois dans le stockage en mémoire et définissez la durée pendant laquelle la table restaurée restera ensuite dans le stockage magnétique. Le stockage en mémoire peut être défini en heures, jours, semaines ou mois. Le stockage magnétique peut être défini en jours, semaines, mois ou années.
6. (Facultatif) Activer les écritures de stockage magnétique : vous avez la possibilité d'autoriser les écritures sur stockage magnétique. Lorsque cette option est cochée, les données à arrivée tardive, c'est-à-dire les données horodatées en dehors de la période de rétention de la mémoire, seront écrites directement dans le stockage magnétique.
7. (Facultatif) Emplacement des journaux d'erreurs Amazon S3 : vous pouvez spécifier un emplacement S3 dans lequel vos journaux d'erreurs seront stockés. Parcourez vos fichiers S3 ou copiez-collez le chemin du fichier S3.

   > **Note**
   >
   > Si vous choisissez de spécifier l'emplacement du journal des erreurs S3, le rôle que vous utilisez pour cette restauration doit être autorisé à écrire dans un compartiment S3 ou doit contenir une politique avec cette autorisation.

8. Choisissez le rôle IAM à transmettre pour effectuer des restaurations. Vous pouvez utiliser le rôle IAM par défaut ou en spécifier un autre.
9. Cliquez sur Restaurer la sauvegarde.

Vos tâches de restauration seront visibles sous Ressources protégées. Vous pouvez consulter le statut actuel de votre tâche de restauration en cliquant sur le bouton d'actualisation ou sur CTRL-R.

Pour restaurer une table Amazon Timestream à l'aide d'une API, d'une interface de ligne de commande ou d'un kit SDK

Utilisez `StartRestoreJob` pour restaurer une table Timestream via l'API.

Pour restaurer un flux temporel à l'aide de AWS CLI, utilisez l'opération `start-restore-job.` et spécifiez les métadonnées suivantes :

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

Voici un exemple de modèle :

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-
f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
 'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStor
\":true,\"MagneticStoreRejectedDataLocation\":{\"S3Configuration\":{\"BucketName\":
\"bucketname\",\"EncryptionOption\":\"SSE_S3\"}}}"' \
--region us-west-2 \
--endpoint-url url
```

Vous pouvez également utiliser `DescribeRestoreJob` pour vous aider à obtenir des informations de restauration.

Dans le AWS CLI, utilisez l'opération `describe-restore-job` et utilisez les métadonnées suivantes :

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
```

```
EnableMagneticStoreWrites?: boolean;
```

Voici un exemple de modèle :

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Restauration d'un cluster Amazon Redshift

Vous pouvez restaurer des instantanés automatisés et manuels dans la AWS Backup console ou via la CLI.

Lorsque vous restaurez un cluster Amazon Redshift, les paramètres du cluster d'origine sont saisis par défaut dans la console. Vous pouvez définir différents paramètres pour les configurations ci-dessous. Lors de la restauration d'une table, vous devez spécifier les bases de données source et cible. Pour plus d'informations sur ces configurations, consultez Restauration d'un cluster à partir d'un instantané dans le Guide de gestion Amazon Redshift.

- Table unique ou cluster : vous pouvez choisir de restaurer un cluster entier ou une seule table. Si vous choisissez de restaurer une seule table, la base de données source, le schéma source et le nom de la table source sont nécessaires, ainsi que le cluster cible, le schéma et le nouveau nom de table.
- Type de nœud : chaque cluster Amazon Redshift est composé d'un nœud principal et d'au moins un nœud de calcul. Lorsque vous restaurez un cluster, vous devez spécifier le type de nœud qui répond à vos exigences en matière de processeur, de RAM, de capacité de stockage et de type de lecteur.
- Nombre de nœuds : lorsque vous restaurez un cluster, vous devez spécifier le nombre de nœuds nécessaires.
- Récapitulatif de configuration
- Autorisations du cluster

Pour restaurer un cluster ou une table Amazon Redshift à l'aide de la console AWS Backup

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.

2. Dans le volet de navigation, choisissez Paramètres et l'ID de ressource Amazon Redshift que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Points de récupération, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Options de restauration
    a. Restaurez un cluster à partir d'un instantané, ou
    b. Restaurez une table unique dans un instantané sur un nouveau cluster. Si vous choisissez cette option, vous devez configurer les éléments suivants :
        i. Activez ou désactivez les noms sensibles à la casse.
        ii. Entrez les valeurs de la table source, y compris la base de données, le schéma et la table. Les informations de la table source se trouvent dans la console Amazon Redshift.
        iii. Entrez les valeurs de la table cible, y compris la base de données, le schéma et le nouveau nom de la table.
5. Spécifiez les nouveaux paramètres de configuration de votre cluster.
    a. Pour la restauration du cluster : choisissez l'identifiant du cluster, le type de nœud et le nombre de nœuds.
    b. Spécifiez la zone de disponibilité et les fenêtres de maintenance.
    c. Vous pouvez associer des rôles supplémentaires en cliquant sur Associer des rôles IAM.
6. Facultatif : configurations supplémentaires :
    a. L'option Utiliser la valeur par défaut est activée par défaut.
    b. Utilisez les menus déroulants pour sélectionner les paramètres de mise en réseau et de sécurité, les groupes de sécurité VPC, le groupe de sous-réseaux du cluster et la zone de disponibilité.
    c. Activez ou désactivez Routage VPC amélioré.
    d. Déterminez si vous souhaitez rendre le point de terminaison de votre cluster accessible au public. Si tel est le cas, les instances et les appareils extérieurs au VPC peuvent se connecter à votre base de données via le point de terminaison du cluster. Si cette option est activée, entrez l'adresse IP élastique.
7. Facultatif : configuration de la base de données. Vous pouvez choisir de saisir

   a. Port de base de données (en tapant dans le champ de texte)
   b. Groupes de paramètres
8. Maintenance : vous pouvez choisir
   a. Fenêtre de maintenance
   b. Suivi de la maintenance, que ce soit en cours, finie ou en aperçu. Cela contrôle la version du cluster qui est appliquée au cours d'une fenêtre de maintenance.
9. L'instantané automatique est défini par défaut.
   a. Période de rétention de l'instantané automatique. La période de rétention doit être comprise entre 0 et 35 jours. Choisissez 0 pour ne pas créer d'instantanés automatiques.
   b. La période de rétention manuelle des instantanés est de 1 à 3 653 jours.
   c. Il existe une case à cocher facultative pour la relocalisation du cluster. Si cette case est cochée, cela permet de relocaliser votre cluster dans une autre zone de disponibilité. Une fois que vous avez activé la relocalisation, vous pouvez utiliser le point de terminaison d'un VPC.
10. Surveillance : après la restauration d'un cluster, vous pouvez configurer la surveillance via CloudWatch Amazon Redshift.
11. Choisissez le rôle IAM à transmettre pour effectuer des restaurations. Vous pouvez utiliser le rôle par défaut ou en spécifier un autre.

Vos tâches de restauration seront visibles sous Tâches. Vous pouvez consulter le statut actuel de votre tâche de restauration en cliquant sur le bouton d'actualisation ou sur CTRL-R.

Restauration d’un cluster Amazon Redshift à l’aide d’une API, d’une interface de ligne de commande ou d’un kit SDK

Utilisez `StartRestoreJob` pour restaurer un cluster Amazon Redshift.

Pour restaurer un Amazon Redshift à l'aide de AWS CLI, utilisez la commande `start-restore-job` et spécifiez les métadonnées suivantes :

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
AquaConfigurationStatus // optional string
```

```
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
IamRoles // optional array of strings
KmsKeyId // optional string
MaintenanceTrackName // optional string
ManageMasterPassword // optional Boolean
ManualSnapshotRetentionPeriod // optional integer
MasterPasswordSecretKmsKeyId // optional string
NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
VpcSecurityGroupIds // optional array of strings
RestoreType // CLUSTER_RESTORE  or TABLE_RESTORE
```

Pour plus d'informations, consultez RestoreFromClusterSnapshot dans la Référence de l'API Amazon Redshift et restore-from-cluster-snapshot dans le Guide de l'AWS CLI .

Voici un exemple de modèle :

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region Région AWS
-\-endpoint-url URL
```

Voici un exemple :

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-
cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-
restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \
```

Vous pouvez également utiliser `DescribeRestoreJob` pour vous aider à obtenir des informations de restauration.

Dans le AWS CLI, utilisez l'opération `describe-restore-job` et utilisez les métadonnées suivantes :

```
Region
```

Voici un exemple de modèle :

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region Région AWS
```

Voici un exemple :

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

Restauration d'une base de données SAP HANA sur une instance Amazon EC2

Les bases de données SAP HANA sur les instances EC2 peuvent être restaurées à l'aide de la AWS Backup console, de l'API ou de. AWS CLI

Rubriques

- Restaurez une base de données d'instance SAP HANA sur Amazon EC2 à l'aide de la console AWS Backup

- StartRestoreJob API pour SAP HANA sur EC2
- Interface de ligne de commande pour SAP HANA sur EC2
- Résolution des problèmes

Restaurez une base de données d'instance SAP HANA sur Amazon EC2 à l'aide de la console AWS Backup

Notez que les tâches de sauvegarde et de restauration impliquant la même base de données ne peuvent pas être exécutées simultanément. Lorsqu'une tâche de restauration de base de données SAP HANA est en cours, les tentatives de sauvegarde de la même base de données peuvent entraîner le message d'erreur suivant : « Impossible de sauvegarder la base de données tant qu'elle est arrêtée ».

1. Accédez à la AWS Backup console à l'aide des informations d'identification fournies dans les prérequis.
2. Dans le menu déroulant Emplacement de restauration cible, choisissez une base de données à remplacer par le point de récupération que vous utilisez pour la restauration (notez que l'instance hébergeant la base de données cible de restauration doit également disposer des autorisations des conditions préalables).

   > **Important**
   >
   > Les restaurations de bases de données SAP HANA sont destructrices. La restauration d'une base de données remplacera la base de données à l'emplacement de restauration cible spécifié.

3. Suivez cette étape uniquement si vous effectuez une restauration de copie du système ; sinon, passez à l'étape 4.

   Les restaurations de copies du système sont des tâches de restauration qui restaurent vers une base de données cible différente de la base de données source qui a généré le point de récupération. Pour les restaurations de copies du système, notez la commande `aws ssm-sap put-resource-permission` qui vous est fournie sur la console. Cette commande doit être copiée, collée et exécutée sur la machine qui a rempli les conditions préalables. Lorsque vous exécutez la commande, utilisez les informations d'identification du rôle dans les conditions préalables où vous configurez les autorisations requises pour l'enregistrement des applications.

```
// Example command
aws ssm-sap put-resource-permission \
--region us-east-1 \
--action-type RESTORE \
--source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
--resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
```

4. Une fois que vous avez choisi l'emplacement de restauration, vous pouvez voir l'ID de ressource, le Nom de l'application, le Type de base de données et l'Instance EC2 de la base de données cible.
5. Facultatif Vous pouvez ouvrir les Paramètres de restauration avancés pour modifier l'option de restauration de votre catalogue. La sélection par défaut consiste à restaurer le dernier catalogue à partir d' AWS Backup.
6. Cliquez sur Restaurer la sauvegarde.
7. L'emplacement cible sera remplacé lors de la restauration (« restauration destructive »). Vous devez donc confirmer que vous l'autorisez dans la boîte de dialogue contextuelle suivante.

    a. Pour continuer, vous devez comprendre que la base de données existante sera remplacée par celle que vous restaurez.

    b. Une fois que cela est compris, vous devez reconnaître que les données existantes seront remplacées. Pour confirmer cela et continuer, tapez remplacer dans le champ de saisie de texte.
8. Cliquez sur Restaurer la sauvegarde.

Si la procédure est réussie, une bannière bleue s'affiche en haut de la console. Cela signifie que la tâche de restauration est en cours. Vous serez automatiquement redirigé vers la page Tâches où votre tâche de restauration apparaîtra dans la liste des tâches de restauration. Cette tâche la plus récente aura le statut `Pending`. Vous pouvez rechercher, puis cliquer sur l'ID de la tâche de restauration pour voir les détails de chaque tâche de restauration. Vous pouvez actualiser la liste des tâches de restauration en cliquant sur le bouton d'actualisation pour afficher les modifications apportées au statut des tâches de restauration.

StartRestoreJob API pour SAP HANA sur EC2

Cette action récupère la ressource enregistrée identifiée par un Amazon Resource Name (ARN).

Syntaxe de la demande

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Paramètres de demande URI : la demande n'utilise pas de paramètres URI.

Corps de la requête : la demande accepte les données suivantes au format JSON :

IdempotencyTokenChaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques. `StartRestoreJob` Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Metadonnées

Un ensemble de paires clé-valeur de métadonnées. Contient des informations, telles que le nom de la ressource, nécessaires pour restaurer un point de récupération. Vous pouvez obtenir les métadonnées de configuration relatives à une ressource au moment de sa sauvegarde en appelant `GetRecoveryPointRestoreMetadata`. Cependant, des valeurs autres que celles fournies par `GetRecoveryPointRestoreMetadata` peuvent être nécessaires pour restaurer une ressource. Par exemple, vous devrez peut-être fournir un nouveau nom de ressource si l'original existe déjà.

Vous devez inclure des métadonnées spécifiques pour restaurer une instance SAP HANA sur Amazon EC2. Consultez les StartRestoreJob métadonnées des éléments spécifiques à SAP HANA.

Pour récupérer les métadonnées pertinentes, vous pouvez utiliser l'appel `GetRecoveryPointRestoreMetadata`.

Exemple de point de récupération de base de données SAP HANA standard :

```
"RestoreMetadata": {
```

```
        "BackupSize": "1660948480",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "SYSTEM",
        "HanaBackupEndTime": "1674838362",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
        "HanaBackupStartTime": "1674838349",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/DATABASENAME",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
    }
```

Exemple de point de récupération d'une base de données SAP HANA en continu :

```
"RestoreMetadata": {
        "AvailableRestoreBases":
 "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
        "BackupSize": "1711284224",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "TENANT",
        "EarliestRestorablePitrTimestamp": "1674764799789",
        "HanaBackupEndTime": "1668032687",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_HDB_FULL",
        "HanaBackupStartTime": "1668032667",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "LatestRestorablePitrTimestamp": "1674850299789",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
    }
```

Interface de ligne de commande pour SAP HANA sur EC2

La commande `start-restore-job` récupère la ressource enregistrée identifiée par un Amazon Resource Name (ARN). L'interface de ligne de commande suivra les directives de l'API ci-dessus.

Résumé :

```
start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
[--no-paginate]
[--output value]
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]
[--ca-bundle value]
[--cli-read-timeout value]
[--cli-connect-timeout value]
```

Options

`--recovery-point-arn` (chaîne) est une chaîne sous la forme d'un Amazon Resource Number (ARN) qui identifie de manière unique un point de récupération ; par exemple `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

`--metadata` (map) : un ensemble de paires clé-valeur de métadonnées. Contient des informations, telles que le nom de la ressource, nécessaires pour restaurer un point de récupération. Vous pouvez obtenir les métadonnées de configuration relatives à une ressource au moment de sa sauvegarde en appelant `GetRecoveryPointRestoreMetadata`. Cependant, des valeurs autres que celles fournies par `GetRecoveryPointRestoreMetadata` peuvent être nécessaires pour restaurer une ressource. Vous devez spécifier des métadonnées spécifiques pour restaurer une instance SAP HANA sur Amazon EC2 :

- `aws:backup:request-id` : il s'agit de n'importe quelle chaîne UUID utilisée pour l'idempotence. Cela ne modifie en rien votre expérience de restauration.
- `aws:backup:TargetDatabaseArn` : spécifiez la base de données dans laquelle vous souhaitez effectuer la restauration. Il s'agit de l'ARN de base de données SAP HANA sur Amazon EC2.
- `CatalogRestoreOption` : spécifiez d'où vous souhaitez restaurer votre catalogue. Il doit s'agir de `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP` ou `CATALOG_FROM_LOCAL_PATH`.
- `LocalCatalogPath`: Si la valeur CatalogRestoreOption des métadonnées est`CATALOG_FROM_LOCAL_PATH`, spécifiez le chemin d'accès au catalogue local sur votre instance EC2. Il doit s'agir d'un chemin de fichier valide dans votre instance EC2.
- `RecoveryType` : actuellement, les types de récupération `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY` et `MOST_RECENT_TIME_RECOVERY` sont pris en charge.

clé = (chaîne) ; valeur = (chaîne). Syntaxe raccourcie :

```
KeyName1=string,KeyName2=string
```

Syntaxe JSON :

```
{"string": "string"
  ...}
```

`--idempotency-token` est une chaîne choisie par l'utilisateur que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartRestoreJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

`--resource-type` est une chaîne qui lance une tâche de restauration d'un point de récupération pour l'une des ressources suivantes : `SAP HANA on Amazon EC2` pour SAP HANA sur Amazon EC2. Facultatif Les ressources SAP HANA peuvent être balisées à l'aide de la commande `aws ssm-sap tag-resource`

Sortie : `RestoreJobId` est une chaîne identifiant de manière unique la tâche qui restaure un point de récupération.

Résolution des problèmes

Si l'une des erreurs suivantes se produit lors d'une tentative de sauvegarde, consultez la résolution associée.

- Erreur : erreur du journal de sauvegarde continue

  Afin de conserver les points de récupération pour les sauvegardes continues, des journaux sont créés par SAP HANA pour toutes les modifications. Lorsque les journaux ne sont pas disponibles, le statut de chacun de ces points de récupération continue est `STOPPED`. Le dernier point de récupération viable pouvant être utilisé pour la restauration est celui dont le statut est `AVAILABLE`. Si les données du journal sont manquantes pour la période entre les points de récupération dotés d'un statut `STOPPED` et les points dotés d'un statut `AVAILABLE`, il n'est pas possible de garantir la réussite de la restauration. Si vous entrez une date et une heure comprises dans cette plage, il AWS Backup tentera de faire la sauvegarde, mais utilisera l'heure de restauration disponible la plus proche. Cette erreur sera affichée par le message `“Encountered an issue with log backups. Please check SAP HANA for details."`

  Résolution : dans la console, l'heure de restauration la plus récente, basée sur les journaux, est affichée. Vous pouvez saisir une heure plus récente que l'heure indiquée. Toutefois, si les données pour cette période ne sont pas disponibles dans les journaux, AWS Backup nous utiliserons la date de restauration la plus récente.

- Erreur : `Internal error`

  Solution : créez un dossier d'assistance depuis votre console ou contactez votre interlocuteur en AWS Support fournissant les détails de votre restauration, tels que l'identifiant de la tâche de restauration.

- Erreur : `The provided role arn:aws:iam::`*`ACCOUNT_ID`*`:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  Résolution : assurez-vous que le rôle assumé lors de l'appel de restauration dispose des autorisations requises pour créer des rôles liés au service.

- Erreur : `User: arn:aws:sts::`*`ACCOUNT_ID`*`:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:`*`ACCOUNT_ID`*`:...`

  Résolution : assurez-vous que le rôle assumé lors de l'appel des autorisations de restauration décrites dans les conditions préalables est correctement entré.

- Erreur : `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

Résolution : assurez-vous que l'agent Backint a été correctement installé. Vérifiez tous les prérequis, en particulier Installer AWS BackInt l'agent et AWS Systems Manager pour SAP sur votre serveur d'applications SAP, puis réessayez d'installer l' BackInt agent.

- Erreur : `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  Résolution : la tâche de restauration a été annulée par le flux de travail du service. Réessayez la tâche de restauration.

- Erreur : `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

  Résolution : une instabilité transitoire du réseau se produit sur l'instance. Réessayez la restauration. Si ce problème se produit régulièrement, essayez d'ajouter `ForceRetry: "true"` au fichier de configuration de l'agent à l'adresse `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`.

Pour tout autre problème lié à l'agent AWS Backint, reportez-vous à la section Résoudre les problèmes liés à AWS l'agent Backint pour SAP HANA.

Restauration d'un cluster DocumentDB

Utiliser la AWS Backup console pour restaurer les points de restauration Amazon DocumentDB

Pour restaurer un cluster Amazon DocumentDB, vous devez spécifier plusieurs options de restauration. Pour plus d'informations sur ces options, consultez Restauration à partir d'un instantané de cluster dans le Guide du développeur Amazon DocumentDB.

Pour restaurer un cluster Amazon DocumentDB

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Amazon DocumentDB que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d’option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.

4. Dans le volet Configuration, acceptez les valeurs par défaut ou spécifiez les options pour Identifiant du cluster, Version du moteur, Classe d'instance et Nombre d'instances.

   - REMARQUE : si le VPC par défaut n'existe pas lors de la restauration, vous devez spécifier un sous-réseau dans un autre VPC.

5. Dans le volet Réseau et sécurité, « Aucune préférence » s'affiche.
6. Dans le ncryption-at-rest volet E, acceptez la valeur par défaut ou spécifiez les options pour les paramètres Activer le chiffrement ou Désactiver le chiffrement.
7. Dans le volet Options de cluster, saisissez le Port et choisissez le Groupe de paramètres de cluster.
8. Dans le volet Backup, choisissez la sauvegarde continue pour la point-in-time restauration (PITR), les sauvegardes par snapshot planifiées, ou les deux.
9. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.
10. Dans le volet Maintenance, spécifiez une fenêtre de maintenance ou choisissez Aucune préférence.
11. Dans le volet Balises, vous pouvez choisir Ajouter une balise.
12. Dans le volet Protection contre la suppression, vous pouvez choisir Activer la protection contre la suppression.
13. Après avoir spécifié tous vos paramètres, choisissez Restaurer la sauvegarde.

    Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.
14. Une fois votre restauration terminée, attachez votre cluster Amazon DocumentDB restauré à une instance Amazon RDS.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Amazon DocumentDB

Restaurez d’abord votre cluster. Utilisez `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon DocumentDB :

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
```

```
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

Ensuite, connectez votre cluster Amazon DocumentDB restauré à une instance Amazon RDS à l'aide de `create-db-instance`.

- Pour Linux, macOS ou Unix :

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Pour Windows :

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Restauration d'un cluster Neptune

Utiliser la AWS Backup console pour restaurer les points de récupération Amazon Neptune

La restauration d'une base de données Amazon Neptune nécessite la spécification de plusieurs options de restauration. Pour plus d'informations sur ces options, consultez Restauration à partir d'un instantané de cluster de bases de données dans le Guide du développeur Amazon DocumentDB.

Pour restaurer une base de données Neptune

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation, choisissez Ressources protégées et l'ID de ressource Neptune que vous voulez restaurer.
3. Sur la page Détails de la ressource, une liste des points de récupération pour l'ID de ressource sélectionné s'affiche. Pour restaurer une ressource, dans le volet Sauvegardes, cliquez sur le bouton d'option en regard de l'ID du point de récupération de la ressource. Dans le coin supérieur droit du volet, choisissez Restaurer.
4. Dans le volet Spécifications d'instance, acceptez les valeurs par défaut ou spécifiez le Moteur de base de données et la Version.
5. Dans le volet Paramètres, spécifiez un nom unique pour toutes les instances de cluster de base de données que vous Compte AWS possédez dans la région actuelle. L'identifiant de cluster de base de données n'est pas sensible à la casse, mais il est stocké intégralement en minuscules, comme dans `mydbclusterinstance`. Ce champ est obligatoire.
6. Dans le volet Options de base de données, acceptez les valeurs par défaut ou spécifiez les options pour Port de la base de données et Groupe de paramètres de cluster de base de données.
7. Dans le volet Chiffrement, acceptez la valeur par défaut ou spécifiez les valeurs des paramètres Activer le chiffrement ou Désactiver le chiffrement.
8. Dans le volet Exportations de journaux, choisissez les types de journaux à publier sur Amazon CloudWatch Logs. Le Rôle IAM est déjà défini.
9. Dans le volet Restaurer le rôle, choisissez le rôle IAM que AWS Backup assumera pour cette restauration.
10. Après avoir spécifié tous vos paramètres, choisissez Restaurer la sauvegarde.

    Le volet Restaurer les tâches s'affiche. Un message en haut de la page fournit des informations sur la tâche de restauration.
11. Une fois votre restauration terminée, attachez votre cluster Neptune restauré à une instance Amazon RDS.

Utilisez l' AWS Backup API, la CLI ou le SDK pour restaurer les points de restauration Neptune

Restaurez d'abord votre cluster. Utilisez `StartRestoreJob`. Vous pouvez spécifier les métadonnées suivantes lors des restaurations Amazon DocumentDB :

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

Ensuite, connectez votre cluster Neptune restauré à une instance Amazon RDS à l'aide de `create-db-instance`.

- Pour Linux, macOS ou Unix :

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- Pour Windows :

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

Pour plus d'informations, consultez `RestoreDBClusterFromSnapshot` dans la Référence de l'API de gestion Neptune et `restore-db-cluster-from-snapshot` dans le Guide de l'interface de ligne de commande Neptune.

Restaurez les sauvegardes de CloudFormation Stack

Une sauvegarde CloudFormation composite est une combinaison d'un CloudFormation modèle et de tous les points de restauration imbriqués associés. N'importe quel nombre de points de récupération imbriqués peut être restauré, mais le point de récupération composite (qui est le point de récupération de niveau supérieur) ne peut pas être restauré.

Lorsque vous restaurez un CloudFormation modèle de point de restauration, vous créez une nouvelle pile dont les modifications sont définies pour représenter la sauvegarde.

Restaurez CloudFormation avec la AWS Backup console ;

Depuis la CloudFormation console, vous pouvez voir la nouvelle pile et le nouvel ensemble de modifications. Pour en savoir plus sur les jeux de modifications, consultez Mise à jour des piles à l'aide de jeux de modifications dans le Guide de l'utilisateur AWS CloudFormation .

Déterminez les points de restauration imbriqués à partir desquels vous souhaitez effectuer la restauration avec votre CloudFormation pile, puis restaurez-les à l'aide de la AWS Backup console.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Accédez aux Coffres de sauvegarde, sélectionnez le coffre-fort de sauvegarde contenant le point de récupération souhaité, puis cliquez sur Points de récupération.
3. Restaurez le point AWS CloudFormation de récupération du modèle.

    a. Cliquez sur le point de récupération composite contenant les points de récupération imbriqués que vous souhaitez restaurer pour afficher la page Détails du point de récupération composite.

    b. Sous Points de récupération imbriqués, les points de récupération imbriqués seront affichés. Chaque point de récupération aura un ID de point de récupération, un statut, un ID de ressource, un type de ressource, un type de sauvegarde et l'heure à laquelle le point de récupération a été créé. Cliquez sur le bouton radio situé à côté du point AWS CloudFormation de récupération, puis sur Restaurer. Assurez-vous de sélectionner le point de récupération dont le type de ressource est : AWS CloudFormation et le type de sauvegarde : sauvegarde.

4. Une fois le travail de restauration du CloudFormation modèle terminé, votre AWS CloudFormation modèle restauré sera visible dans la AWS CloudFormation console sous Stacks.
5. Sous Noms des piles, vous devriez trouver le modèle restauré avec le statut `REVIEW_IN_PROGRESS`.
6. Cliquez sur le nom de la pile pour voir les détails de la pile.
7. Il y a des onglets sous le nom de la pile. Cliquez sur Jeux de modifications.
8. Exécutez le jeu de modification.
9. Après ce processus, les ressources de la pile d'origine seront recréées dans la nouvelle pile. Les ressources avec état seront recréées vides. Pour récupérer les ressources dynamiques, revenez à la liste des points de récupération de la AWS Backup console, sélectionnez le point de récupération dont vous avez besoin et lancez une restauration.

Restaurer CloudFormation avec AWS CLI

Dans l'interface de ligne de commande, vous `start-restore-job`permet de restaurer une CloudFormation pile.

La liste suivante répertorie les métadonnées acceptées pour restaurer une CloudFormation ressource.

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```

Tests de restauration

Rubriques

- Présentation
- Comparaison des tests de la restauration avec le processus de restauration
- Gestion des tests de la restauration
- Création d’un plan de test de la restauration

- Mise à jour d’un plan de test de la restauration
- Affichage des plans de test de la restauration existants
- Affichage des tâches de test de la restauration
- Suppression d’un plan de test de la restauration
- Tests de restauration Audit
- Restauration de quotas et de paramètres de test
- Résolution des problèmes liés aux tests de restauration
- Métadonnées déduites de tests de la restauration
- Restaurer la validation des tests

Présentation

Les tests de restauration, une fonctionnalité proposée par AWS Backup, fournissent une évaluation automatique et périodique de la viabilité de la restauration, ainsi que la possibilité de surveiller la durée des tâches de restauration.

Tout d’abord, vous créez un plan de test de la restauration dans lequel vous indiquez le nom de votre plan, la fréquence de vos tests de la restauration et l’heure de début cible. Ensuite, vous attribuez les ressources à inclure dans votre plan. Vous choisissez ensuite d'inclure des points de récupération spécifiques ou aléatoires dans votre test. AWS Backup backup déduit intelligemment les métadonnées qui seront nécessaires à la réussite de votre tâche de restauration.

Lorsque l'heure prévue dans votre plan arrive, AWS Backup démarre les tâches de restauration en fonction de votre plan et surveille le temps nécessaire pour terminer la restauration.

Une fois le plan de test de la restauration terminé, vous pouvez utiliser les résultats pour démontrer la conformité aux exigences organisationnelles ou de gouvernance, telles que la réussite des scénarios de test de la restauration ou le délai d’exécution des tâches de restauration.

Vous pouvez éventuellement l'utiliser Restaurer la validation des tests pour confirmer les résultats du test de restauration.

Une fois que la validation facultative est terminée ou que la fenêtre AWS Backup de validation se ferme, les ressources impliquées dans le test de restauration sont supprimées conformément aux SLA du service.

À la fin du processus de test, vous pouvez afficher les résultats et le délai d’exécution des tests.

Comparaison des tests de la restauration avec le processus de restauration

Le test de la restauration exécute les tâches de restauration de la même manière que les restaurations à la demande et utilise les mêmes points de récupération (sauvegardes) qu'une restauration à la demande. Vous verrez des appels d'`StartRestoreJob`entrée CloudTrail (si vous avez activé cette option) pour chaque tâche démarrée par des tests de restauration

Il existe toutefois quelques différences entre le fonctionnement d'un test de la restauration planifié et celui d'une opération de restauration à la demande :

	Tests de restauration	Restaurer
Compte	La bonne pratique recommandée consiste à désigner un compte à utiliser pour les tests de la restauration	Vous pouvez restaurer des ressources à partir d'un compte
AWS Backup Audit Manager	Peut activer une commande pour confirmer si un test de la restauration répond aux objectifs de restauration spécifiés	
Cadence	Périodiquement dans le cadre d'un plan planifié.	À la demande
Régions	Disponible dans toutes les régions commerciales dans lesquelles AWS Backup elle opère, à l'exception d'Israël (Tel Aviv) Non disponible AWS GovCloud (USA Est), AWS GovCloud (USA Ouest), Chine (Pékin) et Chine (Ningxia).	Disponible dans toutes les régions commerciales dans lesquelles AWS Backup elle opère
Ressources	Les types de ressources que vous pouvez attribuer à	Toutes les ressources peuvent être restaurées.

	Tests de restauration	Restaurer
	votre plan de test incluent : Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, Amazon FSx (Lustre, ONTAP, OpenZFS, Windows), Amazon Neptune, Amazon RDS et Amazon S3.	
Résultats	Une fois le test de restauration terminé, la ressource restaurée est supprimée une fois la Restaurer la validation des tests fenêtre terminée.	Une fois la tâche de restauration terminée, la version restaurée de la ressource est conservée.
Balises	Pour les types de ressources qui prennent en charge les balises lors de la restauration, les tests appliquent des balises lors de la restauration.	Les balises sont facultatives pour les ressources prises en charge.

Gestion des tests de la restauration

Vous pouvez créer, afficher, mettre à jour ou supprimer un plan de test de la restauration dans la console AWS Backup.

Vous pouvez utiliser AWS CLI pour exécuter par programmation des opérations pour les plans de test de la restauration. Chaque CLI est spécifique au AWS service dont elle provient. Les commandes doivent être précédées de `aws backup`.

Suppression de données

Lorsqu'un test de restauration est terminé, AWS Backup commence à supprimer les ressources impliquées dans le test. Cette suppression n’est pas instantanée. Chaque ressource possède une configuration sous-jacente qui détermine la manière dont ces ressources sont stockées et leur cycle de vie. Par exemple, si les compartiments Amazon S3 font partie du test de la restauration, des

règles de cycle de vie sont ajoutées au compartiment. L'exécution des règles et la suppression complète du compartiment et de ses objets peuvent prendre plusieurs jours, mais ces ressources ne seront facturées que jusqu'au jour où la règle de cycle de vie est lancée (par défaut, il s'agit d'un jour). La vitesse de suppression dépend du type de ressource.

Les ressources faisant partie d'un plan de test de la restauration contiennent une balise appelée `awsbackup-restore-test`. Si un utilisateur supprime cette balise, il AWS Backup ne peut pas supprimer la ressource à la fin de la période de test. L'utilisateur devra plutôt la supprimer manuellement.

Pour savoir pourquoi les ressources n'ont peut-être pas été supprimées comme prévu, vous pouvez rechercher les tâches ayant échoué dans la console ou utiliser l'interface de ligne de commande pour appeler la demande d'API `DescribeRestoreJob` afin de récupérer les messages du statut de suppression.

Les plans de sauvegarde (autres que les plans de test de restauration) ignorent les ressources créées par les tests de restauration (celles dont la balise `awsbackup-restore-test` ou le nom commence par`awsbackup-restore-test`).

Contrôle des coûts

Les tests de la restauration ont un coût par test de la restauration. Selon les ressources incluses dans votre plan de test de la restauration, les tâches de restauration incluses dans le plan peuvent également avoir un coût. Consultez Tarification AWS Backup pour plus d'informations.

Lorsque vous configurez un plan de test de la restauration pour la première fois, il peut être avantageux d'inclure un nombre minimum de types de ressources et de ressources protégées afin de vous familiariser avec la fonctionnalité, le processus et les coûts moyens impliqués. Vous pouvez mettre à jour un plan après sa création pour ajouter d'autres types de ressources et des ressources protégées.

Création d'un plan de test de la restauration

Un plan de test de la restauration comporte deux parties : la création du plan et l'attribution des ressources.

Lorsque vous utilisez la console, ces parties sont séquentielles. Dans la première partie, vous définissez le nom, la fréquence et les heures de début. Au cours de la deuxième partie, vous affectez des ressources à votre plan de test.

Lorsque vous utilisez AWS CLI une API, utilisez d'abord `create-restore-testing-plan`. Une fois que vous avez reçu une réponse positive et que le plan a été créé, utilisez alors `create-restore-testing-selection` pour chaque type de ressource que vous souhaitez inclure dans votre plan.

Console

Partie I : Création d'un plan de test de la restauration à l'aide de la console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le menu de navigation de gauche, recherchez Tests de restauration et sélectionnez-le.
3. Choisissez Créer un plan de test de la restauration.
4. Général

   a. Nom : tapez le nom de votre nouveau plan de test de la restauration. Le nom ne peut pas être modifié après la création. Le nom doit contenir uniquement des caractères alphanumériques et des traits de soulignement.

   b. Fréquence des tests : choisissez la fréquence à laquelle les tests de la restauration seront exécutés.

   c. Heure de début : définissez l'heure (en heures et minutes) à laquelle vous préférez que le test commence. Vous pouvez également définir le fuseau horaire local dans lequel vous souhaitez que le plan de test de la restauration fonctionne.

   d. Commencer dans les délais : cette valeur (en heures) correspond à la période pendant laquelle le test de restauration est censé commencer. AWS Backup fait de son mieux pour démarrer toutes les tâches de restauration désignées au cours du délai imparti et répartit les heures de début de manière aléatoire au cours de cette période.
5. Sélection des points de récupération : vous définissez ici les coffres-forts sources, la plage de points de récupération et les critères de sélection pour les points de récupération (sauvegardes) que vous souhaitez inclure dans le plan.

   a. Coffres-forts sources : choisissez d'inclure tous les coffres-forts disponibles ou uniquement des coffres-forts spécifiques pour vous aider à filtrer les points de récupération pouvant figurer dans votre plan. Si vous choisissez des coffres-forts spécifiques, dans le menu déroulant, sélectionnez les coffres-forts que vous souhaitez inclure.

b. Points de récupération éligibles : spécifiez la période à partir de laquelle les points de récupération seront sélectionnés. Vous pouvez sélectionner 1 à 365 jours, 1 à 52 semaines, 1 à 12 mois ou 1 an.

c. Critères de sélection : une fois que votre plage de dates de points de récupération est spécifiée, vous pouvez choisir d'inclure le dernier point ou un point au hasard dans votre plan. Vous pouvez choisir un point aléatoire pour évaluer l'état général des points de récupération à une fréquence plus régulière au cas où une restauration vers une ancienne version serait justifiée.

d. Points de oint-in-time restauration P : si votre plan inclut des ressources dotées de points de sauvegarde continue (point-in-time-restore/PITR), vous pouvez cocher cette case pour que votre plan de test inclue les sauvegardes continues en tant que points de restauration éligibles (voir Disponibilité des fonctionnalités par ressource pour lesquels les types de ressources disposent de cette fonctionnalité).

6. (facultatif) Balises ajoutées pour restaurer le plan de test : vous pouvez choisir d'ajouter jusqu'à 50 balises à votre plan de test de la restauration. Chaque balise doit être ajoutée séparément. Pour ajouter une nouvelle balise, sélectionnez Ajouter une nouvelle balise.

Partie II : Attribution de ressources au plan à l'aide de la console

Dans cette section, vous choisissez les ressources que vous avez sauvegardées à inclure dans votre plan de test de la restauration. Vous choisirez le nom de l'attribution de ressource, le rôle que vous utiliserez pour le test de la restauration et définirez la période de conservation avant le nettoyage. Ensuite, vous allez sélectionner le type de ressource ainsi que l'étendue, et éventuellement affiner votre sélection à l'aide de balises.

> **Tip**
>
> Pour revenir au plan de test de la restauration auquel vous souhaitez ajouter des ressources, vous pouvez accéder à la console AWS Backup, sélectionner Tests de restauration, puis rechercher le plan de test de votre choix et le sélectionner.

1. Général

a. Nom d'attribution de la ressource : entrez un nom pour cette attribution de ressource à l'aide d'une chaîne de caractères alphanumériques et de traits de soulignement, sans espaces blancs.

b. Restaurer le rôle IAM : le test doit utiliser un rôle Identity and Access Management (IAM) que vous désignez. Vous pouvez choisir le rôle AWS Backup par défaut ou un rôle différent. Si la AWS Backup valeur par défaut n'existe pas encore à la fin de ce processus, elle AWS Backup sera créée automatiquement pour vous avec les autorisations nécessaires. Le rôle IAM que vous choisissez pour les tests de la restauration doit contenir les autorisations trouvées dans AWSBackupServicePolicyForRestores.

c. Période de conservation avant le nettoyage : lors d'un test de la restauration, les données de sauvegarde sont temporairement restaurées. Par défaut, ces données sont supprimées une fois le test terminé. Vous avez la possibilité de retarder la suppression de ces données si vous souhaitez exécuter la validation lors de la restauration.

   Si vous prévoyez d'exécuter la validation, sélectionnez Conserver pendant un certain nombre d'heures et entrez une valeur comprise entre 1 et 168 heures incluses. Notez que la validation peut être exécutée par programmation, mais pas depuis la console AWS Backup .

2. Ressources protégées :

   a. Sélectionner un type de ressource : sélectionnez les types de ressources et l'étendue des sauvegardes de ces types à inclure dans le plan de test des ressources. Chaque plan peut contenir plusieurs types de ressources, mais chaque type de ressource doit être attribué au plan individuellement.

   b. Portée de la sélection des ressources : une fois le type choisi, indiquez si vous souhaitez inclure toutes les ressources protégées disponibles de ce type ou si vous souhaitez inclure uniquement des ressources protégées spécifiques.

   c. (facultatif) Affiner la sélection des ressources à l'aide de balises : si vos sauvegardes comportent des balises, vous pouvez filtrer par balises pour sélectionner des ressources protégées spécifiques. Entrez la clé de la balise, la condition pour que cette clé soit incluse ou non, et la valeur de la clé. Sélectionnez ensuite le bouton Ajouter des balises.

      Les balises des ressources protégées sont évaluées en vérifiant les balises du dernier point de récupération dans le coffre-fort de sauvegarde contenant la ressource protégée.

3. Paramètres de restauration : certaines ressources nécessitent de spécifier des paramètres pour préparer une tâche de restauration. Dans la plupart des cas, AWS Backup déduira les valeurs en fonction de la sauvegarde stockée.

Il est recommandé dans la plupart des cas de conserver ces paramètres ; toutefois, vous pouvez modifier les valeurs en choisissant une autre sélection dans le menu déroulant. Parmi les exemples où la modification des valeurs peut être optimale, citons le remplacement des clés de chiffrement, les paramètres Amazon FSx où les données ne peuvent pas être déduites et la création de sous-réseaux.

Par exemple, si une base de données RDS est l'un des types de ressources que vous attribuez à votre plan de test de la restauration, des paramètres tels que la zone de disponibilité, le nom de la base de données, la classe d'instance de base de données et le groupe de sécurité VPC apparaîtront avec des valeurs déduites que vous pouvez modifier le cas échéant.

AWS CLI

La commande de l'interface de ligne de commande `CreateRestoreTestingPlan` est utilisée pour établir un plan de test de la restauration.

Le plan de test doit contenir :

- `RestoreTestingPlan`, qui doit contenir un `RestoreTestingPlanName` unique
- Expression cron `ScheduleExpression`
- `RecoveryPointSelection`

  Bien que nommé de la même manière, ce n'est PAS le même que`RestoreTestingSelection`.

  `RecoveryPointSelection`possède cinq paramètres (trois obligatoires et deux facultatifs). Les valeurs que vous spécifiez déterminent le point de récupération inclus dans le test de restauration. Vous devez indiquer `Algorithm` si vous voulez le dernier point de récupération dans votre répertoire `SelectionWindowDays` ou si vous voulez un point de récupération aléatoire, et vous devez indiquer dans `IncludeVaults` quels coffres-forts les points de récupération peuvent être choisis.

Une sélection peut avoir un ou plusieurs ARN de ressources protégées ou une ou plusieurs conditions, mais elle ne peut pas avoir les deux.

Vous pouvez également inclure :

- ScheduleExpressionTimezone
- Tags
- CreatorRequestId
- StartWindowHours

Utilisez la commande de l'interface de ligne de commande create-restore-testing-plan.

Une fois le plan créé, vous devez lui attribuer des ressources à l'aide de create-restore-testing-selection.

Cela comprend RestoreTestingSelectionName, ProtectedResourceType et l'un des éléments suivants :

- ProtectedResourceArns

- ProtectedResourceConditions

Chaque type de ressource protégée peut avoir une seule valeur. Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour ProtectedResourceArns avec ProtectedResourceConditions. Vous pouvez également inclure jusqu'à 30 ARN de ressources protégées spécifiques dans ProtectedResourceArns.

Détermination du point de récupération

Chaque fois qu'un plan de test est exécuté (selon la fréquence et l'heure de début que vous avez spécifiées), un point de récupération éligible par ressource protégée sélectionnée est restauré par le test de restauration. Si aucun point de récupération pour une ressource ne répond aux critères de sélection des points de récupération, cette ressource ne sera pas incluse dans le test.

Un point de récupération pour une ressource protégée dans une sélection de test est éligible s'il répond aux critères de la période spécifiée et s'il inclut des coffres-forts dans le plan de test de restauration.

Une ressource protégée est sélectionnée si la sélection du test inclut le type de ressource et si l'une des conditions suivantes est vraie :

- L'ARN de la ressource est spécifié dans cette sélection ; ou

- Les conditions des balises associées à cette sélection correspondent aux balises du dernier point de récupération pour la ressource.

Mise à jour d’un plan de test de la restauration

Vous pouvez mettre à jour certaines parties de votre plan de test de la restauration et les sélections de ressources qu’il contient via la console ou AWS CLI.

Console

Mise à jour des plans de test de la restauration et des sélections dans la console

Lorsque vous consultez la page des détails du plan de test de la restauration dans la console, vous pouvez modifier (mettre à jour) de nombreux paramètres de votre plan. Pour ce faire,

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le menu de navigation de gauche, recherchez Tests de restauration et sélectionnez-le.
3. Sélectionnez le bouton Modifier.
4. Réglez la fréquence, l’heure de début et l’heure à laquelle le test débutera après l’heure de début choisie.
5. Enregistrez vos modifications.

AWS CLI

Mettez à jour les plans de test et les sélections de restauration via AWS CLI

Demande UpdateRestoreTestingPlanet UpdateRestoreTestingSelectionpeut être utilisé pour envoyer des mises à jour partielles d'un plan ou d'une sélection spécifique. Les noms ne peuvent pas être modifiés, mais vous pouvez mettre à jour d’autres paramètres. N’incluez que les paramètres que vous souhaitez modifier dans chaque demande.

Avant d'envoyer une demande de mise à jour, utilisez GetRestoreTestingPlanet GetRestoreTestingSelectionpour déterminer si elle RestoreTestingSelection contient des ARN spécifiques ou si elle utilise le caractère générique et les conditions.

Si votre sélection de tests de la restauration contient des ARN (au lieu d’un caractère générique) et que vous souhaitez les remplacer par un caractère générique assorti de conditions, la demande de mise à jour doit inclure à la fois le caractère générique de l’ARN et les conditions. Une

sélection peut avoir des ARN de ressources protégées ou utiliser le caractère générique avec des conditions, mais elle ne peut pas avoir les deux.

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`
- `update-restore-testing-selection`

Affichage des plans de test de la restauration existants

Console

Affichage des détails d'un plan de test de la restauration existant et des ressources attribuées dans la console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Sélectionnez Tests de restauration dans le menu de navigation de gauche. L'écran affiche vos plans de test de la restauration. Les plans sont affichés par défaut dans l'ordre de dernière exécution.
3. Sélectionnez le lien dans un plan pour voir ses détails, y compris un résumé du plan, son nom, sa fréquence, son heure de début et le début au sein de la valeur.

Vous pouvez également consulter les ressources protégées dans le cadre de ce plan, les tâches de test de la restauration des 30 derniers jours incluses dans ce plan et toutes les balises que vous pouvez créer dans le cadre de ce plan de test.

AWS CLI

Obtention d'informations sur un plan de test de la restauration existant et sur une sélection de tests à l'aide de la ligne de commande

- `list-restore-testing-plan`
- `list-restore-testing-selections`
- `get-restore-testing-plan`
- `get-restore-testing-selection`

Affichage des tâches de test de la restauration

Console

Affichage des tâches de test de la restauration existantes dans la console

Les tâches de test de la restauration sont incluses sur la page des tâches de restauration.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Accédez à la page Tâches.

   Vous pouvez également sélectionner Tests de restauration, puis sélectionner un plan de test de la restauration pour voir ses détails et les tâches associées au plan.
3. Sélectionnez l’onglet Tâches de restauration.

   Sur cette page, vous pouvez consulter le statut, l’heure de restauration, le type de restauration, l’ID de ressource, le type de ressource, le plan de test de la restauration auquel appartient la tâche, l’heure de création et l’ID du point de récupération de la tâche de restauration.

   Les tâches incluses dans un plan de test de la restauration ont le type de restauration Test.

Les tâches de test de la restauration comportent plusieurs catégories de statut :

- Un type de statut nécessitant une attention particulière est souligné ; passez le curseur sur le statut pour voir des informations supplémentaires si elles sont disponibles.
- Un statut de validation s'affichera s'il Restaurer la validation des tests a été lancé lors du test (non disponible dans la console).
- Le statut de suppression indique le statut des données générées par le test de la restauration. Trois statuts de suppression sont possibles : Réussi, Suppression et Échec.

  Si la suppression d’une tâche de test de la restauration a échoué, vous devrez supprimer la ressource manuellement car le flux de test de la restauration n’a pas pu la terminer automatiquement. Souvent, une suppression échouée est déclenchée si la balise `awsbackup-restore-test` est supprimée de la ressource.

AWS CLI

Affichage des tâches de test de la restauration existantes depuis la ligne de commande

- `list-restore-jobs-by-protected-resource`

Suppression d'un plan de test de la restauration

Console

Suppression d'un plan de test de la restauration dans la console

1. Accédez à Affichage des plans de test de la restauration existants pour voir vos plans de test de la restauration actuels.
2. Sur la page des détails du plan de test de la restauration, supprimez un plan en sélectionnant Supprimer.
3. Une fois que vous avez sélectionné Supprimer, un écran de confirmation contextuel apparaît pour confirmer que vous souhaitez supprimer votre plan. Sur cet écran, le nom de votre plan de test de la restauration spécifique sera affiché en gras. Pour continuer, saisissez le nom exact du plan de test en distinguant majuscules et minuscules, y compris les soulignements, les tirets et les points.

   Si l'option Supprimer le plan de test de la restauration ne peut pas être sélectionnée, entrez à nouveau le nom jusqu'à ce qu'il corresponde au nom affiché. Une fois la correspondance exacte établie, l'option permettant de supprimer le plan de test de la restauration pourra être sélectionnée.

AWS CLI

Suppression d'un plan de test de la restauration via la ligne de commande

La commande CLI DeleteRestoreTestingSelectionpeut être utilisée pour supprimer une sélection de test de restauration. Incluez `RestoreTestingPlanName` et `RestoreTestingSelectionName` dans la demande.

Toutes les sélections de tests associées à un plan de test doivent être supprimées avant de supprimer le plan de test. Une fois que toutes les sélections de test ont été supprimées, vous

pouvez utiliser la demande DeleteRestoreTestingPland'API pour supprimer un plan de test de restauration. Vous devez inclure `RestoreTestingPlanName`.

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

Tests de restauration Audit

Restaurez les intégrations de test avec AWS Backup Audit Manager pour vous aider à évaluer si une ressource restaurée a été terminée dans le délai de restauration cible.

Pour plus d'informations, consultez la contrôle Temps de restauration des ressources pour atteindre l'objectif dans Contrôles et mesures correctives d'AWS Backup Audit Manager.

Restauration de quotas et de paramètres de test

- 100 plans de test de la restauration
- 50 balises peuvent être ajoutées à chaque plan de test de la restauration
- 30 sélections par plan
- 30 ARN de ressources protégées par sélection
- 30 conditions de ressources protégées par sélection (y compris celles comprises dans `StringEquals` et `StringNotEquals`)
- 30 sélecteurs de coffre-fort par sélection
- Nombre maximum de jours pour la fenêtre de sélection : 365 jours
- Heures de la fenêtre de début : min : 1 heure ; max. : 168 heures (7 jours)
- Longueur maximale du nom du plan : 50 caractères
- Longueur maximale du nom de la sélection : 50 caractères

Des informations supplémentaires concernant les limites peuvent être consultées ici : AWS Backup quotas.

Résolution des problèmes liés aux tests de restauration

Si vous avez des tâches de test de restauration dont l'état de restauration est égal à`Failed`, les raisons suivantes peuvent vous aider à en déterminer la cause et à y remédier.

Les messages d'erreur peuvent être visualisés dans la AWS Backup console sur la page de détails de l'état de la tâche ou à l'aide des commandes de la CLI `list-restore-jobs-by-protected-resource` ou`list-restore-jobs`.

1. Erreur : *`No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.`*

   Solution 1 : mettez à jour votre sélection de test de restauration et remplacez le paramètre`SubnetId`. La AWS Backup console affiche ce paramètre sous la forme « Sous-réseau ».

   Solution 2 : recréer le VPC par défaut.

   Types de ressources concernés : Amazon EC2

2. Erreur : *`No subnets found for the default VPC [vpc]. Please specify a subnet.`*

   Solution 1 : mettez à jour votre sélection de test de restauration et remplacez le paramètre de `SubnetId` restauration. La AWS Backup console affiche ce paramètre sous la forme « Sous-réseau ».

   Solution 2 : créer un sous-réseau par défaut dans le VPC par défaut.

   Types de ressources concernés : Amazon EC2

3. Erreur : *`No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.`*

   Solution 1 : mettez à jour votre sélection de test de restauration et remplacez le paramètre de `DBSubnetGroupName` restauration. La AWS Backup console affiche ce paramètre en tant que groupe de sous-réseaux.

   Solution 2 : créer un sous-réseau par défaut dans le VPC par défaut.

   Types de ressources concernés : Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptune

4. Erreur :*`IAM Role cannot be assumed by AWS Backup`*.

Solution : Le rôle de restauration doit être assumé par AWS Backup. Mettez à jour la politique de confiance du rôle dans IAM pour permettre à celui-ci d'être assumé par `"backup.amazonaws.com"` ou mettez à jour votre sélection de tests de restauration pour utiliser un rôle assumé par. AWS Backup

Types de ressources concernés : tous

5. Erreur : *`Access denied to KMS key.`* ou *`The specified AWS KMS key`* ARN *`does not exist, is not enabled or you do not have permissions to access it.`*

   Solution : Vérifiez les points suivants :

   a. Le rôle de restauration a accès à la AWS KMS clé utilisée pour chiffrer vos sauvegardes et, le cas échéant, à la clé KMS utilisée pour chiffrer la ressource restaurée.

   b. Les politiques de ressources relatives aux clés KMS ci-dessus autorisent le rôle de restauration à y accéder.

   Si les conditions ci-dessus ne sont pas encore remplies, configurez le rôle de restauration et les politiques de ressources pour un accès approprié. Ensuite, exécutez à nouveau le test de restauration.

   Types de ressources concernés : tous

6. Erreurs : *`User ARN is not authorized to perform action on resource because no identity based policy allows the action.`* ou*`Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx`*.

   Solution : le rôle de restauration ne dispose pas des autorisations adéquates. Mettez à jour les autorisations dans IAM pour le rôle de restauration.

   Types de ressources concernés : tous

7. Erreurs : *`User ARN is not authorized to perform action on resource because no resource-based policy allows the action.`* ou *`User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.`*

   Solution : Le rôle de restauration ne dispose pas d'un accès adéquat à la ressource spécifiée dans le message. Mettez à jour la politique de ressources relative à la ressource mentionnée.

Types de ressources concernés : tous

Métadonnées déduites de tests de la restauration

La restauration d'un point de récupération nécessite de restaurer les métadonnées. Pour effectuer des tests de la restauration, AWS Backup déduit automatiquement les métadonnées susceptibles d'aboutir à une restauration réussie. La commande `get-restore-testing-inferred-metadata` peut être utilisée pour prévisualiser ce qui AWS Backup sera déduit. La commande `get-restore-job-metadata` renvoie l'ensemble de métadonnées déduit par AWS Backup. Notez que pour certains types de ressources (Amazon FSx), AWS Backup il n'est pas possible de déduire un ensemble complet de métadonnées.

Les métadonnées de restauration déduites sont déterminées au cours du processus de test de la restauration. Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Certaines remplacements de métadonnées ne sont pas disponibles dans la AWS Backup console.

Chaque ressource prise en charge possède à la fois des clés et des valeurs de métadonnées de restauration déduites et des clés de métadonnées de restauration remplaçables. Seules les paires clé-valeur `RestoreMetadataOverrides` ou les paires clé-valeur imbriquées marquées de la mention « *`obligatoire pour une restauration réussie`* » doivent être incluses ; les autres sont facultatives. Notez que les valeurs de clé ne sont pas sensibles à la casse.

> **Important**
>
> AWS Backup peut en déduire qu'une ressource doit être restaurée avec ses paramètres par défaut, comme une instance Amazon EC2 ou un cluster Amazon RDS restauré sur le VPC par défaut. Toutefois, si la valeur par défaut n'est pas présente, par exemple si le VPC ou le sous-réseau par défaut a été supprimé et qu'aucune modification des métadonnées n'a été saisie, la restauration échouera.

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables

DynamoDB	`deletionProtection` , où la valeur est définie sur `false`
	
	`encryptionType` a la valeur `Default`
	
	`targetTableName` , où la valeur est définie sur une valeur aléatoire commençant par `awsbackup-restore-test-`
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` , dont la valeur est définie sur une zone de disponibilité aléatoire
	
	`encrypted` , dont la valeur est définie sur `true`
		`availabilityZone`
		
		`kmsKeyId`

Amazon EC2	La valeur `disableApiTermination` est définie sur `false`
	
	La valeur `instanceType` est définie sur le type d'instance du point de récupération en cours de restauration
	
	La valeur `requiredImdsV2` est définie sur `true`
		`iamInstanceProfileName` la valeur peut être nulle ou `UseBackedUpValue`
		
		`instanceType`
		
		`requireImdsV2`
		
		`securityGroupIds`
		
		`subnetId`

Amazon EFS	La valeur `encrypted` est définie sur `true` La valeur `file-system-id` est définie sur l'ID du	`kmsKeyId`

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
	système de fichier du point de récupération en cours de restauration `kmsKeyId value` a la valeur `alias/aws/elasticfilesystem` La valeur `newFileSystem` est définie sur `true` La valeur `performanceMode` est définie sur `generalPurpose`	

Amazon FSx pour Lustre	`lustreConfiguration` possède des clés imbriquées. Une clé imbriquée est `automaticBackupRetentionDays`, dont la valeur est définie sur `0`	`kmsKeyId`
		
		`lustreConfiguration` possède une clé imbriquée `logConfiguration`
		
		`securityGroupIds`
		
		`subnetIds`, *nécessaire pour une restauration réussie*

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables
Amazon FSx pour ONTAP NetApp	`name` est défini sur une valeur aléatoire commençant par `awsbackup_restore_test_` `ontapConfiguration` possède des clés imbriquées, notamment : • `junctionPath` où `/name` est le nom du volume en cours de restauration • `sizeInMegabytes` , dont la valeur est définie sur la taille en mégaoctets du point de récupération en cours de restauration • `snapshotPolicy` , où la valeur est définie sur none	`ontapConfiguration` possède des clés imbriquées spécifiques remplaçables, notamment : • `junctionPath` • `ontapVolumeType` • `securityStyle` • `sizeInMegabytes` • `storageEfficiencyEnabled` • `storageVirtualMachineId` , *nécessaire pour une restauration réussie* • `tieringPolicy`

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables

Amazon FSx pour OpenZFS	`openZfzConfiguration`, qui possède des clés imbriquées, notamment :
	• `automaticBackupRetentionDays` avec une valeur définie sur `0`
	• `deploymentType` avec une valeur définie sur le type de déploiement du point de récupération en cours de restauration
	• `throughputCapacity`, dont la valeur est basée sur le `deploymentType`. Si le `deploymentType` est `SINGLE_AZ_1`, la valeur est définie sur `64` ; si le `deploymentType` est `SINGLE_AZ_2 or MULTI_AZ_1`, la valeur est définie sur `160`
		`kmsKeyId`
		`openZfsConfiguration` possède des clés imbriquées spécifiques remplaçables, notamment :
		• `deploymentType`
		• `throughputCapacity`
		• `diskiopsConfiguration`
		`securityGroupIds`
		`subnetIds`

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables

Amazon FSx for Windows File Server	`windowsConfiguration`, qui possède des clés imbriquées, notamment :
	• `automaticBackupRetentionDays` avec une valeur définie sur `0`
	• `deploymentType` avec une valeur définie sur le type de déploiement du point de récupération en cours de restauration
	• `throughputCapacity` avec une valeur définie sur `8`
		`kmsKeyId`
		`securityGroupIds`
		`subnetIds`, *obligatoire pour une restauration réussie*
		`windowsConfiguration`, avec des clés imbriquées spécifiques remplaçables
		• `throughputCapacity`
		• `activeDirectoryId` *nécessaire pour une restauration réussie s'il n'selfManagedActiveDirectoryConfiguration est pas inclus*
		• `selfManagedActiveDirectoryConfiguration` *nécessaire pour une restauration réussie s'il n'activeDirectoryId est pas inclus*
		• `preferredSubnetId`

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables

Amazon RDS, Aurora, Amazon DocumentDB, clusters Amazon Neptune	`availabilityZones` avec une valeur définie sur une liste de trois zones de disponibilité aléatoires au maximum
	
	`dbClusterIdentifier` avec une valeur aléatoire commençant par `awsbackup-restore-test`
	
	`engine` avec une valeur définie sur le moteur du point de récupération en cours de restauration
		`availabilityZones`
		
		`databaseName`
		
		`dbClusterParameterGroupName`
		
		`dbSubnetGroupName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`engine`
		
		`engineMode`
		
		`engineVersion`
		
		`kmskeyId`
		
		`port`
		
		`optionGroupName`
		
		`scalingConfiguration`
		
		`vpcSecurityGroupIds`

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables

Instances Amazon RDS	`dbInstanceIdentifier` avec une valeur aléatoire commençant par `awsbackup-restore-test-`
	
	`deletionProtection` avec une valeur définie sur `false`
	
	`multiAz` avec une valeur définie sur `false`
	
	`publiclyAccessible` avec une valeur définie sur false
		`allocatedStorage`
		
		`availabilityZones`
		
		`dbInstanceClass`
		
		`dbName`
		
		`dbParameterGroupName`
		
		`dbSubnetGroupName`
		
		`domain`
		
		`domainIamRoleName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`iops`
		
		`licensemodel`
		
		`multiAz`
		
		`optionGroupName`
		
		`port`
		
		`processorFeatures`
		
		`publiclyAccessible`
		
		`storageType`
		
		`vpcSecurityGroupIds`

Type de ressource	Clés et valeurs de métadonnées de restauration déduites	Métadonnées remplaçables

Amazon Simple Storage Service (Amazon S3)	`destinationBucketName` avec une valeur aléatoire commençant par `awsbackup-restore-test-`
	
	`encrypted` avec une valeur définie sur `true`
	
	`encryptionType` avec une valeur définie sur `SSE-S3`
	
	`newBucket` avec une valeur définie sur `true`
		`encryptionType`
		
		`kmsKey`

Restaurer la validation des tests

Vous avez la possibilité de créer une validation pilotée par des événements qui s'exécute lorsqu'une tâche de test de restauration est terminée.

Tout d'abord, créez un flux de validation avec n'importe quelle cible prise en charge par Amazon EventBridge, telle que AWS Lambda. Ensuite, ajoutez une EventBridge règle qui attend que la tâche de restauration atteigne son statut`COMPLETED`. Troisièmement, créez un plan de test de restauration (ou laissez un plan existant s'exécuter comme prévu). Enfin, une fois le test de restauration terminé, surveillez les journaux du flux de travail de validation pour vous assurer qu'il s'est déroulé comme prévu (une fois la validation exécutée, un statut de validation s'affiche dans la AWS Backup console).

1. Configurer le flux de travail de validation

   Vous pouvez configurer un flux de travail de validation à l'aide de Lambda ou de toute autre cible prise en charge par. EventBridge Par exemple, si vous validez un test de restauration contenant une instance Amazon EC2, vous pouvez inclure du code qui envoie un ping à un point de terminaison de contrôle de santé.

   Vous pouvez utiliser les détails de l'événement pour déterminer les ressources à valider.

Vous pouvez utiliser une couche Lambda personnalisée pour utiliser le dernier SDK (car il n'`PutRestoreValidationResult`est pas encore disponible via le SDK Lambda).

Voici un exemple :

```
import { Backup } from "@aws-sdk/client-backup";

export const handler = async (event) => {
  console.log("Handling event: ", event);

  const restoreTestingPlanArn = event.detail.restoreTestingPlanArn;
  const resourceType = event.detail.resourceType;
  const createdResourceArn = event.detail.createdResourceArn;

  // TODO: Validate the resource

  const backup = new Backup();
  const response = await backup.putRestoreValidationResult({
    RestoreJobId: event.detail.restoreJobId,
    ValidationStatus: "SUCCESSFUL", // TODO
    ValidationStatusMessage: "" // TODO
  });

  console.log("PutRestoreValidationResult: ", response);
  console.log("Finished");
};
```

2. Ajouter une EventBridge règle

   Créez une EventBridge règle qui écoute l'`COMPLETE`Dévénement de la tâche de restauration.

   Vous pouvez éventuellement filtrer les événements par type de ressource ou restaurer l'ARN du plan de test. Définissez la cible de cette règle pour appeler le flux de travail de validation que vous avez défini à l'étape 1. Voici un exemple :

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
```

```
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. Laisser le plan de test de restauration s'exécuter et se terminer

   Le plan de test de restauration s'exécutera conformément au calendrier que vous avez configuré.

   Voir Créer un plan de test de restauration si vous n'en avez pas encore un ou Mettre à jour un plan de test de restauration si vous souhaitez modifier les paramètres.

4. Surveillez les résultats

   Une fois qu'un plan de test de restauration a été exécuté comme prévu, vous pouvez consulter les journaux de votre flux de travail de validation pour vous assurer qu'il s'est déroulé correctement.

   Vous pouvez appeler l'API `PutRestoreValidationResult` pour publier les résultats, qui seront ensuite consultables dans la AWS Backup console et via des appels d' AWS Backup API décrivant et répertoriant les tâches de restauration, telles que `DescribeRestoreJob` ou`ListRestoreJob`.

   Une fois qu'un statut de validation est défini, il ne peut pas être modifié.

Affichage d'une liste de sauvegardes

Vous pouvez consulter la liste de vos sauvegardes à l'aide de la AWS Backup console ou par programmation.

Rubriques

- Liste des sauvegardes par ressource protégée dans la console
- Liste des sauvegardes par coffre-fort de sauvegarde dans la console

- Liste des sauvegardes par programmation

Liste des sauvegardes par ressource protégée dans la console

Suivez les étapes ci-dessous pour afficher une liste des sauvegardes pour une ressource spécifique sur la console AWS Backup .

1. Connectez-vous à la AWS Management Console AWS Backup console et ouvrez-la à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Protected resources (Ressources protégées).
3. Choisissez une ressource protégée dans la liste afin d'afficher la liste des sauvegardes. Seules les ressources sauvegardées par AWS Backup sont répertoriées sous Ressources protégées.

Vous pouvez afficher les sauvegardes pour la ressource. Cette vue vous permet également de choisir une sauvegarde et de la restaurer.

Liste des sauvegardes par coffre-fort de sauvegarde dans la console

Suivez les étapes ci-dessous pour afficher une liste des sauvegardes organisées dans un coffre-fort de sauvegarde.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le panneau de navigation, choisissez Backup vaults (Coffres-forts de sauvegarde).
3. Dans la section Backups (Sauvegardes), affichez la liste de toutes les sauvegardes organisées dans ce coffre-fort de sauvegarde. Dans cette vue, vous pouvez trier les sauvegardes en fonction de n'importe quel en-tête de colonne (y compris le statut), ainsi que sélectionner une sauvegarde pour la restaurer, la modifier ou la supprimer.

Liste des sauvegardes par programmation

Vous pouvez répertorier les sauvegardes par programmation à l'aide des opérations d'API `ListRecoveryPoint` :

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

Par exemple, la commande suivante AWS Command Line Interface (AWS CLI) répertorie toutes vos sauvegardes avec le `EXPIRED` statut :

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

Vous pouvez utiliser AWS Backup Audit Manager pour vérifier la conformité de vos AWS Backup politiques par rapport aux contrôles que vous définissez. Un contrôle est une procédure conçue pour réaliser un audit de la conformité d'une exigence de sauvegarde, telle que la fréquence des sauvegardes ou la période de rétention des sauvegardes.

AWS Backup Audit Manager vous aide à répondre à des questions telles que :

- « Est-ce que je sauvegarde toutes mes ressources ? »
- « Toutes mes sauvegardes sont-elles chiffrées ? »
- « Mes sauvegardes ont-elles lieu quotidiennement ? »

Vous pouvez utiliser AWS Backup Audit Manager pour rechercher les activités de sauvegarde et les ressources qui ne sont pas encore conformes aux contrôles que vous avez définis. Notez que seules les ressources actives seront incluses lorsque les contrôles évalueront la conformité des ressources. Par exemple, une instance Amazon EC2 en cours d'exécution sera évaluée. Une instance EC2 à l'état arrêté ne sera pas incluse dans l'évaluation de conformité.

Vous pouvez également l'utiliser pour générer automatiquement une piste d'audit de rapports quotidiens et à la demande à des fins de gouvernance de sauvegarde.

Les étapes suivantes fournissent une vue d'ensemble de l'utilisation d' AWS Backup Audit Manager. Pour des présentations détaillées, choisissez l'un des sujets à la fin de cette page.

1. Créez des frameworks contenant un ou plusieurs modèles de contrôle de gouvernance. Les questions précédentes sont des exemples de trois modèles de contrôle de gouvernance. Vous pouvez personnaliser les paramètres de certains modèles de contrôle de gouvernance. Par exemple, vous pouvez personnaliser le dernier contrôle pour demander : « Mes sauvegardes ont-elles lieu chaque semaine ? » plutôt que tous les jours.
2. Consultez votre framework pour voir combien de vos ressources sont conformes (ou non conformes) aux contrôles que vous avez définis dans ce framework.
3. Créez des rapports sur le statut de vos sauvegardes et de votre conformité. Conservez ces rapports comme preuve démontrable de vos pratiques de conformité ou pour identifier les activités de sauvegarde individuelles et les ressources qui ne sont pas encore conformes.

AWS Backup Audit Manager génère automatiquement un nouveau rapport toutes les 24 heures et le publie sur Amazon S3. Vous pouvez également générer des rapports à la demande.

> **Note**
>
> Avant de créer votre premier framework lié à la conformité, vous devez activer le suivi des ressources. Cela permet AWS Config de suivre vos AWS Backup ressources. Pour obtenir de la documentation technique sur la gestion du suivi des ressources, consultez la section Configuration à l' AWS Config aide de la console dans le guide du AWS Config développeur. Des frais s'appliquent lorsque vous activez le suivi des ressources. Pour plus d'informations sur le suivi des ressources, la tarification et la facturation pour AWS Backup Audit Manager, consultez la section Comptage, coûts et facturation.

Rubriques

Utilisation de frameworks d'audit

Un framework est un ensemble de contrôles qui vous aide à évaluer vos pratiques de sauvegarde. Vous pouvez utiliser des contrôles personnalisables prédéfinis pour définir vos politiques et évaluer si vos pratiques de sauvegarde sont conformes à vos politiques. Vous pouvez également configurer des rapports quotidiens automatiques pour obtenir des informations sur le statut de conformité de vos frameworks.

Chaque cadre s'applique à un seul compte et Région AWS. Vous pouvez déployer un maximum de 15 frameworks par compte et par région. Vous ne pouvez pas déployer de frameworks dupliqués (cadres contenant les mêmes contrôles et paramètres).

Il existe deux types différents de frameworks :

- Le framework AWS Backup (recommandé) : utilisez le framework AWS Backup pour déployer tous les contrôles disponibles afin de surveiller votre activité de sauvegarde, votre couverture et vos ressources par rapport aux bonnes pratiques que nous recommandons.
- Un framework personnalisé que vous définissez : utilisez un framework personnalisé pour choisir un ou plusieurs contrôles spécifiques et pour personnaliser les paramètres de contrôle.

Rubriques

Choix de vos contrôles

Le tableau suivant répertorie les contrôles AWS Backup Audit Manager, leurs paramètres personnalisables et leurs types de ressources AWS Config d'enregistrement. Chaque contrôle nécessite le type de ressource d'enregistrement `AWS Config: resource compliance`, car ce type enregistre votre statut de conformité.

Contrôles disponibles

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
Les ressources de sauvegarde sont protégées par un plan de sauvegarde	Évalue si les ressources de sauvegarde sont protégées par un plan de sauvegarde.	Aucun	`AWS Backup: backup selection`

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
Le plan de sauvegarde a une fréquence minimale et une rétention minimale	Évalue si la fréquence des sauvegardes est d'au moins [1 jour] et si la période de rétention est d'au moins [35 jours].	Fréquence de sauvegarde ; période de rétention	`AWS Backup: backup plans`
Les coffres-forts empêchent la suppression manuelle des points de récupération	Évalue si les coffres-forts de sauvegarde n'autorisent pas la suppression manuelle des points de restauration, sauf pour certains rôles AWS Identity and Access Management (IAM). Par défaut, il n'existe aucune exception de rôle IAM. Il n'existe pas non plus d'exception au rôle IAM lorsque vous déployez ce contrôle avec le AWS Backup framework.	Jusqu'à 5 rôles IAM permettant la suppression manuelle des points de récupération	`AWS Backup: backup vaults`
Les points de récupération sont chiffrés	Évalue si les points de récupération sont chiffrés.	Aucun	`AWS Backup: recovery points`

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
Rétention minimale établie pour le point de récupération	Évalue si la période de rétention du point de récupération est d'au moins [35 jours].	Période de rétention du point de récupération	`AWS Backup: recovery points`
Une copie de sauvegarde entre régions est planifiée	Évalue si une ressource est configurée pour créer des copies de ses sauvegardes vers une autre Région AWS.	Région AWS	`AWS Backup: backup selection`
Une copie de sauvegarde entre comptes est planifiée	Évalue si une copie de sauvegarde entre comptes est configurée pour une ressource.	AWS ID de compte	`AWS Backup: backup selection`
Les sauvegardes sont protégées par AWS Backup Vault Lock	Évalue si une ressource est configurée pour contenir des sauvegardes dans un coffre-fort de sauvegarde verrouillé.	Nombre minimum de jours de rétention ; nombre maximal de jours de rétention	`AWS Backup: backup selection`
Le dernier point de récupération a été créé	Évalue si un point de récupération a été créé dans le délai spécifié.	Valeur en heures [1 à `744`] ou en jours [1 à `31`].	`AWS Backup recovery points`

Nom du contrôle	Description du contrôle	Paramètres personnalisables	AWS Config type de ressource d'enregistrement
Temps de restauration des ressources pour atteindre l'objectif	Évalue si la tâche de tests de la restauration s'est terminée dans le délai de restauration cible	Valeur en minutes	Aucun

Pour plus d'informations sur ces contrôles, consultez Contrôles et mesures correctives.

Pour obtenir la liste des ressources AWS Backup prises en charge qui ne prennent pas en charge tous les contrôles, consultez la section AWS Backup Audit Manager du Disponibilité des fonctionnalités par ressource tableau.

> **Note**
>
> Si vous ne souhaitez utiliser aucune des commandes précédentes, vous pouvez toujours utiliser AWS Backup Audit Manager pour créer des rapports quotidiens sur vos tâches de sauvegarde, de copie et de restauration. Consultez Utilisation des rapports d'audit.

Activation du suivi des ressources

Avant de créer votre premier framework lié à la conformité, vous devez activer le suivi des ressources. Cela permet AWS Config de suivre vos AWS Backup ressources. Pour obtenir de la documentation technique sur la gestion du suivi des ressources, consultez la section Configuration à l' AWS Config aide de la console dans le guide du AWS Config développeur.

Des frais s'appliquent lorsque vous activez le suivi des ressources. Pour plus d'informations sur le suivi des ressources, la tarification et la facturation pour AWS Backup Audit Manager, consultez la section Comptage, coûts et facturation.

Rubriques

- Activation du suivi des ressources à l'aide de la console
- Activation du suivi des ressources à l'aide de l' AWS Command Line Interface (AWS CLI)

- Activation du suivi des ressources avec un modèle AWS CloudFormation

Activation du suivi des ressources à l'aide de la console

Pour activer le suivi des ressources à l'aide de la console :

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, sous Audit Manager, choisissez Cadres.
3. Activez le suivi des ressources en choisissant Gérer le suivi des ressources.
4. Choisissez Accéder aux AWS Config paramètres.
5. Choisissez Activer ou désactiver l'enregistrement.
6. Choisissez Activer l'enregistrement pour tous les types de ressources suivants ou choisissez d'activer l'enregistrement pour certains types de ressources. Consultez Contrôles et corrections d'AWS Backup Audit Manager pour savoir quels types de ressources sont requis pour vos contrôles.

   - `AWS Backup: backup plans`
   - `AWS Backup: backup vaults`
   - `AWS Backup: recovery points`
   - `AWS Backup: backup selection`

   > **Note**
   >
   > AWS Backup Audit Manager est requis `AWS Config: resource compliance` pour chaque contrôle.

7. Choisissez Fermer.
8. Attendez que la bannière bleue avec le texte Activation du suivi des ressources se transforme en bannière verte avec le texte Le suivi des ressources est activé.

Vous pouvez vérifier si vous avez activé le suivi des ressources et, dans l'affirmative, quels types de ressources vous enregistrez, à deux endroits de la AWS Backup console. Dans le volet de navigation de gauche, vous avez deux options :

- Choisissez Cadres, puis choisissez le texte sous Statut de l'enregistreur AWS Config .

- Choisissez Paramètres, puis choisissez le texte sous Statut de l'enregistreur AWS Config .

Activation du suivi des ressources à l'aide de l' AWS Command Line Interface (AWS CLI)

Si vous n'êtes pas encore inscrit AWS Config, il peut être plus rapide de le faire en utilisant le. AWS CLI

Pour activer le suivi des ressources à l'aide de l' AWS CLI :

1. Tapez la commande suivante pour déterminer si vous avez déjà activé votre enregistreur AWS Config .

```
$ aws configservice describe-configuration-recorders
```

   a. Si votre liste `ConfigurationRecorders` est vide comme ceci :

```
{
  "ConfigurationRecorders": []
}
```

      Votre enregistreur n'est pas activé. Passez à l'étape 2 pour créer votre enregistreur.

   b. Si vous avez déjà activé l'enregistrement pour toutes les ressources, votre sortie `ConfigurationRecorders` ressemblera à ceci :

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
```

```
}
```

Puisque vous avez activé toutes les ressources, vous avez déjà activé le suivi des ressources. Il n'est pas nécessaire de suivre le reste de cette procédure pour utiliser AWS Backup Audit Manager.

c. Si vos `ConfigurationRecorders` ne sont pas vides, mais que vous n'avez pas activé l'enregistrement pour toutes les ressources, ajoutez des ressources de sauvegarde à votre enregistreur existant à l'aide de la commande suivante. Passez ensuite à l'étape 3.

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

2. Créez un AWS Config enregistreur avec les types de ressources AWS Backup Audit Manager

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default, \
roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig \
--recording-group
 resourceTypes="['AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint','AWS::Config::ResourceCompliance']"
```

3. Décrivez votre AWS Config enregistreur.

```
$ aws configservice describe-configuration-recorders
```

Vérifiez qu'il possède les types de ressources AWS Backup Audit Manager en comparant votre sortie avec la sortie attendue suivante.

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

4. Créez un compartiment Amazon S3 comme destination pour stocker les fichiers AWS Config de configuration.

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. Utilisez *policy.json* pour AWS Config autoriser l'accès à votre bucket. Consultez l'exemple *policy.json* suivant.

```
$ aws s3api put-bucket-policy --bucket MyBucket --policy file://policy.json
```

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

```
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:GetBucketAcl",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketExistenceCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:ListBucket",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketDelivery",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

6. Configurez votre bucket comme canal AWS Config de distribution

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. Activer AWS Config l'enregistrement

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. Vérifiez que `"FrameworkStatus":"ACTIVE"` se trouve dans la dernière ligne de votre sortie `DescribeFramework` comme suit.

```
$ aws backup describe-framework --framework-name test --region us-east-1
```

```
{
  "FrameworkName":"test",
 "FrameworkArn":"arn:aws:backup:us-east-1:accountId:framework:test-
f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription":"",
  "FrameworkControls":[
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"35"
        },
        {
          "ParameterName":"requiredFrequencyValue",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
      "ControlInputParameters":[

      ],
```

```
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    }
  ],
  "CreationTime":1633463605.233,
  "DeploymentStatus":"COMPLETED",
  "FrameworkStatus":"ACTIVE"
}
```

Activation du suivi des ressources avec un modèle AWS CloudFormation

Pour un AWS CloudFormation modèle qui active le suivi des ressources, consultez la section Utilisation AWS Backup d'Audit Manager avec AWS CloudFormation.

Création de frameworks à l'aide de la console AWS Backup

Après avoir activé le suivi des ressources, créez un framework en suivant les étapes ci-dessous.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Cadres.
3. Choisissez Créer un cadre.

4. Pour Nom du cadre, entrez un nom unique. Ce nom de framework doit contenir entre 1 et 256 caractères, commencer par une lettre et être composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).
5. (Facultatif) Entrez une Description du cadre.
6. Dans Contrôles, vos contrôles actifs seront affichés. Par défaut, tous les contrôles éligibles à une ressource sont répertoriés.

   Pour modifier les contrôles actifs, cliquez sur Modifier les contrôles.

   a. La première case à cocher indique si le contrôle est activé. Pour désactiver un contrôle, décochez la case.

   b. Sous Choisir les ressources à évaluer, vous pouvez sélectionner le mode de sélection des ressources, soit par type, soit par balise, soit par ressource unique.

   La liste des contrôles d'AWS Backup Audit Manager décrit les options de personnalisation pour chaque contrôle.
7. (Facultatif) Balisez votre framework en choisissant Ajouter une nouvelle balise. Vous pouvez utiliser des balises pour rechercher et filtrer vos frameworks ou suivre vos coûts.
8. Choisissez Créer un cadre.

AWS Backup Audit Manager peut prendre plusieurs minutes pour créer le framework.

Si l'erreur `AlreadyExists` se produit, un framework avec les mêmes contrôles et paramètres existe déjà. Pour créer correctement un nouveau framework, au moins un contrôle ou paramètre doit être différent des frameworks existants.

Création de frameworks à l'aide de l' AWS Backup API

Le tableau suivant contient des exemples de demandes d'API pour CreateFramework pour chaque contrôle, ainsi que des exemples de réponses d'API aux demandes DescribeFramework correspondantes. Pour utiliser AWS Backup Audit Manager par programmation, vous pouvez vous référer à ces extraits de code.

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Backup resources are protected by a backup plan	{"FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] // Evaluate only RDS instances } }], "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["RDS"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control1", "FrameworkTags": {"key1": "foo"} }

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Backup plan minimum frequency and minimum retention	{"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }],	{"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": {

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	"Tags": {"key1": "prod"} } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Vaults prevent manual deletion of recovery points	{"FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"],	{"FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:r

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**

	<pre>"Complian
	ceResourceTypes":
	["AWS::Backup::Bac
	kupVault"]
	}
	}
	],
	"IdempotencyToken":
	"Control3",
	"FrameworkTags":
	{"key1": "foo"}
	}</pre>
		<pre>ole/service-role/Q
		uickSightAction"}
		],
		"ControlScope":
		{"Complia
		nceResourceIds":["
		default"],
		"Complian
		ceResourceTypes":
		["AWS::Backup::Bac
		kupVault"]
		}
		}
		],
		"CreationTime":
		1516925490,
		"DeploymentStatus":
		"Active",
		"FrameworkStatus":
		"Completed",
		"IdempotencyToken":
		"Control3",
		"FrameworkTags":
		{"key1": "foo"}
		}</pre>

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Minimum retention established for recovery point	{"FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags":

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
		<pre> {"key1": "foo"} }</pre>

Backup recovery points are encrypted	<pre>{"FrameworkName":
	 "Control5",
	 "FrameworkDescript
	ion": "This is a test
	 framework",
	 "FrameworkControls":
	  [
	  {"ControlName":
	 "BACKUP_RECOVERY_P
	OINT_ENCRYPTED",
	  "ControlInputParam
	eters":
	  [],
	  "ControlScope":
	 {} // Default scope
	 (no scope input) is all
	 recovery points
	  }
	  ],
	 "IdempotencyToken":
	 "Control5",
	 "FrameworkTags":
	  {"key1": "foo"}
	}</pre>
		<pre>{"FrameworkName":
		 "Control5",
		"FrameworkArn":
		 "arn:aws:backup:us
		-east-1:1234567890
		12:framework/Contr
		ol7-7e7655ae-1e31-
		45cb-96a0-4f43d8c1
		9642",
		 "FrameworkDescript
		ion": "This is a test
		 framework",
		  "FrameworkControls
		":
		  [
		  {"ControlName":
		 "BACKUP_RECOVERY_P
		OINT_ENCRYPTED",
		  "ControlInputParam
		eters":
		  [],
		  "ControlScope": {}
		  }
		  ],
		 "CreationTime":
		 1516925490,
		 "DeploymentStatus":
		 "Active",
		 "FrameworkStatus":
		 "Completed",
		 "IdempotencyToken":
		 "Control5",
		 "FrameworkTags":
		  {"key1": "foo"}
		}</pre>

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Cross-Region backup copy is scheduled	{"FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Cross-account backup copy is scheduled	{"FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Backups are protected by AWS Backup Vault Lock	{"FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Last recovery point was created	{"FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
Restore time for resources meet target	{"FrameworkName":"Control10", "FrameworkDescription":"This is a test framework", "FrameworkControls":[{ "ControlName":"RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[{ "ParameterName":"maxRestoreTime", "ParameterValue":"720" }], "ControlScope":{ "ComplianceResourceIds":[ ], "ComplianceResourceTypes":["DynamoDB" // Evaluates only DynamoDB databases] } }]"IdempotencyToken":"Control10", "FrameworkTags":{ "key1":"foo" }	{"FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": {"key1": "foo"} }

Contrôle	Demande d'**CreateFramework**	Réponse de **DescribeFramework**
	}	

Affichage du statut de conformité du framework

Une fois que vous avez créé un framework d'audit, il apparaît dans votre tableau Cadres. Vous pouvez consulter ce tableau en choisissant Frameworks dans le volet de navigation de gauche de la AWS Backup console. Pour consulter les résultats de l'audit de votre framework, choisissez son Nom du cadre. Vous accédez ainsi à la page Détails du cadre, qui comporte deux sections : Résumé et Contrôles.

La section Résumé répertorie les statuts suivants de gauche à droite :

- Le Statut de conformité est le statut de conformité global de votre framework d'audit, tel que déterminé par le statut de conformité de chacun de ses contrôles. Le statut de conformité de chaque contrôle est déterminé par le statut de conformité de chaque ressource qu'il évalue.

  Le statut de conformité du framework est `Compliant` si toutes les ressources concernées par vos évaluations de contrôle ont validé ces évaluations. Si une ou plusieurs ressources échouent à une évaluation de contrôle, le statut de conformité sera `Non-Compliant`. Pour en savoir plus sur comment rechercher vos ressources non conformes, consultez Recherche de ressources non conformes. Pour en savoir plus sur comment rendre vos ressources conformes, consultez la section sur les corrections dans Contrôles et corrections d'AWS Backup Audit Manager.
- Le Statut du cadre indique si vous avez activé le suivi des ressources pour toutes vos ressources. Les statuts possibles sont les suivants :
  - `Active` lorsque l'enregistrement est activé pour toutes les ressources que le framework évalue.
  - `Partially active` lorsque l'enregistrement est désactivé pour au moins une ressource que le framework évalue.
  - `Inactive` lorsque l'enregistrement est désactivé pour toutes les ressources que le framework évalue.
  - `Unavailable`lorsque AWS Backup Audit Manager n'est pas en mesure de valider le statut de l'enregistrement pour le moment.

Pour corriger un statut **`Partially active`** ou **`Inactive`**

1. Choisissez Cadres dans le volet de navigation de gauche.
2. Choisissez Gérer le suivi des ressources.
3. Suivez les instructions affichées dans la fenêtre contextuelle pour activer l'enregistrement qui n'était pas activé auparavant pour vos types de ressources.

Pour plus d'informations sur les types de ressources qui nécessitent un suivi des ressources en fonction des contrôles que vous avez inclus dans vos frameworks, consultez le composant de ressources Contrôles et corrections d'AWS Backup Audit Manager.

- Le Statut du déploiement fait référence au statut de déploiement de votre framework. Ce statut doit le plus souvent être `Completed`, mais peut également être `Create in progress`, `Update in progress`, `Delete in progress` et `Failed`.
  - Un statut `Failed` signifie que le framework ne s'est pas déployé correctement. Supprimer le cadre, puis recréez-le via la console AWS Backup ou via l'API AWS Backup.
- Les Contrôles conformes indiquent le nombre de contrôles du framework, toutes les évaluations ayant réussi.
- Les Contrôles non conformes indiquent le nombre de contrôles du framework avec au moins une évaluation ayant échoué.

La section Contrôles affiche les informations suivantes :

- Le Statut du contrôle fait référence au statut de conformité de chaque contrôle. Un contrôle peut être `Compliant`, ce qui signifie que toutes les ressources réussissent cette évaluation, `Non-compliant`, ce qui signifie qu'au moins une ressource n'a pas réussi cette évaluation, ou `Insufficient data`, ce qui signifie que le contrôle n'a trouvé aucune ressource à évaluer dans le cadre de l'évaluation.
- La Portée de l'évaluation peut limiter chaque contrôle à un ou plusieurs Types de ressources, à un ID de ressource ou à une Clé de balise et à une Valeur de balise, en fonction de la manière dont vous avez personnalisé votre contrôle lors de la création de votre framework d'audit. Si tous les champs sont vides (comme indiqué par un tiret, « - »), le contrôle évalue toutes les ressources applicables.

Recherche de ressources non conformes

AWS Backup Audit Manager vous aide à identifier les ressources non conformes de deux manières.

- Lorsque vous affichez le statut de conformité du cadre, choisissez le nom du contrôle dans la section Détails. Cela vous amène à la AWS Config console, où vous pouvez consulter la liste de vos `Non-Compliant` ressources.
- Après avoir créé un plan de rapport avec le modèle de conformité des ressources qui inclut votre framework, vous pouvez afficher votre rapport pour identifier toutes vos ressources `Non-Compliant` sur tous vos contrôles.

  En outre, votre `Resource compliance report` indique la dernière fois qu' AWS Backup Audit Manager a évalué chacun de vos contrôles.

Mise à jour de frameworks d'audit

Vous pouvez mettre à jour la description, les contrôles et les paramètres d'un framework d'audit existant.

Pour mettre à jour un framework existant

1. Dans le volet de navigation de gauche de la AWS Backup console, choisissez Frameworks.
2. Choisissez le framework que vous souhaitez modifier par son Nom du cadre.
3. Choisissez Modifier.

Suppression de frameworks d'audit

Pour supprimer un framework existant

1. Dans le volet de navigation de gauche de la AWS Backup console, choisissez Frameworks.
2. Choisissez le framework que vous souhaitez supprimer par son Nom du cadre.
3. Sélectionnez Delete (Supprimer).
4. Tapez le nom de votre framework et choisissez Supprimer le cadre.

Utilisation des rapports d'audit

AWS Backup Les rapports d'Audit Manager sont des preuves générées automatiquement de votre AWS Backup activité, telles que :

- Quelles tâches de sauvegarde ont été terminées et à quel moment
- Quelles ressources vous avez sauvegardé

Il existe deux types de rapports. Lorsque vous créez un rapport, vous en choisissez le type.

L'un d'entre eux est un rapport sur les tâches, qui indique les tâches terminées au cours des dernières 24 heures et toutes les tâches actives. Les rapports de tâches n'affichent pas un statut `completed with issues`. Pour trouver ce statut, vous pouvez filtrer les `Completed` offres d'emploi comportant un ou plusieurs messages de statut. AWS Backup n'inclura un message d'état dans le cadre du statut `Completed` d'une tâche que si le message nécessite une attention ou une action.

Le deuxième type de rapport est un rapport de conformité. Les rapports de conformité peuvent surveiller les niveaux de ressources ou les différents contrôles en vigueur.

AWS Backup Audit Manager fournit un rapport quotidien dans votre compartiment Amazon S3. Si le rapport concerne la région et le compte actuels, vous pouvez choisir de recevoir le rapport au format CSV ou JSON. Dans le cas contraire, le rapport est disponible au format CSV. Le calendrier du rapport quotidien peut fluctuer sur plusieurs heures car AWS Backup Audit Manager effectue une randomisation pour maintenir ses performances. Vous pouvez également exécuter un rapport à la demande à tout moment.

Tous les titulaires de comptes peuvent créer des rapports entre régions ; les titulaires de comptes de gestion et d'administrateur délégué peuvent également créer des rapports entre comptes.

Vous pouvez avoir un maximum de 20 plans de rapport par Compte AWS.

> **Note**
>
> Les ressources telles que RDS qui ne sont pas en mesure d'afficher des octets incrémentiels de données d'une sauvegarde spécifique afficheront 0 pour la valeur `backupSizeInBytes`.

Pour permettre à AWS Backup Audit Manager de créer des rapports quotidiens ou à la demande, vous devez d'abord créer un plan de rapport à partir d'un modèle de rapport.

Rubriques

Choix de votre modèle de rapport

Un modèle de rapport définit les informations que votre plan de rapport inclut dans votre rapport. Lorsque vous automatisez vos rapports à l'aide d'un plan de rapports, AWS Backup Audit Manager vous fournit les rapports des dernières 24 heures. AWS Backup Audit Manager crée ces rapports entre 1 h et 5 h UTC. Il propose les modèles de rapports suivants.

Modèles de rapports Backup

Modèles de rapports Backup. Ces modèles vous fournissent des mises à jour quotidiennes sur vos tâches de sauvegarde, de restauration ou de copie. Vous pouvez utiliser ces rapports pour surveiller votre position opérationnelle et identifier les échecs susceptibles de nécessiter des mesures supplémentaires. Le tableau suivant répertorie le nom de chaque modèle de rapport de sauvegarde et son exemple de sortie.

Modèle de rapport Backup	Exemple de rapport au format JSON
`BACKUP_JOB_REPORT`	`{ "reportItems": [ { "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2",`

Modèle de rapport Backup	Exemple de rapport au format JSON


```
      "backupJobId": "FCCB040A
-9426-2A49-2EA9-5EAFFAC656AC",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-
west-2:112233445566:instance/
i-0bc877aee7782ba75",
      "backupPlanArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-plan:349f2247-b48
9-4301-83ac-4b7dd724db9a",
      "backupRuleId": "ab88bbf8-
ff4e-4f1b-92e7-e13d3e65dcfb",
      "creationDate": "2021-07-
14T23:53:47.229Z",
      "completionDate": "2021-07-
15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:
ec2:us-west-2::image/ami-03
0cafb98e5a6dcdf",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 858993459
2,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

Modèle de rapport Backup	Exemple de rapport au format JSON

COPY_JOB_REPORT	{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-
	14T15:48:31Z - 2021-07-15T15:48:3
	1Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "copyJobId": "E0AD48A9-0560-B66
	8-3EF0-941FDC0AD6B1",
	      "jobStatus": "RUNNING",
	      "resourceType": "EC2",
	      "resourceArn": "arn:aws:ec2:us-
	west-2:112233445566:instance/
	i-0bc877aee7782ba75",
	      "backupPlanArn": "arn:aws:
	backup:us-west-2:1122334455
	66:backup-plan:349f2247-b48
	9-4301-83ac-4b7dd724db9a",
	      "backupRuleId": "ab88bbf8-
	ff4e-4f1b-92e7-e13d3e65dcfb",
	      "creationDate": "2021-07-
	15T15:42:04.771Z",
	      "backupSizeInBytes": 858993459
	2,
	      "sourceRecoveryPointArn":
	 "arn:aws:ec2:us-west-2::image/
	ami-007b3819f25697299",
	      "sourceBackupVaultArn":
	 "arn:aws:backup:us-west-2:1
	12233445566:backup-vault:Default",
	      "destinationRecoveryPointAr
	n": "arn:aws:ec2:us-east-2::image/
	ami-0eba2199a0bcece3c",
	      "destinationBackupVaultArn"
	: "arn:aws:backup:us-east-2:1
	12233445566:backup-vault:Default",
	      "iamRoleArn": "arn:aws:
	iam::112233445566:role/service-
	role/AWSBackupDefaultServiceRole"
	    }

Modèle de rapport Backup	Exemple de rapport au format JSON
	<pre>] }</pre>

RESTORE_JOB_REPORT	<pre>{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-
	14T15:53:30Z - 2021-07-15T15:53:3
	0Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "restoreJobId": "4CACA67D-4E12-
	DC05-6C2B-0E97D01FA41E",
	      "jobStatus": "RUNNING",
	      "recoveryPointArn": "arn:aws:
	ec2:us-west-2::image/ami-00
	201ecb57a5271ae",
	      "creationDate": "2021-07-
	15T15:52:49.797Z",
	      "backupSizeInBytes": 858993459
	2,
	      "percentDone": "0.00%",
	      "iamRoleArn": "arn:aws:
	iam::112233445566:role/service-
	role/AWSBackupDefaultServiceRole"
	    }
	  ]
	}</pre>

Modèles de rapports de conformité

Les Modèles de rapports de conformité vous offrent des rapports quotidiens sur la conformité de votre activité de sauvegarde et de vos ressources par rapport aux contrôles que vous avez définis dans un ou plusieurs de vos frameworks. Si le statut de conformité de l'un de vos frameworks est `Non-compliant`, consultez un rapport de conformité pour identifier les ressources non conformes.

Types de modèles de rapports de conformité

- `Control compliance report` vous aide à suivre le statut de conformité des contrôles que vous avez définis dans vos frameworks.
- `Resource compliance report` vous aide à suivre le statut de conformité de vos ressources par rapport aux contrôles que vous avez définis dans vos frameworks. Ces rapports incluent des résultats d'évaluation détaillés, notamment des informations d'identification sur les ressources non conformes que vous pouvez utiliser pour identifier et corriger ces ressources.

Le tableau suivant montre un exemple de sortie générée à partir d'un rapport de conformité.

Modèle de rapport de conformité	Exemple de rapport au format JSON
`CONTROL_COMPLIANCE_REPORT`	`{ "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08-17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_Hours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFramework7",`

Modèle de rapport de conformité	Exemple de rapport au format JSON


```
      "frameworkDescription": "A test
 framework",
      "controlName": "BACKUP_P
LAN_MIN_FREQUENCY_AND_MIN_R
ETENTION_CHECK",
      "controlComplianceStatus":
 "NON_COMPLIANT",
      "lastEvaluationTime": "2021-08-
17T03:21:19.995Z",
      "numResourcesCompliant": 0,
      "numResourcesNonCompliant": 25,
      "controlScope": "{Complia
nceResourceTypes: [],}",
      "controlParameters": "{\"requi
redFrequencyValue\":\"1\",\
"requiredRetentionDays\":\"35\",
\"requiredFrequencyUnit\":\"hours
\"}"
    }
  ]
}
```

Modèle de rapport de conformité	Exemple de rapport au format JSON

RESOURCE_COMPLIANCE_REPORT	{
	  "reportItems": [
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-63c74e66",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.963Z"
	    },
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-b3d7c218",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.961Z"
	    }
	  ]
	}

Création de plans de rapport à l'aide de la console AWS Backup

Il existe deux types de rapports. L'un d'entre eux est un rapport sur les tâches, qui indique les tâches terminées au cours des dernières 24 heures et toutes les tâches actives. Le deuxième type de rapport est un rapport de conformité. Les rapports de conformité peuvent surveiller les niveaux de ressources ou les différents contrôles en vigueur. Lorsque vous créez un rapport, vous choisissez le type de rapport à créer.

REMARQUE : en fonction de votre type de compte, l'affichage de la console peut varier. Seuls les comptes de gestion bénéficieront de la fonctionnalité multi-comptes.

À l'instar d'un plan de sauvegarde, vous créez un plan de rapport pour automatiser la création de vos rapports et définir leur compartiment Amazon S3 de destination. Un plan de rapport nécessite que vous disposiez d'un compartiment S3 pour recevoir vos rapports. Pour obtenir des instructions sur la configuration d'un nouveau compartiment S3, consultez Étape 1 : Créer votre premier compartiment S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour créer votre plan de rapport dans la AWS Backup console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Choisissez Créer un plan de rapport.
4. Choisissez l'un des modèles de rapport dans la liste déroulante.
5. Entrez un Nom du plan de rapport unique. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).
6. (Facultatif) Entrez une Description du plan de rapport.
7. Modèles de rapports de conformité pour un seul compte. Choisissez un ou plusieurs frameworks sur lesquels effectuer le rapport. Vous pouvez ajouter un maximum de 1 000 frameworks à un plan de rapport.
    1. Choisissez votre AWS région à l'aide de la liste déroulante.
    2. Choisissez un framework dans cette région à l'aide de la liste déroulante.
    3. Choisissez Ajouter un cadre.
8. (Facultatif) Pour ajouter des balises à votre plan de rapport, choisissez Ajouter des balises au plan de rapport.

9. Si vous utilisez un compte de gestion, vous pouvez spécifier les comptes que vous souhaitez inclure dans ce plan de rapport. Vous pouvez sélectionner Uniquement mon compte, qui générera des rapports uniquement sur le compte auquel vous êtes actuellement connecté. Vous pouvez également sélectionner Un ou plusieurs comptes dans mon organisation (disponibles pour les comptes de gestion et d'administrateur délégué).
10. (Si vous créez un rapport de conformité pour une seule région, ignorez cette étape.) Vous pouvez sélectionner les régions à inclure dans votre rapport. Cliquez sur le menu déroulant pour afficher les régions disponibles. Sélectionnez Toutes les régions disponibles ou les régions que vous préférez.

    - La case à cocher Inclure les nouvelles régions lorsqu'elles sont intégrées dans Backup Audit Manager déclenchera l'inclusion de nouvelles régions dans vos rapports lorsqu'elles seront disponibles.
11. Choisissez le Format de fichier de votre rapport. Tous les rapports peuvent être exportés au format CSV. En outre, les rapports relatifs à une seule région peuvent être exportés au format JSON.
12. Choisissez votre Nom du compartiment S3 à l'aide de la liste déroulante.
13. (Facultatif) Entrez un préfixe de compartiment.

    AWS Backup livre votre compte courant, la région actuelle rend compte às3://*your-bucket-name*/prefix/Backup/*accountID*/*Region*/year/month/day/report-name.

    AWS Backup fournit vos rapports multi-comptes à s3://*your-bucket-name*/prefix/Backup/crossaccount/*Region*/year/month/day/report-name

    AWS Backup fournit vos rapports interrégionaux à s3://*your-bucket-name*/prefix/Backup/*accountID*/crossregion/year/month/day/report-name
14. Choisissez Créer un plan de rapport.

Ensuite, vous devez autoriser votre compartiment S3 à recevoir des rapports de AWS Backup. Après avoir créé un plan de rapport, AWS Backup Audit Manager génère automatiquement une politique d'accès au compartiment S3 que vous pouvez appliquer.

Si vous chiffrez votre compartiment à l'aide d'une clé KMS personnalisée, la politique de clé KMS doit répondre aux exigences suivantes :

- L'`Principal`attribut doit inclure l'ARN `AWSServiceRolePolicyForBackupReports`du rôle lié au service Backup Audit Manager.

- L'`Action`attribut doit inclure `kms:GenerateDataKey` et `kms:Decrypt` au minimum.

La politique AWSServiceRolePolicyForBackupReportsdispose de ces autorisations.

Pour afficher et appliquer cette stratégie d'accès à votre compartiment S3

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Choisissez Modifier.
5. Choisissez Afficher la stratégie d'accès pour le compartiment S3. Vous pouvez également utiliser la politique à la fin de cette procédure.
6. Choisissez Copier les autorisations.
7. Choisissez Modifier la politique du compartiment. Notez que tant que le rapport de sauvegarde n'est pas créé pour la première fois, le rôle lié au service mentionné dans la politique du compartiment S3 n'existera pas encore, ce qui entraîne l'erreur « Principal non valide ».
8. Copiez les autorisations dans la Politique.

Exemple de politique de compartiment

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
      },
      "Action":"s3:PutObject",
      "Resource":[
        "arn:aws:s3:::BucketName/*"
      ],
      "Condition":{
```

```
        "StringEquals":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Si vous utilisez une méthode personnalisée AWS Key Management Service pour chiffrer votre compartiment S3 cible qui stocke les rapports, incluez les actions suivantes dans votre politique :

```
      "Action":[
        "kms:GenerateDataKey",
        "kms:Encrypt"
      ],
      "Resource":[
        "*"
      ],
```

Création de plans de rapports à l'aide de l' AWS Backup API

Vous pouvez également utiliser des plans de rapport par programmation.

Il existe deux types de rapports. L'un d'entre eux est un rapport sur les tâches, qui indique les tâches terminées au cours des dernières 24 heures et toutes les tâches actives. Le deuxième type de rapport est un rapport de conformité. Les rapports de conformité peuvent surveiller les niveaux de ressources ou les différents contrôles en vigueur. Lorsque vous créez un rapport, vous choisissez le type de rapport à créer.

À l'instar d'un plan de sauvegarde, vous créez un plan de rapport pour automatiser la création de vos rapports et définir leur compartiment Amazon S3 de destination. Un plan de rapport nécessite que vous disposiez d'un compartiment S3 pour recevoir vos rapports. Pour obtenir des instructions sur la configuration d'un nouveau compartiment S3, consultez Étape 1 : Créer votre premier compartiment S3 dans le Guide de l'utilisateur Amazon Simple Storage Service.

Si vous chiffrez votre compartiment à l'aide d'une clé KMS personnalisée, la politique de clé KMS doit répondre aux exigences suivantes :

- L'`Principal`attribut doit inclure l'ARN `AWSServiceRolePolicyForBackupReports`du rôle lié au service Backup Audit Manager.

- L'`Action`attribut doit inclure `kms:GenerateDataKey` et `kms:Decrypt` au minimum.

La politique AWSServiceRolePolicyForBackupReportsdispose de ces autorisations.

Pour les rapports à compte unique ou à région unique, utilisez la syntaxe suivante pour appeler CreateReportPlan.

```
{
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   "ReportSetting": {
        "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
 CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
 Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
   "ReportDeliveryChannel": {
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
 CSV if left blank.
   },
   "ReportPlanTags": {
       "string" : "string" // Optional.
   },
   "IdempotencyToken": "string"
}
```

Lorsque vous appelez DescribeReportPlan avec le nom unique d'un plan de rapport, l'API AWS Backup répond avec les informations suivantes.

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
```

```
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

Pour les rapports à comptes multiples et régions multiples, utilisez la syntaxe suivante pour appeler CreateReportPlan.

```
{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ], *//Organization report only support CSV file*
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ], // Use string value of "ROOT" to include all
 organizational units
      "OrganizationUnits": [ "string" ],
      "Regions": ["string"], // Use wildcard value in string to include all Regions
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
   }
}
```

Lorsque vous appelez DescribeReportPlan avec le nom unique d'un plan de rapport, l'API AWS Backup répond avec les informations suivantes pour les plans à comptes multiples et régions multiples :

```
{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
```

```
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts":[ "string" ],
         "OrganizationUnits":[ "string" ],
         "Regions": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "ReportTemplate": "string"
      }
   }
}
```

Création de rapports à la demande

Vous pouvez générer de nouveaux rapports à votre convenance en créant un rapport à la demande en suivant les étapes suivantes. AWS Backup Audit Manager fournit votre rapport à la demande au compartiment Amazon S3 que vous avez spécifié dans votre plan de rapport.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Choisissez Créer un rapport à la demande.

Vous pouvez générer un rapport à la demande pour un plan de rapport existant.

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Rapports sur les plans, sélectionnez un plan de rapport en cliquant sur la case d'option à côté du nom du plan de rapport.
4. Cliquez sur Actions, puis sur Créer un rapport à la demande.

Vous pouvez le faire pour plusieurs rapports, même s'ils sont en cours de génération.

Affichage des rapports d'audit

Vous pouvez ouvrir, consulter et analyser les rapports AWS Backup Audit Manager à l'aide des programmes que vous utilisez habituellement pour travailler avec des fichiers CSV ou JSON. Notez que les rapports pour plusieurs régions ou plusieurs comptes ne sont disponibles qu'au format CSV.

Les fichiers volumineux sont divisés en plusieurs rapports si la taille totale du fichier dépasse 50 Mo. Si les fichiers obtenus dépassent 50 Mo, AWS Backup Audit Manager créera des fichiers CSV supplémentaires avec le reste du rapport.

Pour afficher un rapport

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Sous Tâches du rapport, cliquez sur le lien du rapport pour afficher le rapport.
5. Si Statut du rapport est souligné en pointillé, choisissez-le pour obtenir des informations sur votre rapport.
6. Choisissez le rapport à afficher en fonction de son Heure d'achèvement.
7. Cliquez sur le lien S3. Cela ouvre votre compartiment S3 de destination.
8. Sous Nom, choisissez le nom d'un rapport que vous voulez afficher.
9. Pour enregistrer le rapport sur votre ordinateur, choisissez Télécharger.

Mise à jour des plans de rapport

Vous pouvez mettre à jour la description d'un plan de rapport existant, sa destination de livraison et son format. Le cas échéant, vous pouvez également ajouter ou supprimer des frameworks dans le plan de rapport.

Pour mettre à jour un plan de rapport existant

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Choisissez Modifier.

5. Vous pouvez modifier les détails du plan de rapport, y compris le nom et la description du rapport, ainsi que les comptes et les régions inclus dans le rapport.

Suppression de plans de rapport

Vous pouvez supprimer un plan de rapport existant. Lorsque vous supprimez un plan de rapport, tous les rapports déjà créés par ce plan de rapport restent dans leur compartiment Amazon S3 de destination.

Pour supprimer un plan de rapport existant

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, choisissez Rapports.
3. Sous Nom du plan de rapport, sélectionnez un plan de rapport en choisissant son nom.
4. Sélectionnez Delete (Supprimer).
5. Entrez le nom de votre plan de rapport, puis choisissez Supprimer le plan de rapport.

Utilisation AWS Backup d'Audit Manager avec AWS CloudFormation

Nous fournissons les exemples de AWS CloudFormation modèles suivants à titre de référence :

Rubriques

- Activation du suivi des ressources
- Déploiement des contrôles par défaut
- Exonération des rôles IAM de l'évaluation des contrôles
- Création d'un plan de rapport

Activation du suivi des ressources

Le modèle suivant active le suivi des ressources, comme décrit dans Activation du suivi des ressources.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config
```

```
Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
        default: Configuration delivery channel name
      Frequency:
        default: Snapshot delivery frequency
      TopicArn:
        default: SNS topic name
      NotificationEmail:
        default: Notification Email (optional)

Parameters:
  AllSupported:
    Type: String
    Default: True
    Description: Indicates whether to record all supported resource types.
    AllowedValues:
      - True
      - False
```

```
  IncludeGlobalResourceTypes:
    Type: String
    Default: True
    Description: Indicates whether AWS Config records all supported global resource
 types.
    AllowedValues:
      - True
      - False

  ResourceTypes:
    Type: List<String>
    Description: A list of valid AWS resource types to include in this recording group,
 such as AWS::EC2::Instance or AWS::CloudTrail::Trail.
    Default: <All>

  DeliveryChannelName:
    Type: String
    Default: <Generated>
    Description: The name of the delivery channel.

  Frequency:
    Type: String
    Default: 24hours
    Description: The frequency with which AWS Config delivers configuration snapshots.
    AllowedValues:
      - 1hour
      - 3hours
      - 6hours
      - 12hours
      - 24hours

  TopicArn:
    Type: String
    Default: <New Topic>
    Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification
 Service (Amazon SNS) topic that AWS Config delivers notifications to.

  NotificationEmail:
    Type: String
    Default: <None>
    Description: Email address for AWS Config notifications (for new topics).

Conditions:
```

```
  IsAllSupported: !Equals
    - !Ref AllSupported
    - True
  IsGeneratedDeliveryChannelName: !Equals
    - !Ref DeliveryChannelName
    - <Generated>
  CreateTopic: !Equals
    - !Ref TopicArn
    - <New Topic>
  CreateSubscription: !And
    - !Condition CreateTopic
    - !Not
      - !Equals
        - !Ref NotificationEmail
        - <None>

Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours

Resources:

  ConfigBucket:
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
      BucketEncryption:
          ServerSideEncryptionConfiguration:
            - ServerSideEncryptionByDefault:
                SSEAlgorithm: AES256

  ConfigBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AWSConfigBucketPermissionsCheck
```

```
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/
${AWS::AccountId}/*"
          - Sid: AWSConfigBucketSecureTransport
            Action:
              - s3:*
            Effect: Deny
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/*"
            Principal: "*"
            Condition:
              Bool:
                aws:SecureTransport:
                  false

  ConfigTopic:
    Condition: CreateTopic
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Sub "config-topic-${AWS::AccountId}"
      DisplayName: AWS Config Notification Topic
      KmsMasterKeyId: "alias/aws/sns"

  ConfigTopicPolicy:
    Condition: CreateTopic
    Type: AWS::SNS::TopicPolicy
    Properties:
      Topics:
        - !Ref ConfigTopic
      PolicyDocument:
```

```
        Statement:
          - Sid: AWSConfigSNSPolicy
            Action:
              - sns:Publish
            Effect: Allow
            Resource: !Ref ConfigTopic
            Principal:
              Service:
                - config.amazonaws.com

  EmailNotification:
    Condition: CreateSubscription
    Type: AWS::SNS::Subscription
    Properties:
      Endpoint: !Ref NotificationEmail
      Protocol: email
      TopicArn: !Ref ConfigTopic

  ConfigRecorderServiceRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: config.amazonaws.com
      Description: Service Role for AWS Config

  ConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    DependsOn:
      - ConfigBucketPolicy
      - ConfigRecorderServiceRole
    Properties:
      RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
      RecordingGroup:
        AllSupported: !Ref AllSupported
        IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
        ResourceTypes: !If
          - IsAllSupported
          - !Ref AWS::NoValue
          - !Ref ResourceTypes

  ConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    DependsOn:
      - ConfigBucketPolicy
```

```
    Properties:
      Name: !If
        - IsGeneratedDeliveryChannelName
        - !Ref AWS::NoValue
        - !Ref DeliveryChannelName
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: !FindInMap
          - Settings
          - FrequencyMap
          - !Ref Frequency
      S3BucketName: !Ref ConfigBucket
      SnsTopicARN: !If
        - CreateTopic
        - !Ref ConfigTopic
        - !Ref TopicArn
```

Déploiement des contrôles par défaut

Le modèle suivant crée un framework avec les contrôles par défaut décrits dans Contrôles et corrections d'AWS Backup Audit Manager.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
          ControlScope:
            Tags:
```

```
              - Key: customizedKey
                Value: customizedValue
        - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
          ControlInputParameters:
            - ParameterName: crossRegionList
              ParameterValue: 'eu-west-2'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
          ControlInputParameters:
            - ParameterName: crossAccountList
              ParameterValue: '111122223333'
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
        - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
        - ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
          ControlInputParameters:
            - ParameterName: maxRestoreTime
              ParameterValue: '720'

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

Exonération des rôles IAM de l'évaluation des contrôles

Le contrôle BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED vous permet d'exempter jusqu'à cinq rôles IAM qui peuvent toujours supprimer manuellement des points de récupération. Le modèle suivant déploie ce contrôle et exempte également deux rôles IAM.

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
          ControlInputParameters:
            - ParameterName: "principalArnList"
              ParameterValue: !Sub
 "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
ConfigRole"

Outputs:
  FrameworkArn:
```

```
    Value: !GetAtt TestFramework.FrameworkArn
```

Création d'un plan de rapport

Le modèle suivant crée un plan de rapport.

```
Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"

Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
        S3BucketName: !Ref S3BucketName
        S3KeyPrefix: !Ref S3KeyPrefix
      ReportSetting:
        ReportTemplate: !Ref ReportTemplate
        Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
        Accounts: ['123456789098']
        OrganizationUnits: ['ou-abcd-1234wxyz']
      ReportPlanTags:
        - Key: "a"
          Value: "1"
        - Key: "b"
          Value: "2"
```

```
Outputs:
  ReportPlanArn:
    Value: !GetAtt TestReportPlan.ReportPlanArn
```

Utilisation AWS Backup d'Audit Manager avec AWS Audit Manager

AWS Backup Les contrôles d'Audit Manager sont mappés aux contrôles standard prédéfinis AWS Audit Manager, ce qui vous permet d'importer les résultats de conformité de votre AWS Backup Audit Manager dans vos AWS Audit Manager rapports. Vous souhaiterez peut-être le faire pour aider un agent de la conformité, un responsable de l'audit ou un autre collègue qui rend compte des activités de sauvegarde dans le cadre de la posture de conformité globale de votre organisation.

Vous pouvez importer les résultats de conformité de vos contrôles AWS Backup Audit Manager dans vos AWS Audit Manager frameworks. AWS Audit Manager Pour permettre de collecter automatiquement des données à partir de vos contrôles AWS Backup Audit Manager, créez un contrôle personnalisé en AWS Audit Manager suivant les instructions de personnalisation d'un contrôle existant dans le Guide de l'AWS Audit Manager utilisateur. En suivant ces instructions, notez que la source de données des AWS Backup contrôles est AWS Config.

Pour obtenir la liste des AWS Backup commandes, consultez la section Choix de vos commandes.

Contrôles et mesures correctives

Cette page répertorie les contrôles disponibles pour AWS Backup Audit Manager. Vous pouvez choisir le volet d'informations approprié pour afficher la liste des contrôles et accéder à un contrôle spécifique. Pour comparer rapidement les contrôles, consultez le tableau dans Choix de vos contrôles. Pour définir des contrôles par programmation, consultez les extraits de code dans Création de cadres à l'aide de l'API AWS Backup.

Vous pouvez utiliser jusqu'à 50 contrôles par compte et par région. L'utilisation du même contrôle dans deux frameworks différents compte comme l'utilisation de deux contrôles de la limite de 50.

Cette page répertorie chaque contrôle avec les informations suivantes :

- Description. Les valeurs entre crochets (« [ ] ») sont les valeurs des paramètres par défaut.
- La ou les ressources évaluées par le contrôle.
- Les paramètres de la commande.
- Occasion où il y a perte de contrôle.

- L'étendue du contrôle, comme suit :
  - Vous pouvez spécifier Ressources par type en choisissant un ou plusieurs services pris en charge par AWS Backup.
  - Vous spécifiez une étendue des Ressources balisées avec une seule clé de balise et une valeur facultative.
  - Vous pouvez spécifier une ressource unique à l'aide de la liste déroulante Ressource unique.
- Étapes de correction pour rendre les ressources applicables conformes.

Notez que seules les ressources actives seront incluses lorsque les contrôles évalueront la conformité des ressources. Par exemple, une instance Amazon EC2 en cours d'exécution sera évaluée par le contrôle Le dernier point de récupération a été créé. Une instance EC2 à l'état arrêté ne sera pas incluse dans l'évaluation de conformité.

Les ressources de sauvegarde sont protégées par un plan de sauvegarde

Description : évalue si les ressources de sauvegarde sont protégées par un plan de sauvegarde.

Ressource : `AWS Backup: backup selection`

Paramètres : Aucun

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type (par défaut)
- Ressource unique

Correction : attribuez les ressources à un plan de sauvegarde. AWS Backup protège automatiquement vos ressources une fois que vous les avez attribuées à un plan de sauvegarde. Pour plus d'informations, consultez Affectation de ressources à un plan de sauvegarde.

Fréquence minimale du plan de sauvegarde et conservation minimale

Description : évalue si les plans de sauvegarde contiennent au moins une règle de sauvegarde dont la fréquence de sauvegarde est d'au moins [1 jour] et la période de rétention est d'au moins [35 jours].

Ressource : `AWS Backup: backup plans`

Paramètres :

- Fréquence de sauvegarde requise en nombre d'heures ou de jours.
- Période de rétention requise en jours, semaines, mois ou années. Nous recommandons une période de conservation à chaud d'au moins une semaine afin de permettre AWS Backup d'effectuer des sauvegardes incrémentielles lorsque cela est possible, en évitant des frais supplémentaires.

Se produit : modifications de configuration

Portée:

- Ressources balisées
- Ressource unique

Correction : mettez à jour un plan de sauvegarde pour modifier sa fréquence de sauvegarde, sa période de rétention ou les deux. La mise à jour de votre plan de sauvegarde modifie la période de rétention des points de récupération créés par le plan après votre mise à jour.

Les coffres-forts empêchent la suppression manuelle des points de récupération

Description : évalue si les coffres-forts de sauvegarde n'autorisent pas la suppression manuelle des points de récupération, sauf pour certains rôles IAM.

Ressource : `AWS Backup: backup vaults`

Paramètres : les Amazon Resource Names (ARN) d'un maximum de cinq rôles IAM permettaient de supprimer manuellement des points de récupération.

Se produit : modifications de configuration

Portée:

- Ressources balisées
- Ressource unique

Correction : créez ou modifiez une stratégie d'accès basée sur les ressources pour un coffre-fort de sauvegarde. Pour un exemple de politique et des instructions sur la façon de définir une stratégie d'accès au coffre-fort de sauvegarde, consultez Rejeter l'accès à la suppression de points de récupération dans un coffre-fort de sauvegarde.

Les points de récupération sont chiffrés

Description : évalue si les points de récupération sont chiffrés.

Ressource : `AWS Backup: recovery points`

Paramètres : Aucun

Se produit : modifications de configuration

Portée:

- Ressources balisées

Correction : configurez le chiffrement pour les points de récupération. La façon dont vous configurez le chiffrement pour les points de AWS Backup récupération varie en fonction du type de ressource.

Vous pouvez configurer le chiffrement pour les types de ressources qui prennent en charge AWS Backup la gestion complète lors de l'utilisation AWS Backup. Si le type de ressource ne prend pas en charge AWS Backup la gestion complète, vous devez configurer son chiffrement de sauvegarde en suivant les instructions de ce service, telles que le chiffrement Amazon EBS dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud. Pour consulter la liste des types de ressources qui prennent en charge la AWS Backup gestion complète, consultez la section « AWS Backup Gestion complète » du Disponibilité des fonctionnalités par ressource tableau.

Rétention minimale établie pour le point de récupération

Description : évalue si la période de rétention du point de récupération est d'au moins [35 jours].

Ressource : `AWS Backup: recovery points`

Paramètres : période de rétention du point de récupération requise en jours, semaines, mois ou années. Nous recommandons une période de conservation à chaud d'au moins une semaine afin de permettre AWS Backup d'effectuer des sauvegardes incrémentielles lorsque cela est possible, en évitant des frais supplémentaires.

Se produit : modifications de configuration

Portée:

- Ressources balisées

Correction : modifiez les périodes de rétention de vos points de récupération. Pour plus d'informations, consultez Modification d'une sauvegarde.

Une copie de sauvegarde entre régions est planifiée

Description : Évalue si une ressource est configurée pour créer des copies de ses sauvegardes AWS dans une autre région.

Ressource : `AWS Backup: backup selection`

Paramètres :

- Sélectionnez le Région AWS ou les endroits où la copie de sauvegarde doit se trouver (facultatif)
- Région

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

Correction : mettez à jour un plan de sauvegarde pour modifier l' Région AWS emplacement de la copie de sauvegarde.

Une copie de sauvegarde entre comptes est planifiée

Description : évalue si une ressource est configurée pour créer des copies de ses sauvegardes vers un autre compte. Vous pouvez ajouter jusqu'à 5 comptes pour que le contrôle soit évalué. Le compte de destination doit se trouver dans la même organisation que le compte source dans AWS Organizations.

Ressource : `AWS Backup: backup selection`

Paramètres :

- Sélectionnez le ou les ID de AWS compte sur lesquels la copie de sauvegarde doit exister (facultatif)
- ID de compte

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

Correction : mettez à jour un plan de sauvegarde pour modifier ou ajouter le ou les identifiants de AWS compte sur lesquels la copie doit se trouver.

Les sauvegardes sont protégées par AWS Backup Vault Lock

Description : évalue si une ressource possède des sauvegardes immuables stockées dans un coffre-fort de sauvegarde verrouillé.

Ressource : `AWS Backup: backup selection`

Paramètres :

- Entrez les jours de rétention minimum et maximum pour AWS Backup Vault Lock (facultatif)
- Nombre minimum de jours de rétention
- Nombre maximum de jours de rétention

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées

- Ressources par type
- Ressource unique

Correction : verrouillez un coffre-fort de sauvegarde pour définir son nom, modifiez ses jours de rétention minimum ou maximum, ou les deux. Peut également inclure `ChangeableForDays` pour un verrouillage de coffre-fort en mode conformité.

Le dernier point de récupération a été créé

Description : ce contrôle évalue si un point de récupération a été créé dans le délai spécifié (en jours ou en heures).

Le contrôle est conforme si un point de récupération de la ressource a été créé dans le délai spécifié. Le contrôle n'est pas conforme si aucun point de récupération n'a été créé dans le nombre de jours ou d'heures spécifié.

Ressource : `AWS Backup: recovery points`

Paramètres :

- Entrez le délai spécifié en nombres entiers, en heures ou en jours.
- Les valeurs `hours` peuvent être comprises entre `1` et `744`.
- Les valeurs `days` peuvent être comprises entre `1` et `31`.

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

Correction:

- Mettez à jour un plan de sauvegarde pour modifier le délai spécifié pour la création du point de récupération.
- En outre, vous pouvez créer une sauvegarde à la demande.

Temps de restauration des ressources pour atteindre l'objectif

Description : évalue si la restauration des ressources protégées est terminée dans le délai de restauration cible.

Ce contrôle vérifie si le temps de restauration d'une ressource donnée correspond à la durée cible. La règle est NON_COMPLIANT si la `LatestRestoreExecutionTimeMinutes` du type de ressource est supérieure à `maxRestoreTime` exprimée en minutes.

Paramètres :

- `maxRestoreTime` (en minutes)

Se produit : automatiquement toutes les 24 heures

Portée:

- Ressources balisées
- Ressources par type
- Ressource unique

> **Note**
>
> AWS Backup ne prévoit aucun accord de niveau de service (SLA) concernant la durée de restauration. Les temps de restauration peuvent varier en fonction de la charge et de la capacité du système, même pour les restaurations contenant les mêmes ressources.

Gestion AWS Backup des ressources sur plusieurs Comptes AWS

> **Note**
>
> Avant de gérer les ressources sur plusieurs Comptes AWS AWS Backup entrées, vos comptes doivent appartenir à la même organisation dans le AWS Organizations service.

Vous pouvez utiliser la fonctionnalité de gestion entre comptes AWS Backup pour gérer et surveiller vos tâches de sauvegarde, de restauration et de copie avec Comptes AWS AWS Organizations lesquelles vous les configurez. AWS Organizationsest un service qui propose une gestion basée sur des règles pour plusieurs comptes de gestion Comptes AWS à partir d'un seul compte de gestion. Elle vous permet de standardiser la façon dont vous mettez en œuvre les stratégies de sauvegarde, en réduisant simultanément les erreurs et les efforts liés aux procédures manuelles. À partir d'une vue centralisée, vous pouvez facilement identifier les ressources dans tous les comptes qui répondent aux critères qui vous intéressent.

Si vous le configurez AWS Organizations, vous pouvez le configurer AWS Backup pour surveiller les activités de tous vos comptes en un seul endroit. Vous pouvez également créer une politique de sauvegarde et l'appliquer à certains comptes faisant partie de votre organisation et consulter les activités agrégées des tâches de sauvegarde directement depuis la AWS Backup console. Cette fonctionnalité permet aux administrateurs de sauvegarde de surveiller efficacement le statut des tâches de sauvegarde pour des centaines de comptes dans l'ensemble de leur entreprise à partir d'un seul compte principal. Les Quotas AWS Organizations s'appliquent.

Par exemple, vous définissez une stratégie de sauvegarde A qui prend les sauvegardes quotidiennes de ressources spécifiques et les conserve pendant 7 jours. Vous choisissez d'appliquer la stratégie de sauvegarde A à l'ensemble de l'organisation. (Ceci signifie que chaque compte de l'organisation bénéficie de cette politique de sauvegarde, ce qui crée un plan de sauvegarde correspondant visible dans ce compte.) Ensuite, vous créez une unité d'organisation nommée Finance et vous décidez de conserver ses sauvegardes pendant seulement 30 jours. Dans ce cas, vous définissez une stratégie de sauvegarde B, qui remplace la valeur du cycle de vie, et l’attachez à cette unité d'organisation Finance. Ceci signifie que tous les comptes de l'unité d'organisation Finance bénéficient d’un nouveau plan de sauvegarde efficace qui prend les sauvegardes quotidiennes de toutes les ressources spécifiées et les conserve pendant 30 jours.

Dans cet exemple, la politique de sauvegarde A et la politique de sauvegarde B ont été fusionnées en une seule politique de sauvegarde, qui définit la politique de protection pour tous les comptes sous l'unité d'organisation nommée Finance. Tous les autres comptes de l'organisation restent protégés par la politique de sauvegarde A. La fusion est effectuée uniquement pour les politiques de sauvegarde qui partagent le même nom de plan de sauvegarde. Vous pouvez également faire coexister les stratégies A et B dans ce compte sans les fusionner. Vous pouvez utiliser des opérateurs de fusion avancés dans la vue JSON de la console uniquement. Pour plus d'informations sur la fusion des politiques, consultez Définition des politiques, syntaxe des politiques et héritage de politique dans le Guide de l'utilisateur AWS Organizations . Pour des références et des cas d'utilisation supplémentaires, consultez le blog Gérer les sauvegardes à grande échelle dans le cadre de votre AWS Organizations utilisation AWS Backup et le didacticiel vidéo Gérer les sauvegardes à grande échelle dans le cadre de votre AWS Organizations utilisation AWS Backup.

Consultez la section Disponibilité des fonctionnalités par AWS région pour savoir où la fonctionnalité de gestion multicomptes est disponible.

Pour utiliser la gestion inter-comptes, procédez comme suit :

1. Créez un compte de gestion dans le compte de gestion AWS Organizations et ajoutez-y des comptes.
2. Activez la fonctionnalité de gestion entre comptes dans. AWS Backup
3. Créez une politique de sauvegarde à appliquer à tous les utilisateurs Comptes AWS de votre compte de gestion.

   > **Note**
   >
   > Pour les plans de sauvegarde gérés par Organizations, les paramètres d’activation des ressources dans le compte de gestion remplacent les paramètres d’un compte membre, même si un ou plusieurs comptes d’administrateur délégué sont configurés. Les comptes d’administrateur délégué sont des comptes membres dotés de fonctionnalités améliorées et ne peuvent pas remplacer les paramètres comme le fait un compte de gestion.

4. Gérez les tâches de sauvegarde, de restauration et de copie dans tous vos Comptes AWS

Rubriques

- Création d'un compte de gestion dans Organizations

- Activation de la gestion entre comptes
- Administrateur délégué
- Création d'une politique de sauvegarde
- Surveillance des activités dans plusieurs Comptes AWS
- Règles d'activation des ressources
- Définition des politiques, syntaxe des politiques et héritage de politique

Création d'un compte de gestion dans Organizations

Tout d'abord, vous devez créer votre organisation et la configurer avec AWS les comptes des membres AWS Organizations.

Pour créer un compte de gestion dans AWS Organizations et ajouter des comptes

- Pour obtenir des instructions, veuillez consulter Didacticiel : Création et configuration d'une organisation dans le Guide de l'utilisateur AWS Organizations .

Activation de la gestion entre comptes

Avant de pouvoir utiliser la gestion multi-comptes dans AWS Backup, vous devez activer la fonctionnalité (c'est-à-dire l'activer). Une fois la fonctionnalité activée, vous pouvez créer des stratégies de sauvegarde qui vous permettent d'automatiser la gestion simultanée de plusieurs comptes.

Pour activer la gestion inter-comptes

1. Ouvrez le Console AWS Backup à l'adresse https://console.aws.amazon.com/backup/. Connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Dans le volet de navigation de gauche, choisissez Paramètres pour ouvrir la page de gestion inter-comptes.
3. Dans la section Stratégies de sauvegarde choisissez Activer.

   Ceci vous donne accès à tous les comptes et vous permet de créer des stratégies qui automatisent la gestion de plusieurs comptes dans votre organisation simultanément.
4. Dans la section Surveillance inter-comptes choisissez Activer.

Ceci vous permet de surveiller les activités de sauvegarde, de copie et de restauration de tous les comptes de votre organisation à partir de votre compte de gestion.

Administrateur délégué

L'administration déléguée permet aux utilisateurs assignés à un compte membre enregistré d'effectuer la plupart des tâches AWS Backup administratives de manière pratique. Vous pouvez choisir de déléguer l'administration AWS Backup à un compte membre AWS Organizations, étendant ainsi la capacité de gestion AWS Backup depuis l'extérieur du compte de gestion et à l'ensemble de l'organisation.

Par défaut, un compte de gestion est le compte utilisé pour modifier et gérer les politiques. À l'aide de la fonctionnalité d'administrateur délégué, vous pouvez déléguer ces fonctions de gestion aux comptes membres que vous désignez. À leur tour, ces comptes peuvent gérer les politiques, en plus du compte de gestion.

Une fois qu'un compte membre a été enregistré pour l'administration déléguée, il devient un compte administrateur délégué. Notez que les comptes, et non les utilisateurs, sont désignés comme administrateurs délégués.

L'activation des comptes d'administrateur délégué permet de gérer les politiques de sauvegarde, de minimiser le nombre d'utilisateurs ayant accès au compte de gestion et de permettre le suivi des tâches entre comptes.

Le tableau ci-dessous présente les fonctions du compte de gestion, les comptes délégués en tant qu'administrateurs de Backup et les comptes membres de l' AWS organisation.

> **Note**
>
> Les comptes d’administrateur délégué sont des comptes membres dotés de fonctionnalités améliorées, mais ne peuvent pas remplacer les paramètres d’activation du service d’autres comptes membres comme le fait un compte de gestion.

PRIVILÈGES	COMPTE DE GESTION	ADMINISTRATEUR DÉLÉGUÉ	COMPTE MEMBRE
Enregistrer/annuler l'enregistrement des comptes d'adminis trateurs délégués	Oui	Non	Non
Gérez les politiques de sauvegarde entre les comptes dans AWS Organizations	Oui	Oui	Non
Surveiller les tâches entre comptes	Oui	Oui	Non

Prérequis

Avant de pouvoir déléguer l'administration des sauvegardes, vous devez d'abord enregistrer au moins un compte membre dans votre AWS organisation en tant qu'administrateur délégué. Avant de pouvoir enregistrer un compte en tant qu'administrateur délégué, vous devez d'abord configurer les éléments suivants :

- AWS Organizations doit être activé et configuré avec au moins un compte membre en plus de votre compte de gestion par défaut.
- Dans la AWS Backup console, assurez-vous que les politiques de sauvegarde, la surveillance entre comptes et les fonctionnalités de sauvegarde entre comptes sont activées. Ils se trouvent sous le volet Administrateurs délégués de la AWS Backup console.
  - La surveillance entre comptes vous permet de surveiller les activités de sauvegarde sur tous les comptes de votre organisation à partir du compte de gestion, ainsi que des comptes d'administrateur délégué.
  - Facultatif : sauvegarde entre comptes, qui permet aux comptes de votre organisation de copier des sauvegardes vers d'autres comptes (pour les ressources multicomptes prises en charge par Backup).
  - Activez l'accès au service avec AWS Backup.

Deux étapes sont impliquées dans la configuration de l'administration déléguée. La première étape consiste à déléguer le suivi des tâches entre comptes. La deuxième étape consiste à déléguer la gestion des politiques de sauvegarde.

Enregistrement d'un compte membre en tant que compte administrateur délégué

Voici la première section : Utilisation de la AWS Backup console pour enregistrer un compte d'administrateur délégué afin de surveiller les tâches entre comptes. Pour déléguer AWS Backup des politiques, vous allez utiliser la console Organizations dans la section suivante.

Pour enregistrer un compte membre à l'aide de la AWS Backup console :

1. Ouvrez le Console AWS Backup à l'adresse https://console.aws.amazon.com/backup/. Connectez-vous à l’aide des informations d’identification de votre compte de gestion.
2. Sous Mon compte, dans le menu de navigation de gauche de la console, choisissez Paramètres.
3. Dans le volet Administrateur délégué, cliquez sur Enregistrer l'administrateur délégué ou Ajouter un administrateur délégué.
4. Sur la page Enregistrer l'administrateur délégué, sélectionnez le compte que vous souhaitez enregistrer, puis choisissez Enregistrer un compte.

Ce compte désigné sera désormais enregistré en tant qu'administrateur délégué, doté de privilèges administratifs lui permettant de surveiller les tâches entre les comptes de l'organisation et de consulter et de modifier les politiques (délégation de politiques). Ce compte membre ne peut pas enregistrer ou annuler l'enregistrement d'autres comptes administrateur délégué. Vous pouvez utiliser la console pour enregistrer jusqu'à 5 comptes en tant qu'administrateurs délégués.

Pour enregistrer un compte membre par programmation :

Utilisez la commande `register-delegated-administrator` de l'interface de ligne de commande. Vous pouvez spécifier les paramètres suivants dans votre demande d'interface de ligne de commande :

- `service-principal`
- `account-id`

Vous trouverez ci-dessous un exemple de demande d'interface de ligne de commande pour enregistrer un compte membre par programmation :

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Annuler l'enregistrement d'un compte membre

Utilisez la procédure suivante pour supprimer l'accès administratif AWS Backup en annulant l'enregistrement d'un compte de membre de votre AWS organisation qui avait été précédemment désigné comme administrateur délégué.

Pour annuler l'enregistrement d'un compte membre à l'aide de la console

1. Ouvrez le Console AWS Backup à l'adresse https://console.aws.amazon.com/backup/. Connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Sous Mon compte, dans le menu de navigation de gauche de la console, choisissez Paramètres.
3. Dans la section Administrateur délégué, cliquez sur Annuler l'enregistrement du compte.
4. Sélectionnez le compte ou les comptes dont vous voulez annuler l'enregistrement.
5. Dans la boîte de dialogue Annuler l'enregistrement du compte, examinez les implications en matière de sécurité, puis tapez `confirm` pour terminer l'annulation.
6. Sélectionnez `Deregister account`.

Pour annuler l'enregistrement d'un compte membre par programmation :

Utilisez la commande d'interface de ligne de commande `deregister-delegated-administrator` pour annuler l'inscription d'un compte administrateur délégué. Vous pouvez spécifier les paramètres suivants dans votre demande d'API :

- `service-principal`
- `account-id`

Vous trouverez ci-dessous un exemple de demande d'interface de ligne de commande pour annuler l'enregistrement d'un compte membre par programmation :

```
aws organizations deregister-delegated-administrator \
```

```
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Déléguez AWS Backup les politiques via AWS Organizations

Dans la AWS Organizations console, vous pouvez déléguer l'administration de plusieurs politiques, y compris les politiques de Backup.

À partir du compte de gestion connecté à la console AWS Organizations, vous pouvez créer, afficher ou supprimer une politique de délégation basée sur les ressources pour votre organisation. Pour connaître les étapes de délégation des politiques, consultez Création d'une politique de délégation basée sur les ressources dans le Guide de l'utilisateur AWS Organizations .

Création d'une politique de sauvegarde

Après avoir activé la gestion entre comptes, créez une politique de sauvegarde entre comptes à partir de votre compte de gestion.

> **Warning**
>
> Lorsque vous créez une politique avec JSON, les noms de clé dupliqués sont rejetés. Le nom de chaque clé doit être unique si plusieurs plans, règles ou sélections sont inclus dans une seule politique.

Création d'une politique de sauvegarde via la AWS Backup console

1. Dans le volet de navigation de gauche, choisissez Stratégies de sauvegarde. Sur la page Stratégies de sauvegarde, choisissez Créer des stratégies de sauvegarde.
2. Dans la section Détails, entrez un nom de stratégie de sauvegarde et fournissez une description.
3. Dans la section Détails des plans de sauvegarde, cliquez sur l'onglet Éditeur et procédez comme suit :
   a. Pour Nom du plan de sauvegarde, entrez un nom.
   b. Pour Régions, choisissez une région dans la liste.
4. Dans la section Configuration de règle de sauvegarde, choisissez Ajouter une règle de sauvegarde.

Le nombre maximum de règles par plan de sauvegarde est de 10. Si un plan contient plus de 10 règles, le plan de sauvegarde sera ignoré et aucune sauvegarde ne sera créée à partir de celui-ci.

a. Dans Nom de la règle, entrez le nom de la règle. Le nom de la règle est sensible à la casse et ne peut contenir que des caractères alphanumériques ou des traits d'union.

b. Pour Planification, choisissez une fréquence de sauvegarde dans la liste Fréquence, puis choisissez l'une des options dans Fenêtre de sauvegarde . Nous vous recommandons de choisir Utiliser la fenêtre de sauvegarde par défaut – recommandé.

5. Pour Cycle de vie, choisissez les paramètres de cycle de vie de votre choix.

6. Pour Nom du coffre de sauvegarde, entrez un nom. Il s'agit du coffre-fort de sauvegarde où les points de récupération créés par vos sauvegardes seront stockés.

   Assurez-vous que le coffre-fort de sauvegarde existe dans tous vos comptes. AWS Backup ne vérifie pas cela.

7. (facultatif) Choisissez une région de destination dans la liste si vous souhaitez que vos sauvegardes soient copiées vers une autre Région AWS, puis ajoutez des balises. Vous pouvez choisir des balises pour les points de récupération créés, quels que soient les paramètres de copie entre régions. Vous pouvez également ajouter d'autres règles.

8. Dans la section Affectation des ressources, indiquez le nom du rôle AWS Identity and Access Management (IAM). Pour utiliser le rôle AWS Backup de service, fournissez`service-role/AWSBackupDefaultServiceRole`.

   AWS Backup assume ce rôle dans chaque compte afin d'obtenir les autorisations nécessaires pour effectuer des tâches de sauvegarde et de copie, y compris les autorisations relatives aux clés de chiffrement, le cas échéant. AWS Backup utilise également ce rôle pour effectuer des suppressions du cycle de vie.

   > **Note**
   >
   > AWS Backup ne confirme pas que le rôle existe ou qu'il peut être assumé.
   > Pour les plans de sauvegarde créés par la gestion entre comptes, AWS Backup ils utiliseront les paramètres opt-in du compte de gestion et remplaceront les paramètres spécifiques aux comptes.

Pour chaque compte où vous souhaitez ajouter des politiques de sauvegarde, vous devez créer vous-même les coffres-forts et les rôles IAM.

9. Ajoutez des balises pour sélectionner les ressources que vous souhaitez sauvegarder. Le nombre maximum de balises autorisées est de 30.

   AWS Organizations La politique permet de spécifier un maximum de 30 balises si un plan de sauvegarde est créé via la politique des Organizations. Des balises supplémentaires peuvent être incluses en utilisant plusieurs affectations de ressources ou en engageant plusieurs plans de sauvegarde.

   Si le nombre de balises dépasse 30 dans la même sélection de sauvegarde, soit en modifiant la sélection existante, soit en l'utilisant`@@append`, le plan de sauvegarde deviendra invalide et sera supprimé du compte local.

10. Dans la section Paramètres avancés, choisissez Windows VSS si la ressource que vous souhaitez sauvegarder exécute Microsoft Windows sur une instance Amazon EC2. Cela vous permet d'effectuer des sauvegardes Windows VSS cohérentes avec les applications.

    Note

    AWS Backup prend actuellement en charge les sauvegardes cohérentes avec les applications des ressources exécutées uniquement sur Amazon EC2. Les types d'instances ou applications ne sont pas tous pris en charge pour les sauvegardes VSS Windows. Pour plus d'informations, consultez Création de sauvegardes Windows VSS.

11. Choisissez Ajouter un plan de sauvegarde pour l'ajouter à la stratégie, puis choisissez Créer une stratégie de sauvegarde.

    La création d'une stratégie de sauvegarde ne protège pas vos ressources tant que vous ne l'avez pas attachée aux comptes. Vous pouvez choisir le nom de votre stratégie et afficher les détails.

    Voici un exemple de AWS Organizations politique qui crée un plan de sauvegarde. Si vous activez Sauvegarde Windows VSS, vous devez ajouter des autorisations vous permettant d'effectuer des sauvegardes cohérentes avec les applications, comme indiqué dans la section `advanced_backup_settings` de la politique.

```
{
```

```
 "plans": {
   "PiiBackupPlan": {
     "regions": {
       "@@append":[
         "us-east-1",
         "eu-north-1"
       ]
     },
     "rules": {
       "Hourly": {
         "schedule_expression": {
           "@@assign": "cron(0 0/1 ? * * *)"
         },
         "start_backup_window_minutes": {
           "@@assign": "60"
         },
         "complete_backup_window_minutes": {
           "@@assign": "604800"
         },
         "target_backup_vault_name": {
           "@@assign": "FortKnox"
         },
         "recovery_point_tags": {
           "owner": {
             "tag_key": {
               "@@assign": "Owner"
             },
             "tag_value": {
               "@@assign": "Backup"
             }
           }
         },
         "lifecycle": {
           "delete_after_days": {
             "@@assign": "365"
           },
           "move_to_cold_storage_after_days": {
             "@@assign": "180"
           }
         },
         "copy_actions": {
           "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault" :
{
           "target_backup_vault_arn" : {
```

```
            "@@assign" : "arn:aws:backup:eu-north-1:$account:backup-
vault:myTargetBackupVault"  },
              "lifecycle": {
                "delete_after_days": {
                  "@@assign": "365"
                },
                "move_to_cold_storage_after_days": {
                  "@@assign": "180"
                }
              }
            }
          }
        }
      },
      "selections": {
        "tags": {
          "SelectionDataType": {
            "iam_role_arn": {
              "@@assign": "arn:aws:iam::$account:role/MyIamRole"
            },
            "tag_key": {
              "@@assign": "dataType"
            },
            "tag_value": {
              "@@assign": [
                "PII",
                "RED"
              ]
            }
          }
        }
      },
      "backup_plan_tags": {
        "stage": {
          "tag_key": {
            "@@assign": "Stage"
          },
          "tag_value": {
            "@@assign": "Beta"
          }
        }
      }
    }
  }
```

```
}
```

12. Dans la section Cibles, choisissez l'unité d’organisation ou le compte auquel vous souhaitez attacher la stratégie, puis choisissez Attacher. La stratégie peut également être ajoutée à des unités d’organisation ou comptes spécifiques.

> **Note**
>
> Assurez-vous de valider votre politique et d'inclure tous les champs obligatoires dans la stratégie. Si certaines parties de la stratégie ne sont pas valides, AWS Backup ignore ces parties, mais les parties valides de la stratégie fonctionneront comme prévu. Actuellement, AWS Backup ne valide pas l'exactitude des AWS Organizations politiques. Si vous appliquez une politique au compte de gestion et une autre à un compte membre et qu'elles entrent en conflit (par exemple, si les périodes de rétention des sauvegardes sont différentes), les deux politiques s'exécuteront sans problème (c'est-à-dire qu'elles s'appliqueront indépendamment pour chaque compte). Par exemple, si la politique du compte de gestion sauvegarde un volume Amazon EBS une fois par jour et que la politique locale sauvegarde un volume EBS une fois par semaine, les deux politiques s'exécutent.
> Si des champs obligatoires sont manquants dans la politique effective qui sera appliquée à un compte (probablement en raison de la fusion entre différentes politiques), AWS Backup n'applique pas du tout la politique au compte. Si certains paramètres ne sont pas valides, il les AWS Backup ajuste.

Quels que soient les paramètres d'opt-in d'un compte membre, dans le cadre d'un plan de sauvegarde créé à partir d'une politique de sauvegarde, les paramètres d'opt-in spécifiés dans le compte de gestion de l'organisation AWS Backup seront utilisés.

Lorsque vous attachez une stratégie à une unité d’organisation, chaque compte qui rejoint cette unité d’organisation bénéficie automatiquement de cette stratégie et chaque compte supprimé de l'unité d’organisation perd cette stratégie. Les plans de sauvegarde correspondants sont automatiquement supprimés de ce compte.

Surveillance des activités dans plusieurs Comptes AWS

Pour surveiller les tâches de sauvegarde, de copie et de restauration entre les comptes, vous devez activer la surveillance inter-comptes. Ceci vous permet de surveiller les activités de sauvegarde dans tous les comptes à partir du compte de gestion de votre organisation. Après votre inscription, toutes les tâches de votre organisation qui ont été créées après l'inscription sont visibles. Lorsque vous vous désinscrivez, AWS Backup conserve les tâches dans la vue agrégée pendant 30 jours (à partir de l'état Terminus). Les tâches créées après la désinscription ne sont pas visibles et n'affichent pas les tâches de sauvegarde nouvellement créées. Pour obtenir des instructions sur l'inscription, veuillez consulter Activation de la gestion entre comptes.

Pour surveiller plusieurs comptes

1. Ouvrez le Console AWS Backup à l'adresse https://console.aws.amazon.com/backup/. Connectez-vous à l'aide des informations d'identification de votre compte de gestion.
2. Dans le volet de navigation de gauche, choisissez Paramètres pour ouvrir la page de gestion inter-comptes.
3. Dans la section Surveillance inter-comptes choisissez Activer.

   Ceci vous permet de surveiller les activités de sauvegarde et de restauration de tous les comptes de votre organisation à partir de votre compte de gestion.
4. Dans le volet de navigation de gauche, choisissez Surveillance inter-comptes.
5. Sur la page Surveillance inter-comptes, cliquez sur l'onglet Tâches de sauvegarde, Tâches de restauration ou Tâches de copie pour afficher toutes les tâches créées dans l'ensemble de vos comptes. Vous pouvez voir chacune de ces tâches par Compte AWS identifiant, et vous pouvez voir toutes les tâches d'un compte donné.
6. Dans la zone de recherche, vous pouvez filtrer les tâches par ID de compte, Statut ou ID de tâche.

   Par exemple, vous pouvez cliquer sur l'onglet Tâches de sauvegarde et afficher toutes les tâches de sauvegarde créées dans l'ensemble de vos comptes. Vous pouvez filtrer la liste par ID de compte et afficher toutes les tâches de sauvegarde créées dans ce compte.

Règles d'activation des ressources

Si le plan de sauvegarde d'un compte membre a été créé par une politique de sauvegarde au niveau des organisations, les paramètres d' AWS Backup opt-in du compte de gestion des organisations remplaceront les paramètres d'opt-in de ce compte membre, mais uniquement pour ce plan de sauvegarde.

Si le compte membre dispose également de plans de sauvegarde locaux créés par les utilisateurs, ces plans de sauvegarde suivront les paramètres d'acceptation du compte membre, sans référence aux paramètres d'activation du compte de gestion Organizations.

Définition des politiques, syntaxe des politiques et héritage de politique

Les sujets suivants sont documentés dans le guide de AWS Organizations l'utilisateur.

- Stratégies de sauvegarde : consultez Stratégies de sauvegarde.
- Syntaxe d'une politique : consultez Syntaxe et exemples d'une stratégie de balise.
- Héritage pour les types de politique de gestion : consultez Héritage pour les types de politique de gestion.

AWS Backup et AWS CloudFormation

En général

Avec AWS CloudFormation, vous pouvez allouer et gérer vos ressources AWS de manière sûre et reproductible à l'aide de modèles que vous créez. Vous pouvez utiliser les modèles AWS CloudFormation et StackSets pour gérer vos plans de sauvegarde, vos sélections de ressources de sauvegarde et vos coffres-forts de sauvegarde. Pour plus d'informations sur AWS CloudFormation, consultez Fonctionnement d'AWS CloudFormation dans Guide de l'utilisateur AWS CloudFormation.

Avant de créer votre pile AWS CloudFormation ou StackSet, tenez compte des éléments suivants :

- Créez des modèles distincts pour vos plans de sauvegarde et vos coffres-forts de sauvegarde. Vous ne pouvez supprimer que des coffres-forts de sauvegarde vides. Vous ne pouvez pas supprimer une pile qui inclut des coffres-forts de sauvegarde s'ils contiennent des points de récupération.
- Vérifiez que vous disposez d'une fonction du service disponible avant de créer votre pile. Le rôle de service AWS Backup par défaut est créé pour vous la première fois que vous affectez des ressources à un plan de sauvegarde. Si vous n'avez pas attribué de ressources à votre plan de sauvegarde, faites-le avant de créer votre pile. Vous pouvez également spécifier un rôle personnalisé que vous créez. Pour plus d'informations sur les rôles , consultez Fonctions du service IAM.

Déploiement d'un coffre-fort de sauvegarde, d'un plan de sauvegarde et d'attribution de ressources avec AWS CloudFormation

Pour des exemples de modèles AWS CloudFormation qui déploient un coffre-fort de sauvegarde, des plans de sauvegarde et une attribution de ressources, consultez Affectation de ressources à l'aide de AWS CloudFormation.

Déploiement de plans de sauvegarde avec AWS CloudFormation

Pour des exemples de modèles AWS CloudFormation qui déploient des plans de sauvegarde, consultez Modèles AWS CloudFormation de plans de sauvegarde.

Déploiement de frameworks AWS Backup Audit Manager et de plans de rapports avec AWS CloudFormation

Pour des exemples de modèles AWS CloudFormation qui déploient des frameworks AWS Backup Audit Manager et des plans de rapports, consultez Modèles AWS CloudFormation de plans de sauvegarde.

Déploiement de plans de sauvegarde entre comptes avec AWS CloudFormation

Vous pouvez utiliser AWS CloudFormation StackSets sur plusieurs comptes dans une AWS organisation. Des exemples de modèles sont disponibles dans le Guide de l'utilisateur AWS CloudFormation.

La publication Automatiser la sauvegarde centralisée à grande échelle pour les services AWS avec AWS Backup constitue un excellent point de départ et une excellente référence. Avec Ibukun Oyewumi et Sabith Venkitachalapathy (juillet 2021).

En savoir plus sur AWS CloudFormation

Pour plus d'informations sur l'utilisation d'AWS CloudFormation avec AWS Backup, consultez Référence des types de ressources AWS Backup dans le Guide de l'utilisateur AWS CloudFormation.

Pour plus d'informations sur le contrôle de l'accès aux ressources de services AWS lors de l'utilisation d'AWS CloudFormation, consultez Contrôler l'accès avec AWS Identity and Access Management dans le Guide de l'utilisateur AWS CloudFormation.

Sécurité dans AWS Backup

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

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- 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 conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Backup, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud : votre responsabilité pour AWS Backup inclut, sans toutefois s'y limiter, les éléments suivants. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation, et la législation et la réglementation applicables.
  - Répondre aux communications que vous recevez de AWS.
  - Gestion des informations d'identification que vous et votre équipe utilisez. Pour plus d'informations, consultez la section Gestion des identités et des accès dans AWS Backup.
  - Configuration de vos plans de sauvegarde et attributions de ressources pour refléter les politiques de protection des données de votre organisation. Pour plus d'informations, consultez Gestion des plans de sauvegarde.
  - Tester régulièrement votre capacité à trouver certains points de récupération et à les restaurer. Pour plus d'informations, consultez la page Utilisation des sauvegardes.
  - Intégrer AWS Backup des procédures dans les procédures écrites de reprise après sinistre et de continuité des activités de votre organisation. Pour un point de départ, consultez Mise en route avec AWS Backup.
  - Assurez-vous que vos employés connaissent et se sont entraînés à utiliser AWS Backup les procédures de votre organisation en cas d'urgence. Pour plus d'informations, consultez le Cadre AWS Well-Architected.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Backup. Les rubriques suivantes expliquent comment procéder

à la configuration AWS Backup pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Backup ressources.

Rubriques

Validation de conformité pour AWS Backup

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 :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — Ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- 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 décrivent 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, telles que la norme PCI DSS, 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.

Protection des données dans AWS Backup

AWS Backup est conforme au modèle de responsabilité AWS partagée, qui inclut des réglementations et des directives pour la protection des données. AWS est chargé de protéger

l'infrastructure mondiale qui gère tous les AWS services. AWS conserve le contrôle des données hébergées sur cette infrastructure, y compris les contrôles de configuration de sécurité pour le traitement du contenu client et des données personnelles. AWS les clients et les AWS partenaires du réseau de partenaires (APN), agissant en tant que responsables du traitement des données ou en tant que sous-traitants, sont responsables de toutes les données personnelles qu'ils saisissent dans le AWS Cloud.

Pour des raisons de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer des comptes utilisateur individuels avec AWS Identity and Access Management (IAM). Cela permet de garantir que chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour les besoins de 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 (Secure Sockets Layer) ou TLS (Transport Layer Security) pour communiquer avec les ressources AWS .
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.

Nous vous recommandons vivement de ne jamais placer d’informations identifiables sensibles, telles que les numéros de compte de vos clients, dans des champs de formulaire comme Nom. Cela inclut lorsque vous travaillez avec AWS Backup ou avec d'autres AWS services à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans AWS Backup ou d'autres services peuvent être récupérées pour être insérées dans des journaux de diagnostic. Lorsque vous fournissez une URL à un serveur externe, n’incluez pas les informations d’identification non chiffrées dans l’URL pour valider votre demande adressée au serveur.

Pour en savoir plus sur la protection des données, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD sur le Blog sur la sécurité d’AWS .

Chiffrement pour les sauvegardes dans AWS Backup

> **Note**
>
> AWS Backup Audit Manager vous aide à détecter automatiquement les sauvegardes non chiffrées.

Vous pouvez configurer le chiffrement pour les types de ressources qui prennent en charge AWS Backup la gestion complète lors de l'utilisation AWS Backup. Si le type de ressource ne prend pas en charge AWS Backup la gestion complète, vous devez configurer son chiffrement de sauvegarde en suivant les instructions de ce service, telles que le chiffrement Amazon EBS dans le guide de l'utilisateur d'Amazon Elastic Compute Cloud. Pour consulter la liste des types de ressources qui prennent en charge la AWS Backup gestion complète, consultez la section « AWS Backup Gestion complète » du Disponibilité des fonctionnalités par ressource tableau.

Le tableau suivant répertorie chaque type de ressource pris en charge. Il indique également la façon dont le chiffrement est configuré pour les sauvegardes et si un chiffrement indépendant est pris en charge pour les sauvegardes. Lorsqu' AWS Backup chiffre une sauvegarde de manière indépendante, il utilise l'algorithme de chiffrement AES-256 standard.

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Simple Storage Service (Amazon S3)	Les sauvegardes Amazon S3 sont chiffrées à l'aide d'une clé AWS KMS (AWS Key Management Service) associée au coffre de sauvegarde. La clé AWS KMS peut être une clé CMK gérée par le client ou une clé CMK AWS gérée associée au service. AWS Backup AWS Backup chiffre toutes les sauvegardes même si les compartiments Amazon S3 source ne sont pas chiffrés.	Pris en charge
Machines virtuelles VMware	Les sauvegardes de machines virtuelles sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes de machines virtuelles est configurée dans	Pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
	le AWS Backup coffre dans lequel les sauvegardes de machines virtuelles sont stockées.	
Amazon DynamoDB après avoir activé Sauvegarde DynamoDB avancée	Les sauvegardes DynamoDB sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes DynamoDB est configurée dans AWS Backup le coffre dans lequel les sauvegardes DynamoDB sont stockées.	Pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon DynamoDB sans avoir activé Sauvegarde DynamoDB avancée	Les sauvegardes DynamoDB sont automatiquement chiffrées avec la même clé de chiffrement que celle utilisée pour chiffrer la table DynamoDB source. Les instantanés de tables DynamoDB non chiffrés ne sont pas chiffrés non plus. **Note** AWS Backup Pour créer une sauvegarde d'une table DynamoDB chiffrée, vous devez ajouter les `kms:Decrypt` autorisations `kms:GenerateDataKey` et le rôle IAM utilisé pour la sauvegarde. Vous pouvez également utiliser le rôle de service AWS Backup par défaut.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Elastic File System (Amazon EFS)	Les sauvegardes Amazon EFS sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes Amazon EFS est configurée dans le AWS Backup coffre dans lequel les sauvegardes Amazon EFS sont stockées.	Pris en charge
Amazon Elastic Block Store (Amazon EBS)	Par défaut, les sauvegard es Amazon EBS sont soit chiffrées à l'aide de la clé utilisée pour chiffrer le volume source, soit elles ne sont pas chiffrées. Pendant la restaurat ion, vous pouvez choisir de remplacer la méthode de chiffrement par défaut en spécifiant une clé KMS.	Non pris en charge
AMI Amazon Elastic Compute Cloud (Amazon EC2)	Les AMI ne sont pas chiffrées . Les instantanés EBS sont chiffrés selon les règles de chiffrement par défaut pour les sauvegardes EBS (voir l'entrée relative à EBS). Les instantanés EBS des données et des volumes racines peuvent être chiffrés et attachés à une AMI.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Relational Database Service (Amazon RDS)	Les instantanés Amazon RDS sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer la base de données Amazon RDS source. Les instantanés de bases de données Amazon RDS non chiffrés ne sont pas chiffrés non plus. **Note** AWS Backup prend actuellement en charge tous les moteurs de base de données Amazon RDS, y compris Amazon Aurora.	Non pris en charge
Amazon Aurora	Les instantanés de cluster Aurora sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le cluster Amazon Aurora source. Les instantanés de clusters Aurora non chiffrés ne sont pas chiffrés.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
AWS Storage Gateway	Les instantanés Storage Gateway sont automatiq uement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le volume Storage Gateway source. Les instantanés de volumes Storage Gateway non chiffrés ne sont pas chiffrés non plus. **Note** Vous n'avez pas besoin d'utiliser une clé gérée par le client pour tous les services pour activer Storage Gateway. Il vous suffit de copier la sauvegard e Storage Gateway dans un coffre-fort qui a configuré une clé KMS. Cela est dû au fait que Storage Gateway ne possède pas de clé AWS KMS gérée spécifique au service.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon FSx	Les fonctionnalités de chiffrement des systèmes de fichiers Amazon FSx varient en fonction du système de fichiers sous-jacent. Pour en savoir plus sur votre système de fichiers Amazon FSx en particulier, consultez le Guide de l'utilisateur FSx.approprié.	Non pris en charge
Amazon DocumentDB	Les instantanés de cluster Amazon DocumentDB sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le cluster Amazon DocumentDB source. Les instantanés de clusters Amazon DocumentDB non chiffrés ne sont pas chiffrés.	Non pris en charge
Amazon Neptune	Les instantanés de cluster Neptune sont automatiquement chiffrés avec la même clé de chiffrement que celle utilisée pour chiffrer le cluster Neptune source. Les instantanés de clusters Neptune non chiffrés ne sont pas chiffrés.	Non pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Amazon Timestream	Les sauvegardes d'instant anés de la table Timestream sont toujours chiffrées. La clé de chiffrement AWS KMS pour les sauvegardes Timestrea m est configurée dans le coffre-fort de sauvegarde dans lequel les sauvegardes Timestream sont stockées.	Pris en charge
Amazon Redshift	Les clusters Amazon Redshift sont automatiquement chiffrés avec la même clé de chiffreme nt que celle utilisée pour chiffrer le cluster Amazon Redshift source. Les instantan és de clusters Amazon Redshift non chiffrés ne sont pas chiffrés.	Non pris en charge
AWS CloudFormation	CloudFormation les sauvegard es sont toujours cryptées. La clé de CloudForm ation chiffrement pour les CloudFormation sauvegard es est configurée dans le CloudFormation coffre dans lequel les CloudFormation sauvegardes sont stockées.	Pris en charge

Type de ressource	Configuration du chiffrement	AWS Backup Chiffrement indépendant
Bases de données SAP HANA sur des instances Amazon EC2	Les sauvegardes de base de données SAP HANA sont toujours chiffrées. La clé de AWS KMS chiffrement pour les sauvegardes de base de données SAP HANA est configurée dans le AWS Backup coffre dans lequel les sauvegardes de base de données sont stockées.	Pris en charge

Chiffrement des copies de sauvegarde

Lorsque vous copiez vos sauvegardes sur plusieurs comptes ou régions, les copies sont AWS Backup automatiquement chiffrées pour la plupart des types de ressources, même si la sauvegarde d'origine n'est pas chiffrée. AWS Backup AWS Backup chiffre votre copie à l'aide de la clé KMS du coffre-fort cible. Toutefois, les instantanés de clusters Aurora, Amazon DocumentDB et Neptune non chiffrés sont également déchiffrés.

Chiffrement et copies de sauvegarde

La copie entre comptes avec des clés KMS AWS gérées n'est pas prise en charge pour les ressources qui ne sont pas entièrement gérées par AWS Backup. Reportez-vous AWS Backup Gestion complète à pour déterminer quelles ressources sont entièrement gérées.

Pour les ressources entièrement gérées par AWS Backup, les sauvegardes sont chiffrées à l'aide de la clé de chiffrement du coffre-fort de sauvegarde. Pour les ressources qui ne sont pas entièrement gérées par AWS Backup, les copies entre comptes utilisent la même clé KMS que la ressource source. Pour plus d’informations, consultez Clés de chiffrement et copies entre comptes.

Chiffrement des informations d'identification de l'hyperviseur de machine virtuelle

Les machines virtuelles gérées par un hyperviseur utilisent AWS Backup Gateway pour connecter les systèmes sur site à AWS Backup. Il est important que les hyperviseurs disposent de la même

sécurité robuste et fiable. Cette sécurité peut être obtenue en chiffrant l'hyperviseur, soit à l'aide de clés AWS détenues, soit à l'aide de clés gérées par le client.

AWS clés détenues et gérées par le client

AWS Backup fournit le chiffrement des informations d'identification de l'hyperviseur afin de protéger les informations de connexion sensibles des clients à l'aide de clés de chiffrement AWS détenues. Vous avez la possibilité d'utiliser des clés gérées par le client à la place.

Par défaut, les clés utilisées pour chiffrer les informations d'identification dans votre hyperviseur sont des clés AWS détenues. AWS Backup utilise ces clés pour chiffrer automatiquement les informations d'identification de l'hyperviseur. Vous ne pouvez ni consulter, ni gérer, ni utiliser AWS les clés que vous possédez, ni auditer leur utilisation. Toutefois, vous n'avez pas besoin de prendre de mesure ou de modifier les programmes pour protéger les clés qui chiffrent vos données. Pour plus d'informations, consultez la section sur les clés AWS détenues dans le Guide du AWS KMS développeur.

Les informations d'identification peuvent également être chiffrées à l'aide de clés gérées par le client. AWS Backup prend en charge l'utilisation de clés symétriques gérées par le client que vous créez, possédez et gérez pour effectuer votre chiffrement. Étant donné que vous avez le contrôle total de ce chiffrement, vous pouvez effectuer les tâches suivantes :

- Établissement et gestion des stratégies de clé
- Établissement et gestion des politiques IAM et des octrois
- Activation et désactivation des stratégies de clé
- Rotation des matériaux de chiffrement de clé
- Ajout de balises
- Création d'alias de clé
- Planification des clés pour la suppression

Lorsque vous utilisez une clé gérée par le client, AWS Backup vérifie si votre rôle est autorisé à déchiffrer à l'aide de cette clé (avant l'exécution d'une tâche de sauvegarde ou de restauration). Vous devez ajouter l'action `kms:Decrypt` au rôle utilisé pour démarrer une tâche de sauvegarde ou de restauration.

Comme l'action `kms:Decrypt` ne peut pas être ajoutée au rôle de sauvegarde par défaut, vous devez utiliser un rôle autre que le rôle de sauvegarde par défaut pour utiliser les clés gérées par le client.

Pour plus d'informations, consultez Clés gérées par le client dans le Manuel du développeur AWS Key Management Service .

Octroi requis lors de l'utilisation des clés gérées par le client

AWS KMS nécessite une autorisation pour utiliser votre clé gérée par le client. Lorsque vous importez une configuration d'hyperviseur chiffrée à l'aide d'une clé gérée par le client, AWS Backup vous créez une autorisation en votre nom en envoyant une `CreateGrant`demande à AWS KMS. AWS Backup utilise des autorisations pour accéder à une clé KMS dans un compte client.

Vous pouvez révoquer l'accès à l'autorisation ou supprimer AWS Backup l'accès à la clé gérée par le client à tout moment. Dans ce cas, toutes les passerelles associées à votre hyperviseur ne pourront plus accéder au nom d'utilisateur et au mot de passe de l'hyperviseur chiffrés par la clé gérée par le client, ce qui affectera vos tâches de sauvegarde et de restauration. Plus précisément, les tâches de sauvegarde et de restauration que vous effectuez sur les machines virtuelles de cet hyperviseur échoueront.

Backup gateway utilise cette opération `RetireGrant` pour supprimer un octroi lorsque vous supprimez un hyperviseur.

Surveillance des clés de chiffrement

Lorsque vous utilisez une clé gérée par le AWS KMS client avec vos AWS Backup ressources, vous pouvez utiliser AWS CloudTrailAmazon CloudWatch Logs pour suivre les demandes AWS Backup envoyées à AWS KMS.

Recherchez les AWS CloudTrail événements contenant les `"eventName"` champs suivants pour surveiller les AWS KMS opérations appelées pour accéder AWS Backup aux données chiffrées par votre clé gérée par le client :

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

Gestion des identités et des accès dans AWS Backup

L'accès à AWS Backup nécessite des informations d'identification. Ces informations d'identification doivent être autorisées à accéder aux ressources AWS , par exemple une base de données Amazon DynamoDB ou un système de fichiers Amazon EFS. De plus, les points de récupération créés par AWS Backup certains services AWS Backup pris en charge ne peuvent pas être supprimés à l'aide du service source (tel qu'Amazon EFS). Vous pouvez supprimer ces points de récupération à l'aide de AWS Backup.

Les sections suivantes fournissent des détails sur la façon dont vous pouvez utiliser AWS Identity and Access Management (IAM) et AWS Backup pour sécuriser l'accès à vos ressources.

> **Warning**
>
> AWS Backup utilise le même rôle IAM que celui que vous avez choisi lors de l'attribution des ressources pour gérer le cycle de vie de votre point de restauration. Si vous supprimez ou modifiez ce rôle, vous AWS Backup ne pouvez pas gérer le cycle de vie de votre point de restauration. Dans ce cas, il tentera d'utiliser un rôle lié à un service pour gérer votre cycle de vie. Dans un faible pourcentage de cas, cela peut également ne pas fonctionner, laissant des points de récupération `EXPIRED` sur votre stockage, ce qui peut entraîner des coûts indésirables. Pour supprimer des points de récupération `EXPIRED`, supprimez-les manuellement à l'aide de la procédure décrite dans Suppression des sauvegardes.

Rubriques

Authentification

L'accès aux services que vous sauvegardez AWS Backup ou AWS aux services que vous sauvegardez nécessite des informations d'identification qui AWS peuvent être utilisées pour authentifier vos demandes. Vous pouvez y accéder AWS sous l'un des types d'identités suivants :

- Compte AWS utilisateur root — Lorsque vous vous inscrivez AWS, vous fournissez une adresse e-mail et un mot de passe associés à votre AWS compte. Il s'agit de votre utilisateur root du Compte AWS . Ses informations d'identification fournissent un accès complet à toutes vos AWS ressources.

  > **Important**
  >
  > Pour des raisons de sécurité, nous vous conseillons d'utiliser les informations d'utilisateur racine uniquement pour créer un administrateur. L'administrateur est un utilisateur IAM disposant des autorisations complètes sur votre Compte AWS. Vous pouvez ensuite utiliser cet utilisateur administrateur pour créer d'autres rôles et utilisateurs IAM dotés d'autorisations limitées. Pour plus d'informations, consultez Bonnes pratiques IAM et Création de votre premier utilisateur administrateur et groupe IAM dans le Guide de l'utilisateur IAM.

- Utilisateur IAM : un utilisateur IAM est une identité au sein de votre Compte AWS qui dispose d'autorisations personnalisées spécifiques (par exemple, des autorisations pour créer un coffre-fort de sauvegarde dans lequel stocker vos sauvegardes). Vous pouvez utiliser un nom d'utilisateur et un mot de passe IAM pour vous connecter à des AWS pages Web sécurisées telles que AWS Management Consoleles forums de AWS discussion ou le AWS Support centre.

  En plus de générer un nom utilisateur et un mot de passe, vous pouvez générer des clés d'accès pour chaque utilisateur. Vous pouvez utiliser ces clés lorsque vous accédez aux AWS services par programmation, soit par le biais de l'un des nombreux SDK, soit à l'aide de la (AWS Command Line Interface CLI AWS). Les outils AWS CLI et les SDK utilisent les clés d'accès pour signer de façon cryptographique votre demande. Si vous n'utilisez pas les outils AWS , vous devez signer la demande vous-même. Pour plus d'informations sur l'authentification des demandes, consultez Processus de signature Signature Version 4 dans le document Références générales AWS.

- Rôle IAM : un rôle IAM est une autre identité IAM que vous pouvez créer dans votre compte et qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'un utilisateur IAM, mais ce rôle n'est pas associé à une personne en particulier. Un rôle IAM vous permet d'obtenir des clés

d'accès temporaires qui peuvent être utilisées pour accéder aux AWS services et aux ressources. Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : au lieu de créer un utilisateur IAM, vous pouvez utiliser des identités utilisateur préexistantes provenant du AWS Directory Service répertoire des utilisateurs de votre entreprise ou d'un fournisseur d'identité Web. On parle alors d'utilisateurs fédérés. AWS attribue un rôle à un utilisateur fédéré lorsque l'accès est demandé via un fournisseur d'identité. Pour plus d'informations sur les utilisateurs fédérés, consultez Utilisateurs fédérés et rôles dans le Guide de l'utilisateur IAM.
- Administration entre comptes : vous pouvez utiliser un rôle IAM dans votre compte pour accorder d'autres Compte AWS autorisations afin d'administrer les ressources de votre compte. À titre d'exemple, voir Tutoriel : accès délégué à Comptes AWS l'aide de rôles IAM dans le guide de l'utilisateur IAM.
- AWS accès au service : vous pouvez utiliser un rôle IAM dans votre compte pour accorder à un AWS service l'autorisation d'accéder aux ressources de votre compte. Pour plus d'informations, consultez la section Création d'un rôle pour déléguer des autorisations à un AWS service dans le guide de l'utilisateur IAM.
- Applications exécutées sur Amazon Elastic Compute Cloud (Amazon EC2) : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires des applications exécutées sur une instance Amazon EC2 et effectuant des demandes d'API. AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Contrôle d'accès

Vous pouvez disposer d'informations d'identification valides pour authentifier vos demandes, mais si vous ne disposez pas des autorisations appropriées, vous ne pouvez pas accéder aux AWS Backup ressources telles que les coffres-forts de sauvegarde. Vous ne pouvez pas non plus sauvegarder AWS des ressources telles que les volumes Amazon Elastic Block Store (Amazon EBS).

Chaque AWS ressource appartient à un Compte AWS, et les autorisations de création ou d'accès à une ressource sont régies par des politiques d'autorisation. Un administrateur de compte peut associer des politiques d'autorisation aux identités AWS Identity and Access Management (IAM) (c'est-à-dire aux utilisateurs, aux groupes et aux rôles). Certains services prennent également en charge l'attachement de stratégies d'autorisation aux ressources.

> **Note**
>
> Un administrateur de compte (ou utilisateur administrateur) est un utilisateur doté d'autorisations d'administrateur. Pour plus d'informations, consultez Bonnes pratiques IAM dans le Guide de l'utilisateur IAM.

Lorsque vous accordez des autorisations, vous décidez qui doit les obtenir, à quelles ressources ces autorisations s'appliquent et les actions spécifiques que vous souhaitez autoriser sur ces ressources.

Les sections suivantes expliquent le fonctionnement des stratégies d'accès et leur utilisation pour protéger vos sauvegardes.

Rubriques

Ressources et opérations

Une ressource est un objet qui existe au sein d'un service. AWS Backup les ressources incluent les plans de sauvegarde, les coffres-forts de sauvegarde et les sauvegardes. Backup est un terme général qui fait référence aux différents types de ressources de sauvegarde qui existent dans AWS. Par exemple, les instantanés Amazon EBS, les instantanés Amazon Relational Database Service (Amazon RDS) et les sauvegardes Amazon DynamoDB sont tous des types de ressources de sauvegarde.

Dans AWS Backup, les sauvegardes sont également appelées points de restauration. Lors de l'utilisation AWS Backup, vous travaillez également avec les ressources d'autres AWS services que vous essayez de protéger, tels que les volumes Amazon EBS ou les tables DynamoDB. Des noms Amazon Resource Name (ARN) uniques sont associés à ces ressources. Les ARN identifient les AWS ressources de manière unique. Vous devez disposer d'un ARN pour spécifier une ressource sans aucune ambiguïté au sein d' AWS, par exemple dans les politiques IAM ou les appels d'API.

Le tableau suivant répertorie les ressources, les sous-ressources, le format ARN et un exemple d'ID unique.

AWS Backup ARN des ressources

Type de ressource	Format ARN	Exemple d'ID unique
Plan de sauvegarde	`arn:aws:backup:` *`region`*`:`*`account-id`*`:backup-plan:*`	
Coffre-fort de sauvegarde	`arn:aws:backup:` *`region`*`:`*`account-id`*`:backup-vault:*`	
Point de récupération pour Amazon EBS	`arn:aws:ec2:` *`region`*`::snapshot/*`	`snapshot/snap-05f426fd8kdjb4224`
Point de récupération pour les images Amazon EC2	`arn:aws:ec2:` *`region`*`::image/ami-*`	`image/ami-1a2b3e4f5e6f7g890`
Point de récupération pour Amazon RDS	`arn:aws:rds:` *`region`*`:`*`account-id`*`:snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Point de récupération pour Aurora	`arn:aws:rds:` *`region`*`:`*`account-id`*`:cluster-snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`

Type de ressource	Format ARN	Exemple d'ID unique
Point de récupération pour Storage Gateway	`arn:aws:ec2:` *region*`::snapshot/*`	`snapshot/snap-0d40e49137e31d9e0`
Point de récupération pour DynamoDB sans Sauvegarde DynamoDB avancée	`arn:aws:dynamodb:` *region*`:`*account-id*`:table/*/backup/*`	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`
Point de récupération pour DynamoDB avec Sauvegarde DynamoDB avancée activé	`arn:aws:backup:` *region*`:`*account-id*`:recovery-point:*`	`12a34a56-7bb8-901c-cd23-4567d8e9ef01`
Point de récupération pour Amazon EFS	`arn:aws:backup:` *region*`:`*account-id*`:recovery-point:*`	`d99699e7-e183-477e-bfcd-ccb1c6e5455e`
Point de récupération pour Amazon FSx	`arn:aws:fsx:` *region*`:`*account-id*`:backup/backup-*`	`backup/backup-1a20e49137e31d9e0`
Point de récupération pour une machine virtuelle	`arn:aws:backup:` *region*`:`*account-id*`:recovery-point:*`	`1801234a-5b6b-7dc8-8032-836f7ffc623b`
Point de récupération pour la sauvegarde continue Amazon S3	`arn:aws:backup:` *region*`:`*account-id*`:recovery-point:*`	*my-bucket* `-5ec207d0`
Point de récupération pour la sauvegarde périodique S3	`arn:aws:backup:` *region*`:`*account-id*`:recovery-point:*`	*my-bucket* `-20211231900000-5ec207d0`
Point de récupération pour Amazon DocumentDB	`arn:aws:rds:` *region*`:`*account-id*`:cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`

Type de ressource	Format ARN	Exemple d'ID unique
Point de reprise pour Neptune	`arn:aws:rds: region:account-id :cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Point de reprise pour Amazon Redshift	`arn:aws:redshift: region:account-id :snapshot : resource/awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Point de récupération pour Amazon Timestream	`arn:aws:backup: region:account-id :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta`
Point de récupération pour le AWS CloudFormation modèle	`arn:aws:backup: region:account-id :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`
Point de récupération pour la base de données SAP HANA sur une instance Amazon EC2	`arn:aws:backup: region:account-id :recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`

Les ressources qui prennent en charge AWS Backup la gestion complète comportent toutes des points de récupération au format`arn:aws:backup:region:account-id:`:recovery-point:*, ce qui vous permet d'appliquer plus facilement des politiques d'autorisation pour protéger ces points de récupération. Pour savoir quelles ressources prennent en charge AWS Backup la gestion complète, consultez cette section du Disponibilité des fonctionnalités par ressource tableau.

AWS Backup fournit un ensemble d'opérations permettant de travailler avec AWS Backup les ressources. Pour obtenir la liste des opérations disponibles, consultez AWS Backup Actions.

Propriété des ressources

Il Compte AWS est propriétaire des ressources créées dans le compte, quelle que soit la personne qui les a créées. Plus précisément, le propriétaire Compte AWS de la ressource est l'entité principale (c'est-à-dire l'utilisateur Compte AWS root, un utilisateur IAM ou un rôle IAM) qui authentifie la demande de création de ressource. Les exemples suivants illustrent comment cela fonctionne :

- Si vous utilisez les informations d'identification de l'utilisateur Compte AWS root Compte AWS pour créer un coffre-fort de sauvegarde, vous Compte AWS en êtes le propriétaire.
- Si vous créez un utilisateur IAM dans votre coffre Compte AWS et que vous accordez à cet utilisateur l'autorisation de créer un coffre de sauvegarde, celui-ci peut créer un coffre de sauvegarde. Toutefois, votre compte AWS , auquel l'utilisateur appartient, est propriétaire de la ressource que constitue le coffre-fort de sauvegarde.
- Si vous créez un rôle IAM Compte AWS avec les autorisations nécessaires pour créer un coffre-fort de sauvegarde, toute personne susceptible d'assumer ce rôle peut créer un coffre-fort. Vous Compte AWS, à qui appartient le rôle, êtes propriétaire de la ressource du coffre de sauvegarde.

Spécification des éléments d’une politique : actions, effets et principaux

Pour chaque AWS Backup ressource (voirRessources et opérations), le service définit un ensemble d'opérations d'API (voirActions). Pour accorder des autorisations pour ces opérations d'API AWS Backup , définissez un ensemble d'actions que vous pouvez spécifier dans une politique. Une opération d’API peut exiger des autorisations pour plusieurs actions.

Voici les éléments les plus élémentaires d'une politique :

- Ressource : dans une politique, vous utilisez un Amazon Resource Name (ARN) pour identifier la ressource à laquelle la politique s'applique. Pour plus d’informations, consultez Ressources et opérations.
- Action : vous utilisez des mots clés d’action pour identifier les opérations de ressource que vous voulez accorder ou refuser.
- Effet – Vous spécifiez l’effet produit lorsque l’utilisateur demande l’action spécifique, qui peut être une autorisation ou un refus. Si vous n’accordez pas explicitement l’accès pour (autoriser) une ressource, l’accès est implicitement refusé. Vous pouvez aussi explicitement refuser l’accès à une ressource, ce que vous pouvez faire afin de vous assurer qu’un utilisateur n’y a pas accès, même si une politique différente accorde l’accès.

- Principal – dans les politiques basées sur une identité (politiques IAM), l'utilisateur auquel la politique est attachée est le principal implicite. Pour les politiques basées sur une ressource, vous spécifiez l'utilisateur, le compte, le service ou une autre entité qui doit recevoir les autorisations (s'applique uniquement aux politiques basées sur une ressource).

Pour plus d'informations sur la syntaxe des politiques IAM et pour obtenir des descriptions, consultez Référence de politique JSON IAM dans le manuel Guide de l'utilisateur IAM.

Pour un tableau présentant toutes les actions de l' AWS Backup API, consultezAutorisations d'API : référence des actions, ressources et conditions.

Spécification de conditions dans une politique

Lorsque vous accordez des autorisations, vous pouvez utiliser le langage des politiques IAM afin de spécifier les conditions définissant à quel moment une politique doit prendre effet. Par exemple, il est possible d'appliquer une politique après seulement une date spécifique. Pour plus d'informations sur la spécification de conditions dans un langage de politique, consultez Condition 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 globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

AWS Backup définit son propre ensemble de clés de condition. Pour consulter la liste des clés de AWS Backup condition, reportez-vous à la section Clés de condition pour AWS Backup la référence d'autorisation de service.

Autorisations d'API : référence des actions, ressources et conditions

Lorsque vous configurez Contrôle d'accès et que vous créez une stratégie d'autorisation que vous pouvez attacher à une identité IAM (stratégies basées sur une identité), vous pouvez utiliser la de tableaux ci-dessous comme référence. Le chaque opération d' AWS Backup API, les actions correspondantes pour lesquelles vous pouvez accorder des autorisations pour effectuer l'action et la AWS ressource pour laquelle vous pouvez accorder les autorisations. Vous spécifiez les actions dans le champ `Action` de la politique ainsi que la valeur des ressources dans le champ `Resource` de la politique. Si le champ `Resource` est vide, vous pouvez utiliser le caractère générique (`*`) pour inclure toutes les ressources.

Vous pouvez utiliser des AWS clés de condition larges dans vos AWS Backup polices pour exprimer des conditions. Pour obtenir la liste complète des touches AWS-wide, consultez la section Clés disponibles dans le guide de l'utilisateur IAM.

[1] Utilise la politique d'accès au coffre existante.

[2] Voir AWS Backup ARN des ressources pour les ARN des points de restauration spécifiques aux ressources.

[3] `StartRestoreJob` doit contenir la paire clé-valeur dans les métadonnées de la ressource. Pour obtenir les métadonnées de la ressource, appelez l'API `GetRecoveryPointRestoreMetadata`.

[4] Certains types de ressources nécessitent que le rôle effectuant la sauvegarde dispose d'une autorisation de balisage spécifique `backup:TagResource` si vous prévoyez d'inclure des balises de ressource d'origine dans votre sauvegarde ou d'ajouter des balises supplémentaires à une sauvegarde. Toute sauvegarde avec un ARN commençant par `arn:aws:backup:`*`region`*`:`*`account-id`*`:recovery-point:` ou une sauvegarde continue nécessite cette autorisation. `backup:TagResource`l'autorisation doit être appliquée à `"`*`resourcetype`*`": "arn:aws:backup:`*`region`*`:`*`account-id:`*`recovery-point:*"`

Pour plus d'informations, consultez la rubrique Actions, ressources et clés de condition pour AWS Backup dans la section Référence de l'autorisation de service.

Autorisations de copie de balises

Lorsqu'il AWS Backup exécute une tâche de sauvegarde ou de copie, il tente de copier les balises de votre ressource source (ou point de récupération dans le cas d'une copie) vers votre point de restauration.

> **Note**
>
> AWS Backup ne copie pas les balises de manière native pendant les tâches de restauration. Pour une architecture axée sur les événements qui copiera les balises pendant les tâches de restauration, voir Comment conserver les balises de ressources dans les tâches de AWS Backup restauration.

Au cours d'une tâche de sauvegarde ou de copie, AWS Backup agrège les balises que vous spécifiez dans votre plan de sauvegarde (ou plan de copie, ou sauvegarde à la demande) avec les balises

de votre ressource source. Cependant, AWS impose une limite de 50 balises par ressource, qui AWS Backup ne peut pas être dépassée. Lorsqu'une tâche de sauvegarde ou de copie regroupe les balises du plan et de la ressource source, elle peut découvrir plus de 50 balises au total ; elle ne pourra pas terminer la tâche et échouera. Cela est conforme aux meilleures pratiques en matière de balisage à grande AWSéchelle. Pour en savoir plus, consultez Limites de balises dans le Guide de référence générale AWS .

- Votre ressource possède plus de 50 balises après avoir agrégé vos balises de tâche de sauvegarde avec vos balises de ressource source. AWS prend en charge jusqu'à 50 balises par ressource. Pour plus d'informations, consultez Limites de balises.
- Le rôle IAM que vous attribuez n'est AWS Backup pas autorisé à lire les balises source ou à définir les balises de destination. Pour plus d'informations et des exemples de politiques de rôle IAM, consultez Politiques gérées.

Vous pouvez utiliser votre plan de sauvegarde pour créer des balises qui contredisent les balises de vos ressources source. Lorsque les deux sont en conflit, les balises de votre plan de sauvegarde ont priorité. Utilisez cette technique si vous préférez ne pas copier la valeur d'une balise depuis votre ressource source. Spécifiez la même clé de balise, mais une valeur différente ou vide, à l'aide de votre plan de sauvegarde.

Autorisations requises pour attribuer des balises aux sauvegardes

Type de ressource	Autorisation obligatoire
Système de fichiers Amazon EFS	`elasticfilesystem:DescribeTags`
Système de fichiers Amazon FSx	`fsx:ListTagsForResource`
Base de données Amazon RDS et cluster Amazon Aurora	`rds:AddTagsToResource` `rds:ListTagsForResource`
Volume Storage Gateway	`storagegateway:ListTagsForResource`
Instance Amazon EC2 et volume Amazon EBS	`EC2:CreateTags` `EC2:DescribeTags`

DynamoDB ne prend pas en charge l'attribution de balises aux sauvegardes, sauf si vous activez d'abord Sauvegarde DynamoDB avancée.

Lorsqu'une sauvegarde Amazon EC2 crée un point de restauration d'image et un ensemble de snapshots, elle AWS Backup copie les balises dans l'AMI qui en résulte. AWS Backup copie également les balises des volumes associés à l'instance Amazon EC2 vers les instantanés qui en résultent.

politiques d'accès

Une permissions policy (politique d'autorisation) décrit qui a accès à quoi. Les politiques attachées à une identité IAM sont appelées des politiques basées sur l'identité (politiques IAM). Les politiques associées à une ressource sont appelées politiques basées sur les ressources. AWS Backup prend en charge à la fois les politiques basées sur l'identité et les politiques basées sur les ressources.

> **Note**
>
> Cette section décrit l'utilisation d'IAM dans le contexte de AWS Backup. Elle ne fournit pas d'informations détaillées sur le service IAM. Pour une documentation complète sur IAM, veuillez consulter Qu'est-ce qu'IAM ? dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la syntaxe et les descriptions des politiques IAM, veuillez consulter Référence de politique JSON IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur une identité (politiques IAM)

Les politiques basées sur une identité sont des politiques que vous pouvez attacher à une identité IAM, par exemple à des utilisateurs ou des rôles. Par exemple, vous pouvez définir une politique qui permet à un utilisateur de visualiser et de sauvegarder AWS des ressources, mais l'empêche de restaurer des sauvegardes.

Pour plus d'informations sur les utilisateurs, les groupes, les rôles et les autorisations, consultez Identités (utilisateurs, groupes et rôles) dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur l'utilisation de politiques IAM pour contrôler l'accès aux sauvegardes, consultez Politiques gérées pour AWS Backup.

Politiques basées sur les ressources

AWS Backup prend en charge les politiques d'accès basées sur les ressources pour les coffres-forts de sauvegarde. Vous pouvez ainsi définir une stratégie d'accès qui peut contrôler quels

utilisateurs disposent d'un type d'accès particulier aux sauvegardes organisées dans un coffre-fort de sauvegarde. Les stratégies d'accès basées sur une ressource pour les coffres-forts de sauvegarde permettent de contrôler de manière simple l'accès à vos sauvegardes.

Les politiques d'accès au coffre de sauvegarde contrôlent l'accès des utilisateurs lorsque vous utilisez AWS Backup des API. Certains types de sauvegarde, tels que les instantanés Amazon Elastic Block Store (Amazon EBS) et Amazon Relational Database Service (Amazon RDS), sont également accessibles via les API de ces services. Vous pouvez créer des stratégies d'accès distinctes dans IAM qui contrôlent l'accès à ces API afin d'exercer un contrôle total sur l'accès aux sauvegardes.

Pour savoir comment créer une stratégie d'accès pour les coffres-forts de sauvegarde, consultez Définition de stratégies d'accès sur des coffres-forts de sauvegarde.

Fonctions du service IAM

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. AWS Backup étant le service qui effectue des opérations de sauvegarde en votre nom, vous devez lui transmettre un rôle à assumer lors des opérations de sauvegarde en votre nom. Pour plus d'informations sur les rôles IAM, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

Le rôle auquel vous passez AWS Backup doit disposer d'une politique IAM avec les autorisations permettant d'effectuer des actions associées AWS Backup aux opérations de sauvegarde, telles que la création, la restauration ou l'expiration de sauvegardes. Des autorisations différentes sont requises pour chacun des AWS services pris en AWS Backup charge. Le rôle doit également être AWS Backup répertorié comme une entité de confiance, ce qui AWS Backup permet d'assumer le rôle.

Lorsque vous attribuez des ressources à un plan de sauvegarde ou que vous effectuez une sauvegarde, une copie ou une restauration à la demande, vous devez transmettre un rôle de service autorisé à effectuer les opérations sous-jacentes sur les ressources spécifiées. AWS Backup utilise ce rôle pour créer, étiqueter et supprimer des ressources dans votre compte.

Utilisation de AWS rôles pour contrôler l'accès aux sauvegardes

Vous pouvez utiliser des rôles pour contrôler l'accès à vos sauvegardes en définissant des rôles étroitement limités et en spécifiant quelles personnes peuvent transmettre ce rôle à AWS Backup.

Par exemple, vous pouvez créer un rôle qui accorde uniquement des autorisations pour sauvegarder des bases de données Amazon Relational Database Service (Amazon RDS) et uniquement autoriser les propriétaires de bases de données Amazon RDS à transmettre ce rôle. AWS Backup AWS Backup fournit plusieurs politiques gérées prédéfinies pour chacun des services pris en charge. Vous pouvez attacher ces politiques gérées aux rôles que vous créez. Cela facilite la création de rôles spécifiques au service dotés des autorisations requises. AWS Backup

Pour plus d'informations sur les politiques AWS gérées pour AWS Backup, consultezPolitiques gérées pour AWS Backup.

Rôle de service par défaut pour AWS Backup

Lorsque vous utilisez la AWS Backup console pour la première fois, vous pouvez choisir de AWS Backup créer un rôle de service par défaut pour vous. Ce rôle dispose des autorisations AWS Backup nécessaires pour créer et restaurer des sauvegardes en votre nom.

> **Note**
>
> Le rôle par défaut est automatiquement créé lorsque vous utilisez la AWS Management Console. Vous pouvez créer le rôle par défaut à l'aide du AWS Command Line Interface (AWS CLI), mais cela doit être fait manuellement.

Si vous préférez utiliser des rôles personnalisés, tels que des rôles distincts pour différents types de ressources, vous pouvez également le faire et transmettre vos rôles personnalisés à AWS Backup. Pour voir des exemples de rôles qui permettent la sauvegarde et la restauration pour des types de ressources individuels, consultez la table Politiques gérées par le client.

Le rôle de service par défaut est nomméAWSBackupDefaultServiceRole. Ce rôle de service contient deux politiques gérées, AWSBackupServiceRolePolicyForBackupet AWSBackupServiceRolePolicyForRestores.

AWSBackupServiceRolePolicyForBackupinclut une politique IAM qui accorde des AWS Backup autorisations pour décrire la ressource sauvegardée, ainsi que la possibilité de créer, de supprimer, de décrire ou d'ajouter des balises à une sauvegarde, quelle que soit la AWS KMS clé avec laquelle elle est chiffrée.

AWSBackupServiceRolePolicyForRestoresinclut une politique IAM qui accorde des AWS Backup autorisations pour créer, supprimer ou décrire la nouvelle ressource créée à partir d'une

sauvegarde, quelle que soit la AWS KMS clé avec laquelle elle est chiffrée. Il inclut également des autorisations pour baliser les ressources nouvellement créés.

Pour restaurer une instance Amazon EC2, vous devez lancer une nouvelle instance.

Création d'une fonction du service par défaut dans la console

Les actions spécifiques que vous effectuez dans la AWS Backup console créent le rôle de service AWS Backup par défaut.

Pour créer le rôle de service AWS Backup par défaut dans votre AWS compte

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Pour créer le rôle pour votre compte, attribuez des ressources à un plan de sauvegarde ou créez une sauvegarde à la demande.

   a. Créez un plan de sauvegarde et attribuez des ressources à la sauvegarde. Consultez Création d'une sauvegarde planifiée.

   b. Vous pouvez également créer une sauvegarde à la demande. Consultez Création d'une sauvegarde à la demande.
3. Vérifiez que vous avez créé le `AWSBackupDefaultServiceRole` dans votre compte en suivant ces étapes :

   a. Patientez quelques minutes. Pour plus d'informations, consultez Les modifications que j'apporte ne sont pas toujours visibles immédiatement dans le Guide de l'utilisateur AWS Identity and Access Management.

   b. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/iam/.

   c. Dans le menu de navigation de gauche, choisissez Rôles.

   d. Dans la barre de recherche, saisissez `AWSBackupDefaultServiceRole`. Si cette sélection existe, vous avez créé le rôle AWS Backup par défaut et terminé cette procédure.

   e. Si `AWSBackupDefaultServiceRole` n'apparaît toujours pas, ajoutez les autorisations suivantes à l'utilisateur IAM ou au rôle IAM que vous utilisez pour accéder à la console.

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

```
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
      ],
      "Resource":"*"
    }
  ]
}
```

Pour les régions chinoises, remplacez *aws* par *aws-cn*. Pour AWS GovCloud (US) les régions, remplacez *aws* par *aws-us-gov*.

f. Si vous ne pouvez pas ajouter d'autorisations à votre utilisateur IAM ou à votre rôle IAM, demandez à votre administrateur de créer manuellement un rôle sous un nom autre que `AWSBackupDefaultServiceRole` et de l'associer à ces politiques gérées :

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

Politiques gérées pour AWS Backup

Les politiques gérées sont des politiques autonomes basées sur l'identité que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre. Compte AWS Lorsque vous attachez une politique à une entité principale, vous accordez à cette dernière les autorisations définies dans la politique.

AWS les politiques gérées sont créées et administrées par AWS. Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée.

Les politiques gérées par le client vous fournissent des contrôles précis pour définir l'accès aux sauvegardes. AWS Backup Par exemple, vous pouvez les utiliser pour donner à votre administrateur de sauvegarde de base de données l'accès aux sauvegardes Amazon RDS, mais pas à celles d'Amazon EFS.

Pour plus d'informations, consultez la section Politiques gérées dans le guide de l'utilisateur IAM.

AWS politiques gérées

AWS Backup fournit les politiques AWS gérées suivantes pour les cas d'utilisation courants. Ces stratégies facilitent la définition des autorisations appropriées et le contrôle de l'accès à vos sauvegardes. Il existe deux types de stratégies gérées. L'un des types est conçu pour être affecté aux utilisateurs afin de contrôler leur accès à AWS Backup. L'autre type de stratégie gérée est conçu pour être attaché à des rôles que vous transmettez à AWS Backup. Le tableau suivant répertorie toutes les stratégies gérées fournies par AWS Backup et explique comment elles sont définies. Vous pouvez trouver ces politiques gérées dans la section Politiques de la console IAM.

Politiques

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

Cette politique autorise les utilisateurs à créer des contrôles et des cadres qui définissent leurs attentes en matière de AWS Backup ressources et d'activités, et à auditer les AWS Backup ressources et les activités par rapport à leurs contrôles et cadres définis. Cette politique accorde des autorisations AWS Config et des services similaires pour décrire les attentes des utilisateurs lors des audits.

Cette politique accorde également des autorisations pour fournir des rapports d'audit à Amazon S3 et à des services similaires, et permet aux utilisateurs de rechercher et d'ouvrir leurs rapports d'audit.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupAuditAccessà la référence des politiques AWS gérées.

AWSBackupDataTransferAccess

Cette politique fournit des autorisations pour les API de transfert de données du plan de AWS Backup stockage, permettant à l'agent AWS Backint d'effectuer le transfert des données de sauvegarde avec le plan AWS Backup de stockage. Vous pouvez associer cette politique aux rôles assumés par les instances Amazon EC2 exécutant SAP HANA avec l'agent Backint.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupDataTransferAccessà la référence des politiques AWS gérées.

AWSBackupFullAccess

L'administrateur de sauvegarde dispose d'un accès complet aux AWS Backup opérations, notamment à la création ou à la modification de plans de sauvegarde, à l'affectation de AWS ressources aux plans de sauvegarde et à la restauration des sauvegardes. Les administrateurs de sauvegarde sont chargés de déterminer et d'appliquer la conformité des sauvegardes en définissant des plans de sauvegarde conformes aux exigences professionnelles et réglementaires de l'entreprise. Les administrateurs de sauvegarde s'assurent également que les AWS ressources de leur organisation sont affectées au plan approprié.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupFullAccessà la référence des politiques AWS gérées.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Pour consulter les autorisations associées à cette politique, reportez-vous à la référence des politiques AWS gérées.

AWSBackupOperatorAccess

Les opérateurs de sauvegarde sont des utilisateurs chargés de veiller à ce que les ressources dont ils sont responsables sont correctement sauvegardées. Les opérateurs de sauvegarde sont autorisés à affecter AWS des ressources aux plans de sauvegarde créés par l'administrateur de sauvegarde. Ils sont également autorisés à créer des sauvegardes à la demande de leurs AWS ressources et à configurer la période de conservation des sauvegardes à la demande. Les opérateurs de sauvegarde ne sont pas autorisés à créer ni modifier les plans de sauvegarde, ni supprimer les sauvegardes planifiées après leur création. Les opérateurs de sauvegarde peuvent restaurer les sauvegardes. Vous pouvez limiter les types de ressources qu'un opérateur de sauvegarde peut affecter à un plan de sauvegarde ou restaurer à partir d'une sauvegarde. Pour ce faire, vous n'autorisez le transfert AWS Backup que de certains rôles de service dotés d'autorisations pour un certain type de ressource.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupOperatorAccessà la référence des politiques AWS gérées.

AWSBackupOrganizationAdminAccess

L'administrateur de l'organisation dispose d'un accès complet aux AWS Organizations opérations, notamment à la création, à la modification ou à la suppression de politiques de sauvegarde, à l'attribution de politiques de sauvegarde aux comptes et aux unités organisationnelles et à la surveillance des activités de sauvegarde au sein de l'organisation. Les administrateurs de l’organisation sont responsables de la protection des comptes de leur organisation avec la définition et l’affectation de stratégies de sauvegarde qui répondent aux exigences commerciales et réglementaires de leur organisation.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupOrganizationAdminAccessà la référence des politiques AWS gérées.

AWSBackupRestoreAccessForSAPHANA

Cette politique AWS Backup autorise la restauration d'une sauvegarde de SAP HANA sur Amazon EC2.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupRestoreAccessForSAPHANAà la référence des politiques AWS gérées.

AWSBackupServiceLinkedRolePolicyForBackup

Cette politique est attachée au rôle lié au service nommé AWSServiceRoleforBackup pour permettre d' AWS Backup appeler les AWS services en votre nom pour gérer vos sauvegardes. Pour plus d'informations, consultez the section called “Sauvegarde et copie”.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupServiceLinkedRolePolicyforBackupà la référence des politiques AWS gérées.

AWSBackupServiceLinkedRolePolicyForBackupTest

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupServiceLinkedRolePolicyForBackupTestà la référence des politiques AWS gérées.

AWSBackupServiceRolePolicyForBackup

Permet de AWS Backup créer des sauvegardes de tous les types de ressources pris en charge en votre nom.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupServiceRolePolicyForBackupà la référence des politiques AWS gérées.

AWSBackupServiceRolePolicyForRestores

Permet de AWS Backup restaurer les sauvegardes de tous les types de ressources pris en charge en votre nom.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupServiceRolePolicyForRestoresà la référence des politiques AWS gérées.

Pour les restaurations d'instances EC2, vous devez également inclure les autorisations suivantes pour lancer l'instance EC2 :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
```

```
    ]
}
```

AWSBackupServiceRolePolicyForS3Backup

Cette politique contient les autorisations nécessaires AWS Backup pour sauvegarder n'importe quel compartiment S3. Cela inclut l'accès à tous les objets d'un compartiment et à toute AWS KMS clé associée.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupServiceRolePolicyForS3Backupà la référence des politiques AWS gérées.

AWSBackupServiceRolePolicyForS3Restore

Cette politique contient les autorisations nécessaires AWS Backup pour restaurer une sauvegarde S3 dans un compartiment. Cela inclut les autorisations de lecture et d'écriture sur les buckets et l'utilisation de n'importe quelle AWS KMS clé en ce qui concerne les opérations S3.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupServiceRolePolicyForS3Restoreà la référence des politiques AWS gérées.

AWSServiceRolePolicyForBackupReports

AWS Backup utilise cette politique pour le rôle AWSServiceRoleForBackupReportslié au service. Ce rôle lié à un service donne AWS Backup les autorisations nécessaires pour surveiller et établir des rapports sur la conformité de vos paramètres de sauvegarde, de vos tâches et de vos ressources avec vos frameworks.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSServiceRolePolicyForBackupReportsà la référence des politiques AWS gérées.

AWSServiceRolePolicyForBackupRestoreTesting

Pour consulter les autorisations associées à cette politique, reportez-vous AWSServiceRolePolicyForBackupRestoreTestingà la référence des politiques AWS gérées.

Politiques gérées par le client

Les sections suivantes décrivent les autorisations de sauvegarde et de restauration recommandées pour l' Services AWS application tierce prise en charge par AWS Backup. Vous pouvez utiliser les

politiques AWS gérées existantes comme modèle lorsque vous créez vos propres documents de politique, puis les personnaliser pour restreindre davantage l'accès à vos AWS ressources.

Amazon Aurora

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurer

Commencez par la `RDSPermissions` déclaration de AWSBackupServiceRolePolicyForRestores.

Amazon DynamoDB

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Restaurer

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForRestores:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamoDBRestorePermissions`
- `KMSPermissions`

Amazon EBS

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `EBSResourcePermissions`
- `EBSTagAndDeletePermissions`
- `EBSCopyPermissions`
- `EBSSnapshotTierPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurer

Commencez par la `EBSPermissions` déclaration de AWSBackupServiceRolePolicyForRestores.

Ajoutez la déclaration suivante.

```
{
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `EBSCopyPermissions`
- `EC2CopyPermissions`
- `EC2Permissions`
- `EC2TagPermissions`

- `EC2ModifyPermissions`
- `EBSResourcePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurer

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForRestores:

- `EBSPermissions`
- `EC2DescribePermissions`
- `EC2RunInstancesPermissions`
- `EC2TerminateInstancesPermissions`
- `EC2CreateTagsPermissions`

Ajoutez la déclaration suivante.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Amazon EFS

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `EFSPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurer

Commencez par la `EFSPermissions` déclaration de AWSBackupServiceRolePolicyForRestores.

Amazon FSx

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `FsxBackupPermissions`
- `FsxCreateBackupPermissions`
- `FsxPermissions`
- `FsxVolumePermissions`
- `FsxListTagsPermissions`
- `FsxDeletePermissions`
- `FsxResourcePermissions`
- `KMSPermissions`

Restaurer

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForRestores:

- `FsxPermissions`
- `FsxTagPermissions`
- `FsxBackupPermissions`
- `FsxDeletePermissions`
- `FsxDescribePermissions`
- `FsxVolumeTagPermissions`
- `FsxBackupTagPermissions`
- `FsxVolumePermissions`
- `DSPermissions`
- `KMSDescribePermissions`

Amazon RDS

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurer

Commencez par la `RDSPermissions` déclaration de AWSBackupServiceRolePolicyForRestores.

Amazon S3

Sauvegarde

Commencez par AWSBackupServiceRolePolicyForS3Backup.

Ajoutez les `BackupVaultCopyPermissions` instructions `BackupVaultPermissions` et si vous devez copier des sauvegardes sur un autre compte.

Restaurer

Commencez par AWSBackupServiceRolePolicyForS3Restore.

AWS Storage Gateway

Sauvegarde

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForBackup:

- `StorageGatewayPermissions`
- `EBSTagAndDeletePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Ajoutez la déclaration suivante.

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

Restaurer

Commencez par les affirmations suivantes provenant de AWSBackupServiceRolePolicyForRestores:

- `StorageGatewayVolumePermissions`
- `StorageGatewayGatewayPermissions`
- `StorageGatewayListPermissions`

Machine virtuelle

Sauvegarde

Commencez par la `BackupGatewayBackupPermissions` déclaration de AWSBackupServiceRolePolicyForBackup.

Restaurer

Commencez par la `GatewayRestorePermissions` déclaration de AWSBackupServiceRolePolicyForRestores.

Sauvegarde cryptée

Pour restaurer une sauvegarde chiffrée, effectuez l'une des actions suivantes :

- Ajoutez votre rôle à la liste d'autorisation pour la politique AWS KMS clé
- Ajoutez les instructions suivantes AWSBackupServiceRolePolicyForRestoresà partir de votre rôle IAM pour les restaurations :
  - `KMSDescribePermissions`
  - `KMSPermissions`
  - `KMSCreateGrantPermissions`

Mises à jour des politiques pour AWS Backup

Consultez les détails des mises à jour des politiques AWS gérées AWS Backup depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une stratégie existante	AWS Backup autorisation ajoutée `backup:TagResource` à cette politique. L'autorisation est nécessaire pour obtenir des autorisations de balisage lors de la création d'un point de récupération.	17 mai 2024
AWSBackupServiceRolePolicyForS3Backup – Mise à jour d'une politique existante	AWS Backup autorisation ajoutée `backup:TagResource` à cette politique. L'autorisation est nécessaire pour obtenir des autorisations de balisage lors de la création d'un point de récupération.	17 mai 2024
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	AWS Backup autorisation ajoutée `backup:TagResource` à cette politique. L'autorisation est nécessaire pour obtenir des autorisations de balisage lors de la création d'un point de récupération.	17 mai 2024

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	L'autorisation a été ajoutée`erds:DeleteDBInstanceAutomatedBackups` . Cette autorisation est nécessaire pour AWS Backup prendre en charge la sauvegarde continue et point-in-time-restore les instances Amazon RDS.	1er mai 2024
AWSBackupFullAccess – Mise à jour d'une politique existante	AWS Backup a mis à jour l'Amazon Resource Name (ARN) dans l'autorisation `storagegateway:ListVolumes` de `arn:aws:storagegateway:*:*:gateway/*` à * afin de tenir compte d'une modification du modèle d'API Storage Gateway.	1er mai 2024
AWSBackupOperatorAccess – Mise à jour d'une politique existante	AWS Backup a mis à jour l'Amazon Resource Name (ARN) dans l'autorisation `storagegateway:ListVolumes` de `arn:aws:storagegateway:*:*:gateway/*` à * afin de tenir compte d'une modification du modèle d'API Storage Gateway.	1er mai 2024

Modification	Description	Date
AWSServiceRolePolicyForBackupRestoreTesting – Mise à jour d'une politique existante	Ajout des autorisations suivantes pour décrire et répertorier les points de récupération et les ressources protégées afin de réaliser des plans de test de restauration : `backup:DescribeRecoveryPoint` `backup:DescribeProtectedResource` ,`backup:ListProtectedResources` , et`backup:ListRecoveryPointsByResource` . Ajout de l'autorisation `ec2:DescribeSnapshotTierStatus` de prendre en charge le stockage au niveau des archives Amazon EBS. Ajout de l'autorisation `rds:DescribeDBClusterAutomatedBackups` de prendre en charge les sauvegardes continues d'Amazon Aurora. Les autorisations suivantes ont été ajoutées pour prendre en charge les tests de restauration des sauvegardes Amazon Redshift : `redshift:DescribeC`	14 février 2024

Modification	Description	Date
	`lusters` et. `redshift:DeleteCluster` Ajout de l'autorisation `timestream:DeleteTable` de prendre en charge les tests de restauration des sauvegardes Amazon Timestream.	
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajout des autorisations `ec2:DescribeSnapshotTierStatus` et`ec2:RestoreSnapshotTier` . Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de restaurer les ressources Amazon EBS stockées à AWS Backup partir du stockage d'archives. Pour les restaurations d'instances EC2, vous devez également inclure les autorisations comme illustrées dans l'instruction de politique suivante pour lancer l'instance EC2 :	27 novembre 2023

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Ajout des autorisations `ec2:DescribeSnapshotTierStatus` et `ec2:ModifySnapshotTier` de la prise en charge d'une option de stockage supplémentaire pour les ressources Amazon EBS sauvegardées à transférer vers le niveau de stockage des archives. Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de transférer les ressources Amazon EBS stockées vers le stockage AWS Backup d'archives.	27 novembre 2023

Modification	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajout des autorisations `ec2:DescribeSnapshotTierStatus` et `ec2:ModifySnapshotTier` de la prise en charge d'une option de stockage supplémentaire pour les ressources Amazon EBS sauvegardées à transférer vers le niveau de stockage des archives. Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de transférer les ressources Amazon EBS stockées vers le stockage AWS Backup d'archives. Ajout des autorisations `rds:DescribeDBClusterSnapshots` et `rds:RestoreDBClusterToPointInTime` des autorisations nécessaires pour les PITR (point-in-time restaurations) des clusters Aurora.	

Modification	Description	Date
AWSServiceRolePolicyForBackupRestoreTesting : nouvelle politique	Fournit les autorisations nécessaires pour effectuer des tests de restauration. Les autorisations incluent les actions `list, read, and write` relatives aux services suivants à inclure dans les tests de la restauration : Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx pour Lustre, FSx for Windows File Server, FSx pour ONTAP, FSx pour OpenZFS, Amazon Neptune, Amazon RDS et Amazon S3.	27 novembre 2023
AWSBackupFullAccess – Mise à jour d'une politique existante	Ajout de `restore-testing.backup.amazonaws.com` à `IamPassRolePermissions` et `IamCreateServiceLinkedRolePermissions`. Cet ajout est nécessaire pour AWS Backup effectuer des tests de restauration pour le compte des clients.	27 novembre 2023

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajout des autorisations `rds:DescribeDBClusterSnapshots` et `rds:RestoreDBClusterToPointInTime` des autorisations nécessaires pour les PITR (point-in-time restaurations) des clusters Aurora.	6 septembre 2023
AWSBackupFullAccess – Mise à jour d'une politique existante	Ajout de l'autorisation `rds:DescribeDBClusterAutomatedBackups`, qui est nécessaire pour la sauvegarde et la point-in-time restauration continues des clusters Aurora.	6 septembre 2023
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Ajout de l'autorisation `rds:DescribeDBClusterAutomatedBackups`, qui est nécessaire pour la sauvegarde et la point-in-time restauration continues des clusters Aurora.	6 septembre 2023

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	L'autorisation a été ajoutée`rds:DescribeDBClusterAutomatedBackups` . Cette autorisation est nécessaire pour AWS Backup prendre en charge la sauvegarde et la point-in-time restauration continues des clusters Aurora. Ajout de l'autorisation permettant `rds:DeleteDBClusterAutomatedBackups` au AWS Backup cycle de vie de supprimer et de dissocier les points de restauration continue Amazon Aurora à la fin d'une période de rétention. Cette autorisation est nécessaire pour que le point de récupération Aurora évite une transition vers un état `EXIPIRED`. Ajout de l'autorisation `rds:ModifyDBCluster` qui permet AWS Backup d'interagir avec les clusters Aurora. Cet ajout permet aux utilisateurs d'activer ou de désactiver les sauvegardes continues en fonction des configurations souhaitées.	6 septembre 2023

Modification	Description	Date
AWSBackupFullAccess – Mise à jour d'une politique existante	Ajout de l'action permettant d'accorder `ram:GetResourceShareAssociations` à l'utilisateur l'autorisation d'obtenir des associations de partage de ressources pour le nouveau type de coffre-fort.	08 août 2023
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Ajout de l'action permettant d'accorder `ram:GetResourceShareAssociations` à l'utilisateur l'autorisation d'obtenir des associations de partage de ressources pour le nouveau type de coffre-fort.	08 août 2023
AWSBackupServiceRolePolicyForS3Backup – Mise à jour d'une politique existante	Ajout de l'autorisation `s3:PutInventoryConfiguration` d'améliorer les performances de sauvegarde en utilisant un inventaire des compartiments.	1er août 2023

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Les actions suivantes ont été ajoutées pour autoriser l'utilisateur à ajouter des balises afin de restaurer les ressources :`storagegateway:AddTagsToResource` ,`elasticfilesystem:TagResource` , uniquement `ec2:CreateTags` pour `ec2:CreateAction` cela inclut l'un `RunInstances` ou l'autre `CreateVolume` `fsx:TagResource` , et`cloudformation:TagResource` .	22 mai 2023
AWSBackupAuditAccess – Mise à jour d'une politique existante	La sélection des ressources dans l'API `config:DescribeComplianceByConfigRule` a été remplacée par une ressource générique afin de faciliter la sélection des ressources par un utilisateur.	11 avril 2023
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajout de l'autorisation suivante pour restaurer Amazon EFS à l'aide d'une clé gérée par le client : `kms:GenerateDataKeyWithoutPlaintext` Cela permet de garantir que les utilisateurs disposent des autorisations requises pour restaurer les ressources Amazon EFS.	27 mars 2023

Modification	Description	Date
AWSServiceRolePolicyForBackupReports – Mise à jour d'une politique existante	Mise à jour des `config:DescribeConfigRuleEvaluationStatus` actions `config:DescribeConfigRules` et pour permettre à AWS Backup Audit Manager d'accéder aux règles gérées par AWS Backup Audit Manager AWS Config .	9 mars 2023
AWSBackupServiceRolePolicyForS3Restore – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées : `kms:Decrypt` `s3:PutBucketOwnershipControls` , et `s3:GetBucketOwnershipControls` à la politique `AWSBackupServiceRolePolicyForS3Restore` . Ces autorisations sont nécessaires pour prendre en charge les restaurations d'objets lorsque le chiffrement KMS est utilisé dans la sauvegarde d'origine et pour restaurer des objets lorsque la propriété des objets est configurée sur le compartiment d'origine au lieu de la liste ACL.	13 février 2023

Modification	Description	Date
AWSBackupFullAccess – Mise à jour d'une politique existante	Ajout des autorisations suivantes pour planifier les sauvegardes à l'aide des balises VMware des machines virtuelles et pour prendre en charge la régulation de la bande passante basée sur la planification :,`backup-gateway:Get HypervisorProperty Mappings` ,,, `backup-gateway:GetVirtualMachine` `backup-gateway:PutHypervisorPropertyMappings` , `backup-gateway:GetHypervisor` et. `backup-gateway:StartVirtualMachinesMetadataSync` `backup-gateway:GetBandwidthRateLimitSchedule` `backup-gateway:PutBandwidthRateLimitSchedule`	15 décembre 2022

Modification	Description	Date
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour planifier les sauvegardes à l'aide des balises VMware des machines virtuelles et pour prendre en charge la limitation de bande passante basée sur la planification :`backup-gateway:GetHypervisorPropertyMappings` ,, et. `backup-gateway:GetVirtualMachine` `backup-gateway:GetHypervisor` `backup-gateway:GetBandwidthRateLimitSchedule`	15 décembre 2022
AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync : nouvelle politique	Permet à AWS Backup Gateway de synchroniser les métadonnées des machines virtuelles sur les réseaux locaux avec Backup Gateway.	15 décembre 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de sauvegarde Timestream : `timestream:StartAwsBackupJob` `timestream:GetAwsBackupStatus` ,`timestream:ListTables` ,`timestream:ListDatabases` ,`timestream:ListTagsForResource` , `timestream:DescribeTable` `timestream:DescribeDatabase` , et. `timestream:DescribeEndpoints`	13 décembre 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de restauration Timestream : `timestream:StartAwsRestoreJob` `timestream:GetAwsRestoreStatus` `timestream:ListTables` ,`timestream:ListTagsForResource` ,`timestream:ListDatabases` ,`timestream:DescribeTable` , `timestream:DescribeDatabase` `s3:GetBucketAcl` , et. `timestream:DescribeEndpoints`	13 décembre 2022
AWSBackupFullAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Timestream :`timestream:ListTables` ,`timestream:ListDatabases` , `s3:ListAllMyBuckets` et. `timestream:DescribeEndpoints`	13 décembre 2022

Modification	Description	Date
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Timestream :`timestrea m:ListDatabases` , `timestream:ListTab les s3:ListAl lMyBuckets` , et. `timestream:Describ eEndpoints`	13 décembre 2022
AWSBackupServiceLi nkedRolePolicyForBackup – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Timestream : `timestream:ListDat abases timestrea m:ListTab les ,timestrea m:ListTagsForResou rce ,timestrea m:DescribeDatabase ,timestream:Describ eTable , timestrea m:GetAwsBackupStat us timestream:GetAwsR estoreStatus` , et. `timestream:Describ eEndpoints`	13 décembre 2022

Modification	Description	Date
AWSBackupFullAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Amazon Redshift : `redshift:DescribeClusters redshift:DescribeClusterSubnetGroups ,redshift:DescribeNodeConfigurationOptions ,redshift:DescribeOrderableClusterOptions ,redshift:DescribeClusterParameterGroups , redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules` , et. `ec2:DescribeAddresses`	27 novembre 2022

Modification	Description	Date
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les ressources Amazon Redshift :`redshift:DescribeClusters` ,,`redshift:DescribeClusterSubnetGroups` ,`redshift:DescribeNodeConfigurationOptions` ,`redshift:DescribeOrderableClusterOptions` ,`redshift:DescribeClusterParameterGroups`, . `redshift:DescribeClusterTracks` `redshift:DescribeSnapshotSchedules` , `etec2:DescribeAddresses` .	27 novembre 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de restauration Amazon Redshift :`redshift:RestoreFromClusterSnapshot`, `redshift:RestoreTableFromClusterSnapshot` `redshift:DescribeClusters`, et. `redshift:DescribeTableRestoreStatus`	27 novembre 2022
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de sauvegarde Amazon Redshift :`redshift:CreateClusterSnapshot`,`redshift:DescribeClusterSnapshots`,`redshift:DescribeTags`, `redshift:DeleteClusterSnapshot` `redshift:DescribeClusters`, et. `redshift:CreateTags`	27 novembre 2022
AWSBackupFullAccess – Mise à jour d'une politique existante	Ajout de l'autorisation suivante pour les CloudFormation ressources de support :`cloudformation:ListStacks`.	27 novembre 2022

Modification	Description	Date
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Ajout de l'autorisation suivante pour les CloudFormation ressources de support :`cloudformation:ListStacks` .	27 novembre 2022
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour CloudFormation les ressources de support : `redshift:DescribeClusterSnapshots` `redshift:DescribeTags` ,`redshift:DeleteClusterSnapshot` , et`redshift:DescribeClusters` .	27 novembre 2022
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge les tâches de sauvegarde de la pile d' AWS CloudFormation applications : `cloudformation:GetTemplate` `cloudformation:DescribeStacks` , et`cloudformation:ListStackResources` .	16 novembre 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajout des autorisations suivantes pour prendre en charge les tâches de sauvegarde de la pile d' AWS CloudFormation applications : `cloudformation:CreateChangeSet` et `cloudformation:DescribeChangeSet`	16 novembre 2022
AWSBackupOrganizationAdminAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées à cette politique pour permettre aux administrateurs de l'organisation d'utiliser la fonctionnalité d'administrateur délégué : `organizations:ListDelegatedAdministrator` `organizations:RegisterDelegatedAdministrator` , et `organizations:DeregisterDelegatedAdministrator`	27 novembre 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge SAP HANA sur les instances Amazon EC2 `ssm-sap:GetOperation` :`ssm-sap:ListDatabases` ,,`ssm-sap:BackupDatabase` , `ssm-sap:UpdateHanaBackupSettings` `ssm-sap:GetDatabase` , et. `ssm-sap:ListTagsForResource`	20 novembre 2022
AWSBackupFullAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge SAP HANA sur les instances Amazon EC2 `ssm-sap:GetOperation` :`ssm-sap:ListDatabases` ,`ssm-sap:GetDatabase` , et. `ssm-sap:ListTagsForResource`	20 novembre 2022
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour prendre en charge SAP HANA sur les instances Amazon EC2 `ssm-sap:GetOperation` :`ssm-sap:ListDatabases` ,`ssm-sap:GetDatabase` , et. `ssm-sap:ListTagsForResource`	20 novembre 2022

Modification	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	L'autorisation suivante a été ajoutée pour prendre en charge SAP HANA sur les instances Amazon EC2 : `ssm-sap:GetOperation`	20 novembre 2022
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	L'autorisation suivante a été ajoutée pour prendre en charge les tâches de restauration de la passerelle Backup sur une instance EC2 : `ec2:CreateTags`	20 novembre 2022
AWSBackupDataTransferAccess – Mise à jour d'une politique existante	Ajout des autorisations suivantes pour prendre en charge le transfert sécurisé des données de stockage pour les ressources SAP HANA On Amazon EC2 `backup-storage:StartObject :backup-storage:PutChunk ,,backup-storage:GetChunk ,backup-storage:ListChunks , backup-storage:ListObjects backup-storage:GetObjectMetadata , et. backup-storage:NotifyObjectComplete`	20 novembre 2022

Modification	Description	Date
AWSBackupRestoreAccessForSAPHANA – Mise à jour d'une politique existante	Les autorisations suivantes ont été ajoutées pour permettre aux propriétaires de ressources d'effectuer la restauration des ressources SAP HANA On Amazon EC2 `backup:Get*` : `backup:List*` `backup:Describe*` `backup:StartBackupJob` ,`backup:StartRestoreJob` ,`ssm-sap:GetOperation` ,`ssm-sap:ListDatabases` ,,`ssm-sap:BackupDatabase` , `ssm-sap:RestoreDatabase` `ssm-sap:UpdateHanaBackupSettings` `ssm-sap:GetDatabase` , et. `ssm-sap:ListTagsForResource`	20 novembre 2022
AWSBackupServiceRolePolicyForS3Backup – Mise à jour d'une politique existante	Ajout de l'autorisation `s3:GetBucketAcl` de prendre en charge les opérations de sauvegarde AWS Backup pour Amazon S3.	24 août 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajout des actions suivantes pour autoriser l'accès à la création d'une instance de base de données prenant en charge la fonctionnalité de zone de disponibilité multiple (multi-AZ) :. `rds:CreateDBInstance`	20 juillet 2022
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajout de l'`s3:GetBucketTagging` autorisation d'accorder à l'utilisateur l'autorisation de sélectionner des buckets à sauvegarder avec un caractère générique de ressource. Sans cette autorisation, les utilisateurs qui sélectionnent les compartiments à sauvegarder avec un caractère générique de ressource échouent.	6 mai 2022
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Ajout de ressources de volume dans le cadre des `fsx:ListTagsForResource` actions existantes `fsx:CreateBackup` et ajout d'une nouvelle action `fsx:DescribeVolumes` pour prendre en charge les sauvegardes au niveau du volume FSx for ONTAP.	27 avril 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores : mise à jour d'une politique existante	Les actions suivantes ont été ajoutées pour autoriser les utilisateurs à restaurer FSx pour les volumes ONTAP`fsx:DescribeVolumes` ,`fsx:CreateVolumeFromBackup` , `fsx:DeleteVolume` et. `fsx:UntagResource`	27 avril 2022
AWSBackupServiceRolePolicyForS3Backup : mise à jour d'une politique existante	Ajout des actions suivantes pour autoriser l'utilisateur à recevoir des notifications de modifications apportées à ses compartiments Amazon S3 lors des opérations de sauvegarde : `s3:GetBucketNotification` ets`3:PutBucketNotification` .	25 février 2022

Modification	Description	Date
AWSBackupServiceRolePolicyForS3Backup : nouvelle politique	Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de sauvegarder ses compartiments Amazon S3 : `s3:GetInventoryConfiguration` `s3:PutInventoryConfiguration` ,`s3:ListBucketVersions` ,`s3:ListBucket` ,`s3:GetBucketTagging` ,`s3:GetBucketVersioning` , `s3:GetBucketNotification` `s3:GetBucketLocation` , et `s3:ListAllMyBuckets` Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de sauvegarder ses objets Amazon S3 : `s3:GetObject` `s3GetObjectAcl` ,`s3:GetObjectVersionTagging` ,`s3:GetObjectVersionAcl` ,`s3:GetObjectTagging` , `ets3:GetObjectVersion` . Les actions suivantes ont été ajoutées pour autoriser	17 février 2022

Modification	Description	Date
	l'utilisateur à sauvegarder ses données Amazon S3 chiffrées : `kms:Decrypt` et`kms:DescribeKey` . Les actions suivantes ont été ajoutées pour autoriser l'utilisateur à effectuer des sauvegardes incrémentielles de ses données Amazon S3 en utilisant EventBridge les règles Amazon : `events:DescribeRule` `events:EnableRule` `events:PutRule` ,`events:DeleteRule` ,`events:PutTargets` ,`events:RemoveTargets` ,,`events:ListTargetsByRule` , `events:DisableRule` `cloudwatch:GetMetricData` , et`events:ListRules` .	

Modification	Description	Date
AWSBackupServiceRolePolicyForS3Restore : nouvelle politique	Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de restaurer ses compartiments Amazon S3 : `s3:CreateBucket s3:ListBucketVersions ,,s3:ListBucket , s3:GetBucketVersioning s3:GetBucketLocation , ets3:PutBucketVersioning .` Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de restaurer ses compartiments Amazon S3 : `s3:GetObject s3:GetObjectVersion s3:DeleteObject ,s3:PutObjectVersionAcl ,s3:GetObjectVersionAcl ,s3:GetObjectTagging ,s3:PutObjectTagging ,s3:GetObjectAcl , s3:PutObjectAcl s3:PutObject , ets3:ListMultipartUploadParts .` Les actions suivantes ont été ajoutées pour accorder à	17 février 2022

Modification	Description	Date
	l'utilisateur l'autorisation de chiffrer ses données Amazon S3 restaurées :`kms:Decrypt` ,`kms:DescribeKey` , et`kms:GenerateDataKey` .	
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajouté `s3:ListAllMyBuckets` pour autoriser l'utilisateur à consulter la liste de ses compartiments et à choisir ceux à attribuer à un plan de sauvegarde.	14 février 2022
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajouté `backup-gateway:ListVirtualMachines` pour accorder à l'utilisateur l'autorisation de consulter la liste de ses machines virtuelles et de choisir celles à attribuer à un plan de sauvegarde. Ajouté `backup-gateway:ListTagsForResource` pour accorder à l'utilisateur l'autorisation de répertorier les balises de ses machines virtuelles.	30 novembre 2021

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Ajouté `backup-gateway:Backup` pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs sauvegardes de machines virtuelles. AWS Backup également ajouté `backup-gateway:ListTagsForResource` pour accorder à l'utilisateur l'autorisation de répertorier les balises attribuées à ses sauvegardes de machines virtuelles.	30 novembre 2021
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajouté `backup-gateway:Restore` pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs sauvegardes de machines virtuelles.	30 novembre 2021

Modification	Description	Date
AWSBackupFullAccess – Mise à jour d'une politique existante	Ajout des actions suivantes pour autoriser les utilisateurs à utiliser AWS Backup Gateway pour sauvegarder, restaurer et gérer leurs machines virtuelles :backup-gateway:AssociateGatewayToServer ,,,,backup-gateway:CreateGateway ,backup-gateway:DeleteGateway ,backup-gateway:DeleteHypervisor ,backup-gateway:DisassociateGatewayFromServer ,backup-gateway:ImportHypervisorConfiguration ,backup-gateway:ListGateways ,backup-gateway:ListHypervisors ,backup-gateway:ListTagsForResource ,backup-gateway:ListVirtualMachines ,backup-gateway:PutMaintenanceStartTime ,backup-gateway:TagResource ,backup-gateway:TestHypervisorConfiguration ,backup-gateway:UntagResourc	30 novembre 2021

Modification	Description	Date
	e ,backup-gateway:UpdateGatewayInformation , etbackup-gateway:UpdateHypervisor .	
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les actions suivantes ont été ajoutées pour accorder à l'utilisateur l'autorisation de sauvegarder ses machines virtuelles : backup-gateway:ListGateways backup-gateway:ListHypervisors ,backup-gateway:ListTagsForResource , etbackup-gateway:ListVirtualMachines .	30 novembre 2021
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajouté dynamodb:ListTagsOfResource pour accorder à l'utilisateur l'autorisation de répertorier les balises de ses tables DynamoDB à sauvegarder à l'aide des fonctionnalités de sauvegarde avancées AWS Backup de DynamoDB.	23 novembre 2021

Modification	Description	Date
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Ajouté `dynamodb:StartAwsBackupJob` pour accorder à l'utilisateur l'autorisation de sauvegarder ses tables DynamoDB à l'aide de fonctionnalités de sauvegarde avancées. Ajouté `dynamodb:ListTagsOfResource` pour accorder à l'utilisateur l'autorisation de copier des balises depuis ses tables DynamoDB source vers ses sauvegardes.	23 novembre 2021
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajouté `dynamodb:RestoreTableFromAwsBackup` pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs tables DynamoDB sauvegardées à l'aide des fonctionnalités AWS Backup de sauvegarde avancées de DynamoDB.	23 novembre 2021

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajouté `dynamodb:RestoreTableFromAwsBackup` pour accorder aux utilisateurs les autorisations nécessaires pour restaurer leurs tables DynamoDB sauvegardées à l'aide des fonctionnalités AWS Backup de sauvegarde avancées de DynamoDB.	23 novembre 2021
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les actions ont été supprimées `backup:GetRecoveryPointRestoreMetadata` et `rds:DescribeDBSnapshots` parce qu'elles étaient redondantes. AWS Backup n'avait pas besoin des deux `backup:GetRecoveryPointRestoreMetadata` et `backup:Get*` dans le cadre de`AWSBackupOperatorAccess` . De plus, AWS Backup je n'avais pas besoin des deux `rds:DescribeDBSnapshots` et dans `rds:describeDBSnapshots` le cadre de`AWSBackupOperatorAccess` .	23 novembre 2021

Modification	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajout des nouvelles actions`elasticfilesystem:DescribeFileSystems` ,,`dynamodb:ListTables` ,`storagegateway:ListVolumes` ,`ec2:DescribeVolumes` ,, `ec2:DescribeInstances` `rds:DescribeDBInstances` `rds:DescribeDBClusters` , et `fsx:DescribeFileSystems` pour permettre aux clients de consulter et de choisir parmi une liste de leurs ressources AWS Backup prises en charge lors de la sélection des ressources à affecter à un plan de sauvegarde.	10 novembre 2021
AWSBackupAuditAccess : nouvelle politique	Ajouté `AWSBackupAuditAccess` pour accorder à l'utilisateur l'autorisation d'utiliser AWS Backup Audit Manager. Les autorisations incluent la possibilité de configurer des frameworks de conformité et de générer des rapports.	24 août 2021

Modification	Description	Date
AWSServiceRolePolicyForBackupReports : nouvelle politique	Ajouté `AWSServiceRolePolicyForBackupReports` pour accorder des autorisations pour un rôle lié à un service afin d'automatiser la surveillance des paramètres de sauvegarde, des tâches et des ressources afin de garantir la conformité avec les frameworks configurés par l'utilisateur.	24 août 2021
AWSBackupFullAccess – Mise à jour d'une politique existante	Ajouté `iam:CreateServiceLinkedRole` pour créer un rôle lié à un service (dans la mesure du possible) afin d'automatiser la suppression des points de récupération expirés pour vous. Sans ce rôle lié au service, il est AWS Backup impossible de supprimer les points de récupération expirés une fois que les clients ont supprimé le rôle IAM d'origine qu'ils ont utilisé pour créer leurs points de récupération.	5 juillet 2021

Modification	Description	Date
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajout de la nouvelle action permettant d'`dynamodb:DeleteBackup DeleteRecoveryPoint` autoriser l'automatisation de la suppression des points de restauration DynamoDB expirés en fonction des paramètres du cycle de vie de votre plan de sauvegarde.	5 juillet 2021
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les actions ont été supprimées `backup:GetRecoveryPointRestoreMetadata` et `rds:DescribeDBSnapshots` parce qu'elles étaient redondantes. AWS Backup n'avait pas besoin des deux `backup:GetRecoveryPointRestoreMetadata` et, dans `backup:Get*` le cadre de `AWSBackupOperatorAccess` Also, AWS Backup n'avait pas besoin des deux `rds:DescribeDBSnapshots` et dans `rds:describeDBSnapshots` le cadre de `AWSBackupOperatorAccess`	25 mai 2021

Modification	Description	Date
AWSBackupOperatorAccess – Mise à jour d'une politique existante	Les actions ont été supprimées `backup:GetRecoveryPointRestoreMetadata` et `rds:DescribeDBSnapshots` parce qu'elles étaient redondantes. AWS Backup n'avait pas besoin des deux `backup:GetRecoveryPointRestoreMetadata` et `backup:Get*` dans le cadre de`AWSBackupOperatorAccess` . De plus, AWS Backup je n'avais pas besoin des deux `rds:DescribeDBSnapshots` et dans `rds:describeDBSnapshots` le cadre de`AWSBackupOperatorAccess` .	25 mai 2021
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajout de la nouvelle action `fsx:TagResource` permettant d'accorder `StartRestoreJob` l'autorisation d'appliquer des balises aux systèmes de fichiers Amazon FSx pendant le processus de restauration.	24 mai 2021

Modification	Description	Date
AWSBackupServiceRolePolicyForRestores – Mise à jour d'une politique existante	Ajout des nouvelles actions `ec2:DescribeImages` et `ec2:DescribeInstances` `StartRestoreJob` autorisation vous permettant de restaurer des instances Amazon EC2 à partir de points de récupération.	24 mai 2021
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Ajout de la nouvelle action `fsx:CopyBackup` pour accorder `StartCopyJob` l'autorisation de copier les points de récupération Amazon FSx entre les régions et les comptes.	12 avril 2021
AWSBackupServiceLinkedRolePolicyForBackup – Mise à jour d'une politique existante	Ajout de la nouvelle action `fsx:CopyBackup` pour accorder `StartCopyJob` l'autorisation de copier les points de récupération Amazon FSx entre les régions et les comptes.	12 avril 2021
AWSBackupServiceRolePolicyForBackup – Mise à jour d'une politique existante	Mis à jour pour répondre aux exigences suivantes : AWS Backup Pour créer une sauvegarde d'une table DynamoDB chiffrée, vous devez ajouter les `kms:Decrypt` autorisations `kms:GenerateDataKey` et le rôle IAM utilisé pour la sauvegarde.	10 mars 2021

Modification	Description	Date
AWSBackupFullAccess – Mise à jour d'une politique existante	Mis à jour pour répondre aux exigences suivantes : À utiliser AWS Backup pour configurer des sauvegardes continues pour votre base de données Amazon RDS, vérifiez que l'autorisation d'API `rds:ModifyDBInstance` existe dans le rôle IAM défini par la configuration de votre plan de sauvegarde. Pour restaurer les sauvegardes continues Amazon RDS, vous devez ajouter l'autorisation `rds:RestoreDBInstanceToPointInTime` au rôle IAM que vous avez soumis pour la tâche de restauration. Dans la AWS Backup console, pour décrire la plage de temps disponible pour la point-in-time restauration, vous devez inclure l'autorisation d'`rds:DescribeDBInstanceAutomatedBackups` API dans votre politique gérée par IAM.	10 mars 2021

Modification	Description	Date
AWS Backup a commencé à suivre les modifications	AWS Backup a commencé à suivre les modifications apportées à ses politiques AWS gérées.	10 mars 2021

Utilisation des rôles liés aux services pour AWS Backup

AWS Backup utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Rubriques

- Utilisation de rôles pour sauvegarder et copier
- Utilisation des rôles pour AWS Backup Audit Manager
- Utilisation des rôles pour les tests de la restauration

Utilisation de rôles pour sauvegarder et copier

AWS Backup utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Backup car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Backup définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Backup peut assumer ses rôles. Les autorisations définies comprennent la politique d’approbation et la politique d’autorisation. De plus, cette politique d’autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Backup ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Backup

AWS Backup utilise le rôle lié au service nommé AWSServiceRoleForBackup— Fournit des AWS Backup autorisations pour répertorier les ressources que vous pouvez sauvegarder et pour copier des sauvegardes.

AWS Backup utilise également le rôle pour supprimer toutes les sauvegardes pour tous les types de ressources à l'exception d'Amazon EC2.

Le rôle AWSServiceRoleForBackup lié à un service fait confiance aux services suivants pour assumer le rôle :

- `backup.amazonaws.com`

Pour consulter les autorisations associées à cette politique, reportez-vous AWSBackupServiceLinkedRolePolicyforBackupà la référence des politiques AWS gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Backup

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous listez des ressources à sauvegarder, que vous configurez une sauvegarde entre comptes ou que vous effectuez des sauvegardes dans le AWS Management Console AWS CLI, le ou l' AWS API, vous AWS Backup créez le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous listez des ressources à sauvegarder, que vous configurez une sauvegarde entre comptes ou que vous effectuez des sauvegardes, vous AWS Backup créez à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Backup

AWS Backup ne vous permet pas de modifier le rôle AWSServiceRoleForBackup lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Backup

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyer un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Tout d'abord, vous devez supprimer tous vos points de récupération. Ensuite, vous devez supprimer tous vos coffres-forts de sauvegarde.

> **Note**
>
> Si le AWS Backup service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Backup les ressources utilisées par AWSServiceRoleForBackup (console)

1. Pour supprimer tous vos points de récupération et coffres-forts de sauvegarde (à l'exception de votre coffre-fort par défaut), suivez la procédure décrite dans Suppression d'un coffre-fort de sauvegarde.
2. Pour supprimer votre coffre-fort par défaut, utilisez la commande suivante dans l' AWS CLI :

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

Pour supprimer AWS Backup les ressources utilisées par le AWSServiceRoleForBackup (AWS CLI)

1. Pour supprimer tous vos points de récupération, utilisez delete-recovery-point.
2. Pour supprimer tous vos coffres-forts de sauvegarde, utilisez `delete-backup-vault`.

Pour supprimer AWS Backup les ressources utilisées par AWSServiceRoleForBackup (API)

1. Pour supprimer tous vos points de récupération, utilisez `DeleteRecoveryPoint`.
2. Pour supprimer tous vos coffres-forts de sauvegarde, utilisez `DeleteBackupVault`.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForBackup service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Backup

AWS Backup prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Fonctionnalités et régions prises en charge par AWS Backup.

Utilisation des rôles pour AWS Backup Audit Manager

AWS Backup utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Backup car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Backup définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Backup peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Backup ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Backup

AWS Backup utilise le rôle lié au service nommé AWSServiceRoleForBackupReports— Permet de créer AWS Backup des contrôles, des cadres et des rapports.

Le rôle AWSServiceRoleForBackupReports lié à un service fait confiance aux services suivants pour assumer le rôle :

- `backup.amazonaws.com`

Pour consulter les autorisations associées à cette politique, reportez-vous AWSServiceRolePolicyForBackupReportsà la référence des politiques AWS gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Backup

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un framework ou un plan de rapport dans l' AWS Management Console AWS API AWS CLI, vous AWS Backup créez le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un framework ou un plan de rapport, AWS Backup crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Backup

AWS Backup ne vous permet pas de modifier le rôle AWSServiceRoleForBackupReports lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Backup

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyer un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Vous devez supprimer tous les frameworks et plans de rapports.

> **Note**
>
> Si le AWS Backup service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Backup les ressources utilisées par AWSServiceRoleForBackupReports (console)

1. Pour supprimer tous les frameworks, consultez Suppression des cadres.
2. Pour supprimer tous les plans de rapport, consultez Suppression de plans de rapport.

Pour supprimer AWS Backup les ressources utilisées par le AWSServiceRoleForBackupReports (AWS CLI)

1. Pour supprimer tous les cadres, utilisez delete-framework.
2. Pour supprimer tous les plans de rapport, utilisez delete-report-plan.

Pour supprimer AWS Backup les ressources utilisées par AWSServiceRoleForBackupReports (API)

1. Pour supprimer tous les frameworks, utilisez DeleteFramework.
2. Pour supprimer tous les plans de rapport, utilisez DeleteReportPlan.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForBackupReports service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Backup

AWS Backup prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Fonctionnalités et régions prises en charge par AWS Backup.

Utilisation des rôles pour les tests de la restauration

AWS Backup utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Backup Les rôles liés au service sont prédéfinis par AWS Backup et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Backup car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Backup définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Backup peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Backup ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS Backup

AWS Backup utilise le rôle lié au service nommé AWSServiceRolePolicyForBackupRestoreTesting— Fournit des autorisations de sauvegarde pour effectuer des tests de restauration.

Le rôle AWSServiceRolePolicyForBackupRestoreTesting lié à un service fait confiance aux services suivants pour assumer le rôle :

- `backup.amazonaws.com`

Pour consulter les autorisations associées à cette politique, reportez-vous AWSServiceRolePolicyForBackupRestoreTestingà la référence des politiques AWS gérées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AWS Backup

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous effectuez des tests de restauration dans le AWS Management Console AWS CLI, le ou l' AWS API, vous AWS Backup créez le rôle lié au service pour vous.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour de plus amples informations, veuillez consulter Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous effectuez un test de restauration, AWS Backup crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Backup

AWS Backup ne vous permet pas de modifier le rôle AWSServiceRolePolicyForBackupRestoreTesting lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire

référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Backup

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer votre rôle lié à un service avant de pouvoir le supprimer manuellement.

Nettoyer un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Vous devez supprimer tous les plans de test de la restauration.

> **Note**
>
> Si le AWS Backup service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS Backup les ressources utilisées par AWSServiceRolePolicyForBackupRestoreTesting (console)

- Pour supprimer tous les plans de test de la restauration, consultez Tests de restauration.

Pour supprimer AWS Backup les ressources utilisées par le AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI)

- Pour supprimer les plans de test de la restauration, utilisez `delete-restore-testing-plan`.

Pour supprimer AWS Backup les ressources utilisées par AWSServiceRolePolicyForBackupRestoreTesting (API)

- Pour supprimer les plans de test de la restauration, utilisez `DeleteRestoreTestingPlan`.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRolePolicyForBackupRestoreTesting service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS Backup

AWS Backup prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Fonctionnalités et régions prises en charge par AWS Backup.

Prévention du cas de figure de l'adjoint désorienté entre services

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

Nous vous recommandons d'utiliser les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans les politiques de ressources afin de limiter les autorisations à la ressource octroyées par AWS Backup à un autre service. Si vous utilisez les deux clés de contexte de condition globale, la valeur `aws:SourceAccount` et le compte de la valeur `aws:SourceArn` doit utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de politique.

La valeur de `aws:SourceArn` doit être un coffre-fort AWS Backup lorsque vous utilisez AWS Backup pour publier des rubriques Amazon SNS en votre nom.

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

Sécurité de l'infrastructure dans AWS Backup

En tant que service géré, AWS Backup il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont l' AWS infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS Backup via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2 ou version ultérieure. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Intégrité des données dans AWS Backup

AWS Backup objectif d'intégrité des données

AWS Backup cherche à maintenir l'intégrité lors de la transmission, du stockage et du traitement de vos données. AWS Backup traite les données des ressources stockées comme des informations critiques indépendantes du contenu, dans la mesure où nous offrons le même niveau élevé de sécurité aux clients, quel que soit le type de données que vous stockez. Nous sommes vigilants quant à la sécurité de nos clients et avons mis en place des mesures techniques et physiques sophistiquées contre les accès non autorisés. Vous gardez le contrôle total sur la manière dont vos données sont classées, sur les régions dans lesquelles vous les stockez et sur la manière dont vous contrôlez, archivez et protégez vos données contre toute divulgation.

AWS Backup implémentation de l'intégrité des données

AWS Backup travaille de concert avec d'autres services AWS et avec Amazon pour préserver l'intégrité des données qu'il stocke et avec lesquelles il interagit. Les outils utilisés peuvent varier et peuvent inclure (sans s'y limiter) :

- Validation continue des objets par rapport au total de contrôle pour empêcher la corruption des objets
- Totaux de contrôle internes pour confirmer l'intégrité des données en transit et au repos
- Totaux de contrôle calculés sur les données contenues dans les sauvegardes créées à partir du magasin principal
- Tentative automatique de restauration des niveaux normaux de redondance du stockage d'objets en cas de corruption du disque ou de détection d'une défaillance de l'appareil
- Stockage redondant des données sur plusieurs sites physiques
- Amélioration de la durabilité des objets sur plusieurs zones de disponibilité lors de l'écriture initiale, associée à une réplication ultérieure en cas d'indisponibilité de l'appareil ou de détection d'une corruption des bits
- Totaux de contrôle sur l'ensemble du trafic réseau pour détecter la corruption des paquets de données lors du stockage ou de la récupération de données

AWS Backup stocke nativement les données pour Amazon DynamoDB avec des fonctionnalités avancées, Amazon EFS, Amazon S3, Amazon Timestream et les machines virtuelles exécutées avec VMware connectées via Backup Gateway. AWS Backup facilite les sauvegardes des données stockées avec d'autres services, notamment Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon FSx pour Windows File Server, Amazon FSx pour Lustre, Amazon FSx pour OpenZFS, Amazon FSx pour ONTAP, Amazon Neptune, Amazon RDS et NetApp Amazon Redshift.

Confirmation objective et audit de l'intégrité des données AWS Backup

Les données stockées directement par AWS Backup et celles stockées en partenariat avec les autres AWS services avec lesquels ils AWS Backup interagissent sont soumises au processus rigoureux d'Amazon Simple Storage Service (Amazon S3) qui sous-tend cette intégrité des données. Cette intégrité est confirmée par un auditeur tiers indépendant par le biais d'un rapport d'audit annuel du SOC disponible AWS Artifact dans le AWS Management Console.

Retenues légales et AWS Backup

Une conservation légale est un outil administratif qui permet d'empêcher la suppression de sauvegardes pendant une conservation. Tant que la conservation est en place, les sauvegardes sous conservation ne peuvent pas être supprimées et les politiques de cycle de vie susceptibles de

modifier le statut des sauvegardes (comme le passage à un état `Deleted`) sont retardées jusqu'à ce que la conservation légale soit levée. Une sauvegarde peut avoir plusieurs conservations légales.

Des blocages légaux peuvent être appliqués à une ou plusieurs sauvegardes (également appelées points de restauration) créées AWS Backup si leur cycle de vie le permet. Un type de sauvegarde appelé sauvegarde continue a un cycle de vie maximal de 35 jours. Les blocages légaux ne prolongent pas le cycle de vie d'une sauvegarde continue.

Lorsqu'une conservation légale est créée, elle peut prendre en compte des critères de filtrage spécifiques, tels que les types de ressources et les ID des ressources. En outre, vous pouvez définir la plage de dates de création des sauvegardes que vous souhaitez inclure dans une conservation légale. Les conservations légales et les sauvegardes ont une relation de type « plusieurs à plusieurs », ce qui signifie qu'une sauvegarde peut avoir plusieurs conservations légales et qu'une conservation légale peut inclure plusieurs sauvegardes. Chaque compte peut avoir un maximum de 50 conservations légales actives à un moment donné.

Les conservations légales ne s'appliquent qu'à la sauvegarde d'origine sur laquelle elles sont placées. Lorsqu'une sauvegarde est copiée entre régions ou comptes (si la ressource la prend en charge), elle n'est pas conservée ni conservée légalement. Une conservation légale, comme d'autres ressources, possède un ARN (Amazon Resource Name) unique qui lui est associé. Seuls les points de récupération créés par AWS Backup peuvent faire partie d'une détention légale.

Notez que si AWS Backup Vault Lock fournit des protections et une immuabilité supplémentaires à un coffre-fort, une conservation légale fournit une protection supplémentaire contre la suppression de sauvegardes individuelles (points de récupération). La conservation légale n'expire pas et les données de la sauvegarde sont conservées indéfiniment. La suspension reste active jusqu'à ce qu'elle soit levée par un utilisateur disposant des autorisations suffisantes.

Création d'une conservation légale

Lorsqu'une conservation légale est créée, elle ne contient que des points de récupération déjà créés. Les sauvegardes (points de récupération) dont le statut est `EXPIRED` ou `DELETING` ne seront pas incluses dans la conservation légale. Les points de récupération (sauvegardes) dont le statut est `CREATING` peuvent ne pas être inclus dans la conservation légale, selon le moment où ils sont terminés.

Des blocages légaux peuvent être ajoutés par les utilisateurs disposant des autorisations IAM requises.

Création d'une conservation légale juridique à l'aide de la console

Pour créer une conservation légale

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le tableau de bord situé à gauche de la console, trouvez Mon compte. Choisissez Legal Holds.
3. Choisissez Ajouter une conservation légale.
4. Trois panneaux s'affichent : Détails de la conservation légale, étendue de la conservation légale et balises de conservation légales.

    a. Sous Détails relatifs à la conservation légale, entrez le titre de la conservation légale et une description de la conservation dans les zones de texte prévues à cet effet.

    b. Dans le panneau Portée de la conservation légale, choisissez la manière dont vous souhaitez sélectionner la ressource à inclure dans la conservation légale. Lorsque vous créez une suspension, vous choisissez la méthode utilisée pour sélectionner les ressources relevant de la retenue légale. Vous pouvez choisir d'inclure l'une des méthodes suivantes :

    - Types et identifiants de ressources spécifiques
    - Sélectionnez les coffres-forts de sauvegarde
    - Tous les types de ressources ou tous les coffres-forts de sauvegarde de votre compte

    c. Spécifiez la plage de dates de votre conservation légale. Entrez les dates au format YYYY:MM:DD (les dates sont inclusives).

    d. Vous pouvez éventuellement ajouter des balises pour la mise en attente sous Balises de conservation légales. Les balises peuvent aider à classer la conservation pour une référence et une organisation futures. Vous pouvez ajouter jusqu'à 50 balises au total.
5. Lorsque vous êtes satisfait de la configuration de votre nouvelle conservation légale, cliquez sur le bouton Ajouter une nouvelle conservation.

Créez une conservation légale à l'aide du AWS CLI

Vous pouvez créer une suspension légale à l'aide de la create-legal-holdcommande.

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
```

```
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Affichage des conservations légales

Vous pouvez consulter les informations relatives à la conservation légale dans la AWS Backup console ou par programmation.

Afficher les réservations légales à l'aide de la console

Pour consulter toutes les conservations légales d'un compte à l'aide de la console Backup,

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans la partie gauche du tableau de bord, sous Mon compte, cliquez sur Conservations légales.
3. La table conservation légale affiche le titre, le statut, la description, l'ID et la date de création des conservations existantes. Cliquez sur le carat (flèche vers le bas) à côté de l'en-tête de la table pour filtrer la table en fonction de la colonne sélectionnée.

Affichage des conservations légales par programmation

Pour afficher tous les blocages légaux par programmation, vous pouvez utiliser les appels d'API suivants : ListLegalHoldset. GetLegalHold

Le modèle JSON suivant peut être utilisé pour`GetLegalHold`.

```
GET /legal-holds/{legalHoldId} HTTP/1.1

Request

empty body

Response

{
    Title: string,
    Status: LegalHoldStatus,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
```

```
    CanceledTime: number,

   ResourceSelection: {
        VaultArns: [ string ]
        Resources: [ string ]
   },
   ResourceFilters: {
        DateRange: {
          FromDate: number,
          ToDate: number
        }
   }
}
```

Le modèle JSON suivant peut être utilisé pour`ListLegalHolds`.

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken


Request

empty body
url params:
  MaxResults: number  // optional,
  NextToken: string  // optional

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING
maxResults: 1-1000



Response

{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
```

```
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
  ]

}
```

Les valeurs d'état possibles sont les suivantes.

État	Description
CRÉATION	Les points de récupération demandés sont en cours de conservation et les demandes de suppression de ces points de récupérat ion peuvent réussir puisque la création de la conservation n'est pas terminée.
ACTIF	La conservation légale a été créée. Tous les points de récupération répertoriés dans le cadre de cette conservation légale sont conservés.
CANCELLING	Les conservations légales sont en cours de suppression et les demandes de suppression des points de récupération conservés peuvent aboutir.
ANNULÉE	La conservation légale est entièrement libérée et n'a plus aucun effet. Les points de récupérat ion peuvent être supprimés.

Libération d'une conservation légale

Les blocages légaux restent en vigueur jusqu'à ce qu'ils soient supprimés par un utilisateur disposant des autorisations suffisantes. La suppression d'une conservation légale est également connue sous le nom d'annulation, de suppression ou de libération d'une conservation légale. La suppression d'une conservation légale l'élimine de toutes les sauvegardes auxquelles elle était attachée. Toutes les

sauvegardes qui ont expiré pendant la période de conservation légale sont supprimées dans les 24 heures suivant la levée de la suspension légale.

Libération d'une conservation légale à l'aide de la console

Pour relâcher un blocage à l'aide de la console

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Entrez la description que vous souhaitez associer à la version.
3. Vérifiez les détails, puis cliquez sur Lever la conservation.
4. Lorsque la boîte de dialogue Lever la conservation apparaît, confirmez votre intention de lever la conservation en saisissant `confirm` dans la zone de texte.

    - Cochez la case indiquant que vous annulez la conservation.

Sur la page Conservations légales, vous pouvez voir toutes vos conservations. Si la libération est réussie, le statut de cette conservation sera affiché comme `Released`.

Libérer une suspension légale par le biais d'un programme

Pour supprimer un blocage par programmation, utilisez l'appel d'API. CancelLegalHold

Utilisez le modèle JSON suivant.

```
DELETE /legal-holds/{legalHoldId}


Request

{
   CancelDescription: String
   DeleteAfterDays: number // optional
}


DeleteAfterDays: optional.
  Defaults to 180 days. how long to keep legal hold record after canceled.
  This applies to the actual legal hold record only.
  Recovery points are unlocked as soon as cancelation processes and are not subject to
 this date.
```

```
Response

Empty body

200 if successful
other standard codes
```

AWS PrivateLink

AWS PrivateLink vous permet d'établir une connexion privée entre votre cloud privé virtuel (« VPC ») et les AWS Backup points de terminaison en créant un point de terminaison VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder de manière privée aux AWS Backup API en limitant tout le trafic réseau entre votre VPC AWS Backup et le réseau Amazon.

AWS PrivateLink vous permet d'accéder aux AWS Backup opérations de manière privée sans passerelle Internet, appareil NAT, connexion VPN ou AWS Direct Connect connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les points de terminaison d' AWS Backup API Vos instances n'ont pas non plus besoin d'adresses IP publiques pour utiliser les opérations d'API AWS Backup et d'API de passerelle de sauvegarde disponibles. Le trafic entre votre VPC et celui qui AWS Backup ne quitte pas le réseau Amazon.

Pour plus d'informations sur les points de terminaison d'un VPC, consultez Points de terminaison de VPC d'interface (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de terminaison d'un VPC Amazon

Avant de configurer un point de terminaison VPC d'interface pour les AWS Backup points de terminaison, consultez les propriétés et les limites du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

Toutes les AWS Backup opérations relatives à la gestion des ressources Amazon Backup sont disponibles depuis votre VPC à l'aide de. AWS PrivateLink

Les politiques de point de terminaison d'un VPC sont prises en charge pour les points de terminaison de Backup. Par défaut, l'accès complet aux opérations de Backup est autorisé via le point de terminaison. Pour plus d’informations, consultez Contrôle de l’accès aux services avec points de terminaison d’un VPC dans le Guide de l’utilisateur Amazon VPC.

Création d'un point de AWS Backup terminaison VPC

Vous pouvez créer un point de terminaison VPC à AWS Backup l'aide de la console Amazon VPC ou de la (AWS Command Line Interface CLI).AWS Pour de plus amples informations, veuillez consulter Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC pour AWS Backup utiliser le nom du service. `com.amazonaws.region.backup`

Dans les régions Chine (Beijing) et Chine (Ningxia), le nom du service doit être `cn.com.amazonaws.region.backup`.

Pour les points de terminaison Backup gateway, utilisez `com.amazonaws.region.backup-gateway`.

Les ports TCP suivants doivent être autorisés dans le groupe de sécurité lors de la création d'un point de terminaison d'un VPC pour Backup gateway :

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

Protocole	Port	Direction	Source	Destination	Utilisation
TCP	443 (HTTPS)	Sortant	Backup Gateway	AWS	Pour les communications entre Backup Gateway et le point de terminaison du AWS service

Utilisation du point de terminaison d'un VPC

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API AWS Backup au point de terminaison VPC en utilisant son nom DNS par défaut pour la AWS région, par exemple. `backup.us-east-1.amazonaws.com`

Toutefois, pour les régions Chine (Pékin) et Chine (Ningxia) Régions AWS, les demandes d'API doivent être effectuées avec le point de terminaison VPC `backup.cn-north-1.amazonaws.com.cn` en utilisant `backup.cn-northwest-1.amazonaws.com.cn` et, respectivement.

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une stratégie de point de terminaison de VPC

Vous pouvez attacher une politique de point de terminaison à votre point de terminaison d'un VPC qui contrôle l'accès à l'API Amazon Backup. La politique spécifie :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

> **Important**
>
> Lorsqu'une politique autre que celle par défaut est appliquée à un point de terminaison VPC d'interface AWS Backup pour, certaines demandes d'API ayant échoué, telles que celles `RequestLimitExceeded` émanant de, peuvent ne pas être enregistrées sur Amazon AWS CloudTrail ou sur Amazon. CloudWatch

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions AWS Backup

Voici un exemple de politique de point de terminaison pour AWS Backup. Lorsqu'elle est attachée à un point de terminaison, cette politique donne accès aux AWS Backup actions répertoriées pour tous les principes sur toutes les ressources.

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

Exemple : politique de point de terminaison d'un VPC qui refuse tout accès à partir d'un compte AWS spécifié

La politique de point de terminaison VPC suivante refuse au AWS compte 123456789012 tout accès aux ressources utilisant le point de terminaison. La politique autorise toutes les actions provenant d'autres comptes.

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

Pour plus de détails sur les réponses d'API disponibles, consultez le guide de l'API.

AWS Backup Availability prend actuellement en charge les points de terminaison VPC dans les régions suivantes : AWS

- Région US East (Ohio)
- Région USA Est (Virginie du Nord)
- Région USA Ouest (Oregon)
- Région US West (N. California)
- Région Afrique (Le Cap)
- Région Asie-Pacifique (Hong Kong)
- Région Asie-Pacifique (Mumbai)
- Région Asie-Pacifique (Osaka)
- Région Asie-Pacifique (Séoul)
- Région Asie-Pacifique (Singapour)
- Région Asie-Pacifique (Sydney)
- Région Asie-Pacifique (Tokyo)
- Région Canada (Centre)
- Région Europe (Frankfurt)
- Région Europe (Irlande)
- Région Europe (Londres)
- Région Europe (Paris)
- Région Europe (Stockholm)
- Europe (Milan) Region
- Middle East (Bahrain) Region
- Région Amérique du Sud (São Paulo)
- Région Asie-Pacifique (Jakarta)
- Région Asie-Pacifique (Osaka)
- Région Chine (Beijing)
- Région Chine (Ningxia)
- AWS GovCloud (USA Est)
- AWS GovCloud (US-Ouest)

> **Note**
>
> AWS Backup pour VMware n'est pas disponible dans les régions de Chine (région de Chine (Pékin) et région de Chine (Ningxia)) ou dans la région Asie-Pacifique (Jakarta).

Résilience dans AWS Backup

AWS Backup prend très au sérieux sa résilience et la sécurité de vos données.

AWS Backup stocke vos sauvegardes avec au moins autant de résilience et de durabilité que le AWS service d'origine de votre ressource vous offrirait, si vous les sauvegardiez sur place.

AWS Backup est conçu pour utiliser l'infrastructure AWS mondiale afin de répliquer vos sauvegardes sur plusieurs zones de disponibilité pour une durabilité de 99,999999999 % (11 neuf) par année, à condition que vous respectiez la documentation en vigueur. AWS Backup

AWS Backup chiffre vos plans de sauvegarde au repos et les sauvegarde en permanence. Vous pouvez également restreindre l'accès à vos plans de sauvegarde à l'aide des informations d'identification et des politiques AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Authentification, Contrôle d'accès et Bonnes pratiques de sécurité dans IAM.

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. AWS Backup stocke vos sauvegardes dans toutes les zones de disponibilité. 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, consultez Contrat de niveau de service (SLA)AWS Backup.

En outre, il AWS Backup vous permet de copier vos sauvegardes d'une région à l'autre pour une résilience encore plus grande. Pour plus d'informations sur la fonctionnalité de copie AWS Backup entre régions, voir Création d'une copie de sauvegarde.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

AWS Backup quotas

Les quotas suivants s'appliquent lorsque vous travaillez avec AWS Backup. De nombreux AWS Backup quotas sont ajustables s'ils sont autorisés par le service de type de ressource. Pour demander un ajustement de quota, décrivez votre cas d'utilisation à AWS Support.

AWS Backup quotas

Ressource	Quota	Remarques
Nombre de coffres-forts de sauvegarde par région par compte	300	Vous pouvez demander un ajustement.
Nombre de points de récupération par coffre-fort de sauvegarde	1 000 000	Vous pouvez demander un ajustement.
Nombre de plans de sauvegarde par région par compte	300	Vous pouvez demander un ajustement.
Nombre de versions par plan de sauvegarde	2 000	Vous pouvez demander un ajustement.
Nombre d'affectations de ressources par plan de sauvegarde	100	Non ajustable
Nombre de tâches de sauvegarde actives par compte	Illimité	
Nombre de copies de sauvegarde simultanées par compte sortant vers une région de destination	100	Vous pouvez demander un ajustement pour certaines ressources (actuellement les machines virtuelles, les bases de données Advanced DynamoDB, Timestrea

Ressource	Quota	Remarques
		m, Amazon EFS et SAP HANA sur des instances Amazon EC2).
Nombre de copies simultanées par coffre-fort de sauvegarde de destination dans le compte une fois la limite (entrée ci-dessus) atteinte	5	Non ajustable
Nombre de copies entre comptes simultanées pouvant être effectuées de la même ressource vers la même région de destination	30	Non ajustable.
Nombre de tâches de sauvegarde et de copie simultanées par ressource	1	Non ajustable. Ce quota vous aide à maintenir les performances de vos charges de travail.
Nombre de balises de métadonnées par sauvegarde	50	Vous ne pouvez pas demander d'ajustement. AWS impose ce quota à toutes les ressources. Consultez Limites et exigences de dénomination des balises dans la Référence générale AWS .
Nombre de balises par sélection de ressources dans une politique de sauvegarde entre comptes	30	Non ajustable. Des balises supplémentaires peuvent être incluses en utilisant plusieurs affectations de ressources ou des plans de sauvegarde.
Nombre d'hyperviseurs	10	Non ajustable

Ressource	Quota	Remarques
Nombre de conservations légales	50 par compte	Non ajustable
Nombre maximal de couches de sauvegarde imbriquées dans les piles d'applications	10	Non ajustable

AWS Backup des quotas de ressources Amazon Timestream

Ressource	Quota	Remarques
Nombre de tâches de sauvegarde Timestream simultanées par compte	4	Vous pouvez demander un ajustement.
Nombre de tâches de restauration Timestream simultanées par compte	1	Vous pouvez demander un ajustement.

Il existe des quotas pour une seule attribution de ressource dans une seule règle de sauvegarde. Vous pouvez créer un plan de sauvegarde avec plusieurs règles de sauvegarde.

AWS Backup Quotas d'Audit Manager

Ressource	Quota	Remarques
Nombre de frameworks par région par compte	15	Vous pouvez demander un ajustement.
Nombre de contrôles par région par compte	50	Vous pouvez demander un ajustement.
Nombre de plans de rapports par compte	20	Vous pouvez demander un ajustement.

Ressource	Quota	Remarques
Nombre de frameworks par plan de rapport	1 000	Non ajustable
Nombre maximum de comptes multiplié par régions dans un plan de rapport	300	Non ajustable

Quotas de plans de tests de la restauration

Ressource	Quota	Remarques
Plans de tests de la restauration	100	Non ajustable
Nombre de balises dans chaque plan	50	Non ajustable
Sélections par plan	30	Non ajustable
ARN par sélection de tests de la restauration	30	Non ajustable
Conditions par sélection	30	Comprend ceux contenus dans `StringEquals` et `StringNotEquals` .
Sélecteurs de coffre-fort par sélection de tests de la restauration	30	Non ajustable
Valeur maximale (en jours) de la fenêtre de sélection	365 jours	
Limites des heures de la fenêtre de démarrage	Minimum : 1 heure ; maximum : 168 heures	

Ressource	Quota	Remarques
Nombre maximal de caractères pour le nom du plan de tests de la restauration	50 caractères	Alphanumérique et traits de soulignement, pas d'espaces blancs
Nombre maximal de caractères pour le nom de la sélection de tests de la restauration	50 caractères	Alphanumérique et traits de soulignement, pas d'espaces blancs

AWS Backup gateway quotas

Ressource	Quota	Remarques
Tâches de sauvegarde ou de restauration par passerelle	4	Vous ne pouvez pas demander d'ajustement. Créez plutôt d'autres passerelles et connectez-les à votre hyperviseur.

Lorsque vous gérez des sauvegardes sur plusieurs comptes à l'aide de AWS Organizations, vous pouvez être confronté à des quotas qui s' AWS Organizations imposent. Pour ces quotas, consultez Quotas pour AWS Organizations dans le Guide de l'utilisateur AWS Organizations .

Vous pouvez également être confronté à des quotas imposés par un service AWS Backup pris en charge, notamment :

- Amazon Elastic File System
- Amazon Elastic Block Store
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- Amazon FSx pour Lustre

- Amazon FSx for Windows File Server
- Amazon DocumentDB
- Amazon Neptune
- Amazon Simple Storage Service
- Amazon Timestream

Surveillance

AWS Backup fonctionne avec d'autres AWS outils pour vous permettre de surveiller ses charges de travail. Ces outils incluent :

- AWS Backup tableaux de bord de console
  - Le tableau de bord des tâches permet de surveiller l'état de la tâche ; vous pouvez consulter les métriques indiquant les réussites et les échecs des tâches, filtrés par motif, compte, région et type de ressource.
  - Le tableau de bord des jobs est disponible dans les régions où AWS Backup Audit Manager est pris en charge. Consultez Disponibilité des fonctionnalités par Région AWS pour ces régions. Toutes les autres régions pourront accéder au CloudWatch Tableau de bord.
- Amazon CloudWatch et Amazon EventBridge pour surveiller AWS Backup les processus.
  - Vous pouvez l'utiliser CloudWatch pour suivre les métriques, créer des alarmes et consulter des tableaux de bord.
  - Vous pouvez l'utiliser EventBridge pour afficher et surveiller les AWS Backup événements.

  Pour plus d'informations, consultez Surveillance des AWS Backup événements à l'aide d'Amazon EventBridge et .
- AWS CloudTrailpour surveiller les appels AWS Backup d'API. Vous pouvez identifier l'heure, l'adresse IP source, les utilisateurs et les comptes qui effectuent ces appels. Pour plus d'informations, consultez Journalisation des appels d' AWS Backup API avec CloudTrail.
- Amazon Simple Notification Service (Amazon SNS) pour vous abonner à des sujets AWS Backup connexes tels que les événements de sauvegarde, de restauration et de copie. Pour plus d'informations, consultez Options de notification avec AWS Backup.

AWS Backup tableaux de bord de console

> **Note**
>
> Le tableau de bord des jobs est disponible dans toutes les régions où AWS Backup Audit Manager est pris en charge. Consultez Disponibilité des fonctionnalités par Région AWS pour ces régions. Toutes les autres régions pourront accéder au CloudWatch Tableau de bord.

Rubriques

Présentation des tableaux de bord de sauvegarde

AWS Backup fournit un tableau de bord des tâches dans la console pour vous aider à surveiller l'état de vos tâches de sauvegarde, de copie et de restauration. Les mêmes données affichées visuellement dans la console peuvent être récupérées dans la ligne de commande via AWS CLI.

Le tableau de bord des tâches peut être utilisé pour identifier les problèmes liés aux tâches de sauvegarde, de copie et de restauration par le biais d'une surveillance au niveau de l'organisation ou d'un compte membre. Grâce à ces informations, vous pouvez identifier et diagnostiquer les événements et les problèmes éventuels afin de garantir la fidélité de vos activités.

Le tableau de bord des tâches peut afficher deux périodes. Par défaut, les données des 14 derniers jours sont affichées, mais vous pouvez modifier la vue pour afficher les 7 derniers jours. Si vous modifiez la période, les données seront mises à jour pour refléter le nouvel intervalle de temps.

Notez que le tableau de bord affiche les données jusqu'à la date la plus récente à minuit (UTC), c'est-à-dire que les données du jour en cours ne sont pas incluses. Le tableau de bord est mis à jour quotidiennement entre 1 h 30 et 2 h 30 (UTC) environ.

Affichage du tableau de bord des tâches

Pour consulter le tableau de bord des tâches, connectez-vous à la AWS Backup console et sélectionnez Tableaux de bord des tâches dans la barre de navigation de gauche.

Sur la page du tableau de bord des tâches, vous pouvez sélectionner une tâche de sauvegarde, de copie ou de restauration.

La présentation du tableau de bord des tâches affiche une vue agrégée de la période spécifiée d'activité des tâches, y compris les tâches terminées, terminées avec des problèmes, expirées et ayant échoué. Par défaut, les données des 14 derniers jours sont affichées, mais vous pouvez modifier la vue pour afficher 7 jours.

> **Note**
>
> `Completed with issues` est le statut d'une tâche affiché dans la console qui indique qu'une tâche est terminée avec un message de statut.

État de la tâche

Le diagramme linéaire affiche les courbes de taux de réussite et d'échec des tâches au fil du temps. La courbe du taux de réussite indique une agrégation des tâches terminées et des tâches terminées avec problèmes. La courbe du taux d'échec indique la somme des tâches ayant échoué et expirées en fonction de la plage de temps spécifiée.

Les tâches non terminées ou n'ayant pas échoué (tâches avec un statut créées, en attente, en cours, abandonnées, abandonnées ou partielles) ne sont pas incluses ; les pourcentages totaux peuvent ne pas être égaux à 100 %.

Statut de la tâche au fil du temps

Avec le diagramme à barres, vous pouvez générer un diagramme à barres personnalisé qui indique le nombre de tâches dans chaque catégorie (terminées, terminées avec problèmes, ayant échoué et expirées), réparties par jours.

À l'aide des menus déroulants, choisissez le ou les statuts, les types de ressources et AWS les régions que vous souhaitez voir apparaître dans le graphique. Si vous souhaitez approfondir votre sélection, sélectionnez Afficher les tâches pour afficher une partie préfiltrée de la page de surveillance des tâches/entre comptes.

Vous pouvez placer le pointeur de la souris sur une barre pour afficher une fenêtre contextuelle qui affiche les données de tâches détaillées pour la date sélectionnée.

Tâches problématiques

Une tâche problématique est une tâche dont le statut est Échoué, Expiré ou Terminé avec des problèmes. Chaque diagramme affiche la métrique correspondante qui contient les comptes, les types de ressources ou les principales raisons qui contiennent le plus grand nombre de tâches problématiques.

L'affichage par défaut trie le widget du tableau de bord en fonction de la métrique spécifiée par ordre décroissant, en commençant par la métrique contenant le plus grand nombre de tâches problématiques associées à la métrique.

L'affichage des comptes les plus problématiques ne sera visible que dans les comptes qui y ont accès via Organizations, tels que les comptes administratifs et les comptes d'administrateur délégué. S'il est visible, vous pouvez survoler un compte pour afficher le nombre de tâches problématiques associées au compte choisi.

Vous pouvez sélectionner une barre dans le diagramme pour ouvrir une fenêtre contextuelle. Dans cette fenêtre, vous pouvez sélectionner un statut de tâche pour ouvrir un tableau de surveillance des tâches/entre comptes filtré en fonction du statut sélectionné.

Motifs de tâches problématiques

Le widget Principaux motifs problématiques indique la catégorie de code de message à laquelle appartiennent les messages d'erreur. Cependant, la catégorie peut ne pas expliquer les problèmes rencontrés par une tâche. Développez les catégories de codes de message ci-dessous pour plus de détails sur les messages ou les erreurs spécifiques que vos tâches peuvent rencontrer.

« ERREUR_VSS »

- « La tentative de sauvegarde Windows VSS a échoué car l'état de l'instance ou de l'agent SSM n'est pas valide ou les privilèges sont insuffisants. »
- « La tentative de sauvegarde Windows VSS a échoué en raison de privilèges insuffisants pour effectuer cette opération. »
- « La tentative de sauvegarde Windows VSS a échoué car le fichier ec2-vss-agent.exe n'est pas installé dans l'instance. »
- « Une erreur liée à la tâche de sauvegarde Windows VSS s'est produite lors d'une tentative de sauvegarde normale. »
- « La tentative de sauvegarde Windows VSS a échoué en raison d'un délai d'attente lors de la création d'instantanés compatible avec VSS. »
- « La tentative de sauvegarde Windows VSS a échoué en raison d'une version de Windows Server non prise en charge. Vous pouvez utiliser Windows Server 2012 ou une version ultérieure. »
- « La tentative de sauvegarde Windows VSS a échoué en raison d'un délai d'attente lors de la création d'instantanés compatible avec VSS. »

« LIMITE_DÉPASSÉE »

- « Limite d’abonnés dépassée : vous avez atteint le nombre maximal de sauvegardes simultanées, qui est de 300. Attendez que les autres tâches se terminent et réessayez. Vous pouvez également nous contacter pour AWS Support demander une augmentation de quota. »
- « Le nombre maximum autorisé d’instantanés en cours pour un seul volume est dépassé. »
- « Le nombre maximum autorisé d’instantanés actifs est dépassé. »
- « Impossible de créer plus de 20 instantanés utilisateur »
- « Le jeu de balises résultant ne doit pas comporter plus de 50 balises utilisateur. »
- « Vous avez atteint le maximum de sauvegardes prises en charge pour votre compte/base de données. Consultez Quotas dans le Guide du développeur Timestream pour plus d’informations. »
- « Vous avez atteint votre quota de 50 000 pour le nombre d’images publiques et privées autorisées dans cette région. Désenregistrez les images inutilisées ou demandez une augmentation de votre quota d’AMI. »
- « Votre sauvegarde a réussi, mais nous n'avons pas pu conserver NetworkInterfaces les métadonnées car leur taille dépassait nos limites internes. »
- « REGEX#limite d’abonnés dépassée »
- « REGEX#Plus de 50 balises spécifiées »
- « REGEX#peut avoir au maximum »

« ACCÈS_REFUSÉ »

- « Vous n’êtes pas autorisé à effectuer cette opération. »
- « Accès refusé en essayant d'appeler le AWS Backup service »
- « Les images de AWS Marketplace ne peuvent pas être copiées vers un autre AWS compte. »
- « La tâche de copie a échoué car le coffre-fort de sauvegarde de destination est chiffré avec la clé gérée par le service de sauvegarde par défaut. Le contenu de ce coffre-fort ne peut pas être copié. Seul le contenu d'un coffre-fort Backup chiffré par une AWS KMS clé peut être copié.
- Les instantanés chiffrés avec le ne Clé gérée par AWS peuvent pas être partagés. Spécifiez un autre instantané.
- « Les instantanés chiffrés avec la clé par défaut d’Amazon EBS ne peuvent pas être partagés
- « La tâche de copie a échoué. Les comptes source et de destination doivent être membres de la même organisation. »

- « REGEX#access refusé »
- « REGEX#non autorisé à »
- « REGEX #cannot » doit être assumé par AWS Backup
- « REGEX#n'a pas l'autorisation »
- « REGEX#autorisation manquante »

« TÂCHE_SIMULTANÉE »

- « La tâche de sauvegarde a échoué car une tâche était en cours d'exécution pour la même ressource. »

« FONCTIONNALITÉ_NON_ACTIVÉE »

- « La tâche de copie a échoué. La fonctionnalité de copie entre comptes n'est pas activée pour l'organisation actuelle. »

« TÂCHE_EXPIRÉE »

- « La tâche de sauvegarde a expiré avant d'être terminée. »

« CYCLE_DE_VIE_NON_VALIDE »

- « La tâche de copie a échoué. La rétention spécifiée dans la tâche ne se situe pas dans la plage spécifiée pour le coffre-fort de sauvegarde cible. »
- « REGEX#ne pourrait pas démarrer car il se trouve soit à l'intérieur, soit trop près de la fenêtre de maintenance hebdomadaire configurée »
- « REGEX#ne pourrait pas démarrer car il se trouve soit à l'intérieur, soit trop près de la fenêtre de sauvegarde automatisée »

« ÉTAT_INVALIDE »

- « REGEX#L'instance n'est pas dans l'état »
- « REGEX#pas dans l'état disponible »
- « REGEX#pas dans un état disponible »
- « REGEX#Volume d'instantané impossible »

« ERREUR_CLÉ_KMS »

- « La clé KMS est désactivée ou en attente de suppression ou l’accès à la clé KMS est refusé »
- « L’ID de clé donné n’est pas accessible »
- « La copie de l’instantané de l’AMI a échoué avec une erreur : l’ID de clé donné n’est pas accessible. Vous devez avoir des DescribeKey autorisations sur le « CMK » par défaut.
- « REGEX#clé kms »

« ERREUR_CLÉ_ACCÈS »

- « L'ID de clé d' AWS accès nécessite un abonnement au service »

« HYPERVISEUR_HORS-LIGNE »

- « Cette opération n’est pas valide pour l’hyperviseur spécifié car il n’est pas en ligne »

« RESSOURCE_INTROUVABLE »

- « Le volume spécifié est introuvable. »
- « La machine virtuelle est introuvable. »
- « L’ID de clé donné n’existe pas »
- « REGEX#n’existe pas »
- « REGEX#Impossible de trouver la ressource »
- « REGEX#Impossible de trouver le cryopode »
- « REGEX#Impossible de trouver un point de récupération »
- « REGEX#resource introuvable »
- « REGEX#plus disponible »
- « REGEX#non valide »

« RESSOURCE_NON_PRISE_EN_CHARGE »

- « REGEX#type de ressource non pris en charge »
- « REGEX#Type de ressource non pris en charge »

« ERREUR_COPIE_BALISE »

- « Nous ne sommes pas en mesure de copier les balises de ressources vers votre sauvegarde en raison d'un échec interne. »
- « Nous ne sommes pas en mesure de copier les balises de ressources vers votre sauvegarde car le point de récupération source ou de destination n'est pas disponible »

« JETON_EXPIRÉ »

- « Jeton expiré. Réessayez. »

« OPÉRATION_NON_PRISE_EN_CHARGE »

- « CreateSnapshot méthode non prise en charge sur l'hyperviseur lors de la création d'un instantané. Tâche de sauvegarde interrompue. »
- « UnsupportedOperation : Les copies de sauvegarde de Storage Gateway nécessitent un coffre-fort de sauvegarde créé par l'utilisateur et une clé CMK à destination. »
- « REGEX#Fonctionnalité non prise en charge pour le type de ressource fourni. »

« ERREUR_FATALE »

- « Une erreur interne s'est produite. »
- « La tâche de copie a rencontré une erreur fatale. Veuillez contacter le AWS Support pour obtenir de l'aide supplémentaire. »
- « La tâche de copie a rencontré une erreur fatale. »
- « REGEX#La tâche de sauvegarde a rencontré une erreur fatale »

Obtention des données du tableau de bord via AWS CLI

Vous pouvez utiliser la ligne de commande pour récupérer les mêmes données qui apparaissent dans la console. Utilisez l'une des commandes d'interface de ligne de commande suivantes :

- `list-backup-job-summaries`
- `list-copy-job-summaries`
- `list-restore-job-summaries`

Voici les paramètres valides que vous pouvez inclure dans chaque commande :

```
BackupJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

CopyJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

RestoreJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
AggregationPeriod: (string),
NextToken (string)
```

Cet exemple montre un exemple de demande dans lequel un utilisateur a une entrée `list-backup-job-summaries` dans laquelle la demande veut renvoyer tous les comptes disponibles dont l'état est `FAILED` au cours des 14 derniers jours :

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

Pour obtenir le nombre de tâches dont le statut est `completed with issues`, soustrayez le nombre de tâches `COMPLETED` avec une `MessageCategory` `SUCCESS` du nombre `COMPLETED` total.

Surveillance des AWS Backup événements à l'aide d'Amazon EventBridge

AWS Backup envoie des événements à Amazon EventBridge lorsque l'état d'une tâche de sauvegarde ou de copie change. Vous pouvez l'utiliser EventBridge pour surveiller les AWS Backup événements. Par exemple, vous pouvez recevoir une alarme en cas d'échec d'une tâche de sauvegarde. AWS Backup émet des événements de la meilleure EventBridge manière possible toutes les 5 minutes.

Pour suivre les événements à l'aide de EventBridge, consultez les rubriques suivantes :

- Création d'une règle réagissant aux événements (Amazon EventBridge User Guide)
- Amazon CloudWatch Events and Metrics pour AWS Backup (blog - voir Configurer AWS Backup les événements à envoyer à Amazon EventBridge)

Certains événements indiquent `status: COMPLETED` alors que d'autres événements indiquent `state: COMPLETED`. Cela est conforme à l' AWS Backup API. Certains statuts sont spécifiques à la AWS Backup console : le `Completed with issues` statut est une représentation des `Completed` tâches avec des messages de statut. Pour surveiller les événements `Completed with issues`, surveillez les tâches `COMPLETED` comportant un message de statut.

Vous pouvez également utiliser l'API de AWS Backup notification pour suivre les AWS Backup événements avec Amazon Simple Notification Service (Amazon SNS). Toutefois, elle EventBridge suit un plus grand nombre de modifications que l'API de notification, notamment les modifications apportées aux coffres-forts de sauvegarde, à l'état des tâches de copie, aux paramètres régionaux et au nombre de points de restauration froids ou chauds.

Événements

- Événements Backup Job
- Événements du Backup Plan
- Événements Backup Vault
- Événements Copy Job
- Événements de Recovery Point
- Événements relatifs aux paramètres régionaux
- Événements Restore Job

Événements Backup Job

Voici des exemples d'événements.

État

État : ÉCHEC


```
{
  "version": "0",
  "id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:15:26Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9ab3e749-82c6-4342-9320-5edbf4918b86",
    "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:13:07.392Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "FAILED",
    "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-
west-2:1112233445566:backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86 does not exist.
\"",
    "startBy": "2020-07-30T04:13:07.392Z",
```

```
    "percentDone": 0,
    "retryCount": 3
  }
}
```

État : TERMINÉ

```
{
  "version": "0",
  "id": "dafac799-9b88-0134-26b7-fef4d54a134f",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:41:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:f1d966fe-a3bd-410b-
b292-99f442d13b56"
  ],
  "detail": {
    "backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
    "backupSizeInBytes": "36048",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a",
    "bytesTransferred": "36048",
    "creationDate": "2020-07-15T21:40:31.207Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T21:41:05.921Z",
    "startBy": "2020-07-16T05:40:31.207Z",
    "percentDone": 100,
    "retryCount": 3
  }
}
```

État : COURSE À PIED

```
{
  "version": "0",
```

```
  "id": "44946c39-b519-3505-44e6-ba74afeb2e30",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:39:13Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
    "backupSizeInBytes": "3221225472",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:38:31.152Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-0b5ae24f2ee72d926",
    "resourceType": "EBS",
    "state": "RUNNING",
    "startBy": "2020-07-16T05:00:00Z",
    "expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
    "percentDone": 99,
    "createdBy": {
      "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
      "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
      "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
    }
  }
}
```


État : AVORTÉ


```
{
  "version": "0",
  "id": "4c91ceb0-b798-da82-6818-c29b3dce7543",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T21:33:16Z",
  "region": "us-west-2",
  "resources": [],
```

```
  "detail": {
    "backupJobId": "58cdef95-7680-4c74-80d5-1b64093999c8",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "backupVaultName": "f59bffcd-2538-4bbe-8343-1c60dae27c27",
    "bytesTransferred": "0",
    "creationDate": "2020-07-15T21:33:00.803Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "ABORTED",
    "statusMessage": "\"Backup job was stopped by user.\"",
    "completionDate": "2020-07-15T21:33:01.621Z",
    "startBy": "2020-07-16T05:33:00.803Z",
    "percentDone": 0
  }
}
```


État : EXPIRÉ


```
{
  "version": "0",
  "id": "1d7bbc04-6120-1145-13b9-49b0af465328",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T13:04:57Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "01EE26DC-7107-4D8E-0C54-EAC27C662BA4",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-vault:aws/backup/
AutomatedBackupVaultDel2",
    "backupVaultName": "aws/backup/AutomatedBackupVaultDel2",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T05:10:20.077Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "EXPIRED",
    "statusMessage": "\"Backup job failed because there was a running job for the same
 resource.\"",
    "completionDate": "2020-07-29T13:02:15.234Z",
```

```
    "startBy": "2020-07-29T13:00:00Z",
    "percentDone": 0,
    "createdBy": {
      "backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-plan:aws/
efs/414a5bd4-f880-47ad-95f3-f085108a4c3b",
      "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00NjhlLWIzMTEtNWRjOWY0YTNjN2Vj",
      "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2"
    }
  }
}
```

État : EN ATTENTE

```
{
  "version": "0",
  "id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:03:30Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "2cffdb68-d6ed-485f-9f9b-8b530749f1c2",
    "backupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ed1f2661-5587-48bf-8a98-fadb977bf975",
    "backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975",
    "bytesTransferred": "0",
    "creationDate": "2020-07-29T20:01:06.224Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/MockRCBackupTestRole",
    "resourceArn": "arn:aws:service:us-west-2:1112233445566:resource-type/resource-id",
    "resourceType": "type",
    "state": "PENDING",
    "statusMessage": "",
    "startBy": "2020-07-30T04:01:06.224Z",
    "percentDone": 0
  }
}
```

État : CRÉÉ

```
{
```

```
  "version": "0",
  "id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
  "detail-type": "Backup Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T20:32:53Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
    "state": "CREATED",
    "creationDate": "2020-06-22T20:32:47.466Z"
  }
}
```


Événements du Backup Plan

Voici des exemples d'événements.

État

- État : MODIFIÉ
- État : SUPPRIMÉ
- État : CRÉÉ

État : MODIFIÉ


```
{
  "version": "0",
  "id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
```

```
    "modifiedAt": "2020-06-24T23:18:19.168Z",
    "state": "MODIFIED"
  }
}
```

État : SUPPRIMÉ

```
{
  "version": "0",
  "id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:25Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:83fcb8ee-2d93-42ac-
b06f-591563f3f8de"
  ],
  "detail": {
    "backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
    "versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
    "deletionDate": "2020-06-24T23:18:19.411Z",
    "state": "DELETED"
  }
}
```

État : CRÉÉ

```
{
  "version": "0",
  "id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
  "detail-type": "Backup Plan State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-plan:2c103c5f-6d6e-4cac-9147-
d3afa4c84f59"
  ],
  "detail": {
    "backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
```

```
    "versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4",
    "creationDate": "2020-06-24T23:18:15.318Z",
    "state": "CREATED"
  }
}
```

Événements Backup Vault

Voici des exemples d'événements.

État

- État : CRÉÉ
- État : MODIFIÉ
- État : SUPPRIMÉ

État : CRÉÉ

```
{
  "version": "0",
  "id": "d415609e-5f35-d9a2-76d1-613683e4e024",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:d8864642-155c-4283-a168-
a04f40e12c97"
  ],
  "detail": {
    "backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
    "state": "CREATED"
  }
}
```

État : MODIFIÉ

```
{
  "version": "0",
  "id": "1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890",
```

```
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T23:18:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:nameOfTestBackup"
  ],
  "detail": {
    "backupVaultName": "vaultName",
    "state": "MODIFIED",
    "isLocked": "true"
  }
}
```

État : SUPPRIMÉ

```
{
  "version": "0",
  "id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
  "detail-type": "Backup Vault State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T02:42:37Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:e8189629-1f8e-4ed2-af7d-
b32415d04db1"
  ],
  "detail": {
    "backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
    "state": "DELETED"
  }
}
```

Événements Copy Job

Voici des exemples d'événements.

État

- État : ÉCHEC
- État : COURSE À PIED

- État : TERMINÉ
- État : CRÉÉ

État : ÉCHEC

```
{
  "version": "0",
  "id": "4660bc92-a44d-c939-4542-cda503f14855",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:37:34Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5"
  ],
  "detail": {
    "copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
    "backupSizeInBytes": 22548578304,
    "creationDate": "2020-07-15T20:36:13.239Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/
RoleForEc2BackupWithNoDescribeTagsPermissions",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:instance/i-0515aee7de03f58e1",
    "resourceType": "EC2",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "state": "FAILED",
    "statusMessage": "Access denied exception while trying to list tags",
    "completionDate": "2020-07-15T20:37:28.704Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:55aa945e-c46a-421b-aa27-f94b074e31b7",
    "destinationRecoveryPointArn": {}
  }
}
```

État : COURSE À PIED

```
{
  "version": "0",
  "id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
  "detail-type": "Copy Job State Change",
```

```
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:07:48Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "RUNNING",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": {},
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```


État : TERMINÉ


```
{
  "version": "0",
  "id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T22:08:04Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
  ],
```

```
  "detail": {
    "copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
    "backupSizeInBytes": 3221225472,
    "creationDate": "2020-07-15T22:06:27.234Z",
    "iamRoleArn": "arn:aws:iam::1112233445566:role/OrganizationCanaryTestRole",
    "resourceArn": "arn:aws:ec2:us-west-2:1112233445566:volume/vol-050eba21ee4d3c001",
    "resourceType": "EBS",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "state": "COMPLETED",
    "completionDate": "2020-07-15T22:07:58.111Z",
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:846869de-4589-45c3-ab60-4fbbabcdd3ec",
    "destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/
snap-0726fe70935586180",
    "createdBy": {
      "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:b58e3621-1c53-4997-ad8a-afc3347a850e",
      "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4",
      "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18"
    }
  }
}
```

État : CRÉÉ

```
{
  "version": "0",
  "id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
  "detail-type": "Copy Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T21:06:32Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"
  ],
  "detail": {
    "creationDate": "2020-06-22T21:06:25.754Z",
    "state": "CREATED",
    "sourceBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17",
```

```
    "destinationBackupVaultArn": "arn:aws:backup:us-west-2:1112233445566:backup-
vault:ef09da5a-21a6-461f-a98f-857e9e621a17"
  }
}
```

Événements de Recovery Point

Voici des exemples d'événements.

État

- État : TERMINÉ
- État : SUPPRIMÉ
- État : MODIFIÉ

État : TERMINÉ

```
{
    "version": "0",
    "id": "ab32977c-378d-2122-e985-fgh4596f0709",
    "detail-type": "Recovery Point State Change",
    "source": "aws.backup",
    "account": "1112233445566",
    "time": "2020-07-15T21:39:07Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:rds:us-west-2:1112233445566:cluster-snapshot:awsbackup:job-4ece7121-
d60e-00c2-5c3b-49960142d03b"
    ],
    "detail": {
        "backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-
vault:e6625738-0655-4aa9-bd37-6ec1dd183b15",
        "creationDate": "2020-07-15T21:38:31.152Z",
        "iamRoleArn": "arn:aws:iam::1112233445566:role/FullBackupTestRole",
        "resourceType": "Aurora",
        "resourceArn": "arn:aws:rds:us-west-2:1112233445566:cluster:id",
        "status": "COMPLETED",
        "isEncrypted": "false",
        "storageClass": "WARM",
        "completionDate": "2020-07-15T21:39:05.689Z",
```

```
        "createdBy": {
            "backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanArn": "arn:aws:backup:us-west-2:1112233445566:backup-
plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5",
            "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5",
            "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5"
        },
        "lifecycle": {
            "deleteAfterDays": 100
        },
        "calculatedLifeCycle": {
            "deleteAt": "2020-10-23T21:38:31.152Z"
        }
    }
}
```

État : SUPPRIMÉ

```
{
  "version": "0",
  "id": "6089ee76-d856-0d7c-cee7-0a431cd43343",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T22:38:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:157f892e-
fe46-48da-9dbe-4154f91f8acc",
    "arn:aws:rds:us-west-2:1112233445566:snapshot:awsbackup:job-c1a6d40a-32d1-4d54-
bd70-bced933ef107"
  ],
  "detail": {
    "state": "DELETED",
    "lifecycle": {
      "deleteAfterDays": 300
    },
    "calculatedLifeCycle": {
      "deletedAt": "2021-05-25T22:29:02.452Z"
    }
  }
}
```

État : MODIFIÉ

```
{
  "version": "0",
  "id": "14365bb1-adef-bc00-1ee3-8fac188d7996",
  "detail-type": "Recovery Point State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-02T23:33:57Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:backup-vault:helo12312",
    "arn:aws:dynamodb:us-west-2:1112233445566:table/test/
backup/01593730512469-033578ce"
  ],
  "detail": {
    "calculatedLifeCycle": {
      "toColdStorageAfterDays": "Fri Dec 04 22:55:11 UTC 2020"
    },
    "state": "MODIFIED"
  }
}
```

Événements relatifs aux paramètres régionaux

Voici un exemple d'événement.

```
{
  "version": "0",
  "id": "e7ed82ba-4955-4de5-10d6-dbafcfb68b4f",
  "detail-type": "Region Setting State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-24T22:55:03Z",
  "region": "us-west-2",
  "resources": [],
  "detail": {
    "modifiedAt": "2020-06-24T22:54:57.161Z",
    "ResourceTypeOptInPreference": {
      "Aurora": true
    },
    "state": "MODIFIED"
  }
```

```
}
```

Événements Restore Job

Voici des exemples d'événements.

État

- État : ÉCHEC
- État : COURSE À PIED
- État : TERMINÉ
- État : EN ATTENTE
- État : CRÉÉ

État : ÉCHEC

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-15T20:19:29Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::image/ami-12b3456dfb7f8cf90"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "22548578304",
    "creationDate": "2020-07-15T20:19:07.303Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/TestAWSBackupRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "FAILED",
    "statusMessage": "AWS Backup does not permit attaching a new instance profile to an
 EC2 instance. Please restore using the backed up instance profile."
```

```
  }
}
```

État : COURSE À PIED

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:26:06Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-0fe123ca456cfad7c"
  ],
  "detail": {
    "restoreJobId": "1B234A56-789B-01CD-2A34-4567A08901FD",
    "backupSizeInBytes": "3221225472",
    "creationDate": "2020-07-29T20:26:00.098Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EBS",
    "status": "RUNNING"
  }
}
```

État : TERMINÉ

```
{
  "version":"0",
  "id":"ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type":"Restore Job State Change",
  "source":"aws.backup",
  "account":"1112233445566",
  "time":"2020-07-15T03:14:58Z",
  "region":"us-west-2",
  "resources":[
```

```
    "arn:aws:rds:us-
west-2:1112233445566:snapshot:awsbackup:job-1a2bcd34-567e-8901-23f4-5g6hijkl7890"
  ],
  "detail":{
    "restoreJobId":"AB123456-78C9-0123-456D-789012E34567",
    "backupSizeInBytes":"0",
    "creationDate":"2020-07-15T03:10:01.742Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "iamRoleArn":"arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone":0,
    "resourceType":"RDS",
    "status":"COMPLETED",
    "createdResourceArn":"arn:aws:rds:us-
west-2:1112233445566:db:testinginstance1a2bcd34-567e-8901-23f4-5g6hijkl7890",
    "completionDate":"2020-07-15T03:14:53.128Z"
  }
}
```

État : EN ATTENTE

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-07-29T20:08:26Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:42bb8260-92cd-46a2-ab8d-
b29f4edb47b1"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "backupSizeInBytes": "36048",
    "creationDate": "2020-07-29T20:08:21.083Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
```

```
    "iamRoleArn": "arn:aws:iam::1112233445566:role/RestoreTestRole",
    "percentDone": 0,
    "resourceType": "EC2",
    "status": "PENDING"
  }
}
```

État : CRÉÉ

```
{
  "version": "0",
  "id": "ab32977c-378d-2122-e985-fgh4596f0709",
  "detail-type": "Restore Job State Change",
  "source": "aws.backup",
  "account": "1112233445566",
  "time": "2020-06-22T18:50:49Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:backup:us-west-2:1112233445566:recovery-point:a6560b33-3660-494c-8d47-
efgh939ij32k"
  ],
  "detail": {
    "restoreJobId": "123EA45F-C678-EFE9-0123-4D56FC0E789A",
    "creationDate": "2020-06-22T18:50:46.407Z",
    "createdBy": [
      "arn:aws:backup:us-east-1:123456789012:restore-testing-plan:TestPlan1-
a12b3c45-6d78-90e1-f234-56789b012gh3"
    ],
    "state": "CREATED"
  }
}
```

AWS Backup statistiques avec Amazon CloudWatch

Rubriques

- CloudWatch Tableau de bord
- Métriques avec CloudWatch

CloudWatch Tableau de bord

> **Note**
>
> Le tableau de bord de la console dépend de la région qui accède à la console. Consultez Disponibilité des fonctionnalités par Région AWS pour savoir quelles régions ont accès au tableau de bord des tâches. Les régions non répertoriées pourront accéder au CloudWatch tableau de bord.

Votre AWS Backup console inclut un tableau de bord permettant de consulter les statistiques relatives aux tâches de sauvegarde, de copie et de restauration terminées ou échouées. Dans ce tableau de bord, vous pouvez afficher le statut de la tâche par période, personnalisée en fonction de la période que vous souhaitez.

POUR ACCÉDER AU TABLEAU DE BORD

1. Ouvrez la AWS Backup console à l'adresse https://console.aws.amazon.com/backup.
2. Dans le volet de navigation de gauche, sélectionnez Tableau de bord.

AFFICHAGE ET COMPRÉHENSION DU TABLEAU DE BORD

Le CloudWatch tableau de bord affiche plusieurs widgets. Chaque widget affiche les métriques des tâches par nombre. Chaque widget affiche plusieurs graphiques linéaires. Chaque ligne correspond à une ressource protégée (si aucune ressource attendue ne s'affiche, assurez-vous que la ressource est activée dans Paramètres). Les affichages n'indiquent pas les tâches en cours.

L'axe des Y (valeurs verticales) indique le nombre. L'axe des X (valeurs horizontales) indique des points dans le temps. S'il n'y a aucun point de données à visualiser dans le statut de la tâche sélectionnée, la valeur sera définie sur 0 avec une ligne horizontale sur l'axe des X. La légende indiquant les ressources sera toujours visible.

Les métriques affichent des informations spécifiques au compte et à la région relatives à la connexion actuelle. Pour voir d'autres comptes ou régions, vous devez vous connecter sous le compte choisi.

PERSONNALISATION DU TABLEAU DE BORD

Par défaut, le délai affiché est d'une semaine. Dans le menu supérieur, vous trouverez des options permettant de redéfinir la période affichée. Vous pouvez choisir entre 1 heure, 3 heures, 12 heures,

1 jour, 3 jours et 1 semaine. En outre, vous pouvez sélectionner Personnalisé pour spécifier une valeur différente. La personnalisation modifiera temporairement l'affichage actuel selon vos spécifications.

Vous pouvez survoler un widget, qui affichera un bouton Agrandir en haut à droite du widget. Cliquez sur Agrandir pour ouvrir le widget en mode plein écran. En plein écran, d'autres options permettent de personnaliser l'affichage du graphique, telles que la modification de la période (le délai entre chaque point de données). Aucune modification ne sera conservée une fois l'affichage en plein écran fermé.

Pour afficher un seul type de ressource à la fois, cliquez sur le texte de l'étiquette du type de ressource que vous souhaitez afficher dans la légende du graphique. Cela désélectionnera tous les autres types de ressources. Pour inverser cette étape, cliquez sur la case de couleur d'un type de ressource dans la légende. Pour revenir à l'affichage par défaut de tous les types de ressources avec toutes les étiquettes sélectionnées, cliquez à nouveau sur le texte de l'étiquette de n'importe quel type de ressource sélectionné.

Cliquez sur les trois points verticaux dans le coin supérieur droit d'un widget pour ouvrir un menu déroulant contenant des options permettant d'actualiser, d'agrandir, d'afficher les métriques et d'afficher les journaux. « Afficher dans les métriques » ouvre la métrique utilisée dans le widget dans la CloudWatch console. Vous pouvez y apporter toutes les modifications nécessaires et ajouter le widget à un tableau de bord personnalisé dans le tableau CloudWatch de bord. Les modifications que vous apportez au CloudWatch tableau de bord ne seront pas reflétées dans le tableau de bord de AWS Backup la console. « Afficher sous forme de journaux » ouvre la page d'affichage des journaux dans CloudWatch la console.

Pour ajouter des widgets affichés à votre tableau de CloudWatch bord personnalisé, cliquez sur le bouton Ajouter au tableau de bord situé en haut à droite du tableau de bord. Cela ouvrira la CloudWatch console dans laquelle vous pourrez sélectionner dans quel tableau de bord personnalisé ajouter les six widgets.

Pour plus d'informations, consultez la section Utilisation CloudWatch des métriques Amazon.

Métriques avec CloudWatch

Vous pouvez l'utiliser CloudWatch pour surveiller AWS Backup les métriques. L'espace de `AWS/Backup` noms vous permet de suivre les métriques suivantes. AWS Backup émet des métriques mises à jour CloudWatch toutes les 5 minutes.

Le but de cette page de documentation est de vous fournir les matériaux de référence à utiliser CloudWatch pour surveiller AWS Backup. Pour savoir comment surveiller une métrique à l'aide d'un service unique CloudWatch, consultez le blog Amazon CloudWatch Events and Metrics for AWS Backup ou concentrez-vous sur les métriques et les alarmes dans un seul AWS service dans le guide de CloudWatch l'utilisateur. Pour configurer les alarmes, consultez la section Utilisation d'Amazon CloudWatch Alarms dans le guide de CloudWatch l'utilisateur.

Catégorie	Métriques	Exemple de dimensions	Exemple de cas d'utilisation
Tâches	Nombre de tâches de sauvegarde, de restauration et de copie dans chaque état, y compris `CREATED`, `PENDING`, `RUNNING`, `ABORTED`, `COMPLETED` , `FAILED` et `EXPIRED`. Les différents types de tâches ont différents états disponibles.	Type de ressource, nom du coffre-fort. Le nom du coffre-fort des tâches de copie est celui du coffre-fort de destination.	Surveillez le nombre de tâches de sauvegarde ayant échoué dans un ou plusieurs coffres-forts de sauvegarde spécifiques. Lorsque plus de cinq tâches ont échoué en une heure, envoyez un e-mail ou un SMS via Amazon SNS ou ouvrez un ticket pour que l'équipe d'ingénierie enquête. Critères de notification : il existe une valeur différente de zéro
Points de récupération	Nombre de points de récupération à chaud et à froid dans chaque état : `MODIFIED`, `COMPLETED` ,	Type de ressource, nom du coffre-fort.	Suivez le nombre de points de récupération supprimés pour vos volumes Amazon EBS et suivez séparément le nombre de points

Catégorie	Métriques	Exemple de dimensions	Exemple de cas d'utilisation
	`PARTIAL`, `EXPIRED`, `DELETED`.		de récupération à chaud et à froid dans chaque coffre-fort de sauvegarde. Critères de notification : il existe une valeur différente de zéro

> **Note**
>
> L'état de la tâche de `Completed with issues` est spécifique à la AWS Backup console uniquement ; il ne peut pas être suivi via CloudWatch.

Le tableau suivant répertorie toutes les métriques disponibles.

Métrique	Description
`NumberOfBackupJobsCreated`	Le nombre de tâches de sauvegarde AWS Backup créées.
`NumberOfBackupJobsPending`	Nombre de tâches de sauvegarde sur le point d'être exécutées dans AWS Backup.
`NumberOfBackupJobsRunning`	Nombre de tâches de sauvegarde en cours d'exécution AWS Backup.
`NumberOfBackupJobsAborted`	Nombre de tâches de sauvegarde annulées par l'utilisateur.
`NumberOfBackupJobsCompleted`	Le nombre de tâches de sauvegarde AWS Backup terminées.

Métrique	Description
`NumberOfBackupJobsFailed`	Nombre de tâches de sauvegarde dont le statut est `Failed`. Cela est souvent dû à la planification d'une tâche de sauvegarde pendant ou 1 heure avant une ressource de base de données ou 4 heures avant ou pendant une fenêtre de maintenance ou une fenêtre de sauvegarde automatique d'Amazon FSx, sans pour autant l'utiliser AWS Backup pour effectuer une sauvegarde continue pour les point-in-time restaurations. Consultez la section Point-in-Time Recovery pour obtenir une liste des services pris en charge et des instructi ons sur la façon de les utiliser AWS Backup pour effectuer des sauvegardes continues ou replanifier vos tâches de sauvegarde.
`NumberOfBackupJobsExpired`	Le nombre de tâches de sauvegarde dont le statut est de`EXPIRED`. Le statut d'une tâche de sauvegarde passe `CREATED` à celui d'`EXPIRED`une tâche de sauvegarde qui ne peut pas démarrer dans le délai imparti.
`NumberOfCopyJobsCreated`	Nombre de tâches de copie entre comptes et entre régions créées par AWS Backup .
`NumberOfCopyJobsRunning`	Nombre de tâches de copie entre comptes et entre régions en cours d'exécution dans AWS Backup.
`NumberOfCopyJobsCompleted`	Nombre de tâches de copie entre comptes et entre régions finies par AWS Backup .

Métrique	Description
NumberOfCopyJobsFailed	Nombre de tâches de copie entre comptes et entre régions qui ont été AWS Backup tentées mais qui n'ont pas pu être effectuées.
NumberOfRestoreJobsPending	Nombre de tâches de restauration sur le point d'être exécutées dans AWS Backup.
NumberOfRestoreJobsRunning	Le nombre de tâches de restauration en cours d'exécution AWS Backup.
NumberOfRestoreJobsCompleted	Le nombre de tâches de restauration AWS Backup terminées.
NumberOfRestoreJobsFailed	Nombre de tâches de restauration qui ont été AWS Backup tentées mais qui n'ont pas pu être effectuées.
NumberOfRecoveryPointsCompleted	Le nombre de points de récupération AWS Backup créés.
NumberOfRecoveryPointsPartial	Nombre de points de restauration qui AWS Backup ont commencé à être créés mais qui n'ont pas pu être terminés. AWS réessaie le processus ultérieurement, mais comme la nouvelle tentative a lieu ultérieurement, le point de récupération partiel est conservé.
NumberOfRecoveryPointsExpired	Nombre de points de restauration qui AWS Backup ont tenté de supprimer en fonction du cycle de conservation des sauvegardes, mais qui n'ont pas pu être supprimés. Le stockage consommé par les sauvegardes expirées vous est facturé et vous devriez les supprimer manuellement.
NumberOfRecoveryPointsDeleting	Le nombre de points de récupération qui AWS Backup sont supprimés.

Métrique	Description
`NumberOfRecoveryPointsCold`	Le nombre de points de récupération associés AWS Backup à une chambre froide.

D'autres dimensions sont disponibles en plus de celles indiquées dans le tableau. Pour afficher toutes les dimensions d'une métrique, tapez le nom de cette métrique dans l'`AWS/Backup`espace de noms de la section Metrics de la CloudWatch console.

Journalisation des appels d' AWS Backup API avec CloudTrail

AWS Backup est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS service. CloudTrail capture tous les appels d'API AWS Backup sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Backup console et des appels de code vers les opérations de l' AWS Backup API. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Backup, 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 de l'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 parcours à région unique ou multirégionale à l'aide du. 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 parcours à région unique, vous ne pouvez voir que les événements enregistrés dans le parcours. Région AWS Pour plus d'informations sur les sentiers, consultez les sections Création d'un sentier pour votre organisation Compte AWS et Création d'un sentier pour une organisation dans le guide de AWS CloudTrail l'utilisateur.

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.

AWS Backup événements à CloudTrail

AWS Backup génère ces CloudTrail événements lorsqu'il effectue des sauvegardes, des restaurations, des copies ou des notifications. Ces événements ne sont pas nécessairement générés par l'utilisation des API AWS Backup publiques. Pour plus d'informations, consultez les Service AWS événements dans le guide de AWS CloudTrail l'utilisateur.

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

Comprendre les entrées du fichier AWS Backup journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre les `DeleteRecoveryPoint` actions `StartBackupJobStartRestoreJob`, et ainsi que l'`BackupJobCompleted`événement.

```
{
    "eventVersion": "1.05",
```

```
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
```

```
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
```

```
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
    },
    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "completionDate": {
            "seconds": 1547108091,
```

```
            "nanos": 906000000
        },
        "state": "COMPLETED",
        "percentDone": 100,
        "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",
        "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:BackupVault",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-06692095a6a421233",
        "creationDate": {
            "seconds": 1547101638,
            "nanos": 272000000
        },
        "backupSizeInBytes": 8589934592,
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "resourceType": "EBS"
    }
}
```


Journalisation des événements de gestion entre comptes

Avec AWS Backup, vous pouvez gérer vos sauvegardes dans Comptes AWS l'ensemble de votre AWS Organizationsstructure. AWS Backup génère ces CloudTrail événements lorsque vous créez, mettez à jour ou supprimez une politique de AWS Organizations sauvegarde (qui applique des plans de sauvegarde à vos comptes membres) ou lorsqu'un plan de sauvegarde organisationnel n'est pas valide :

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

Exemple : entrées de fichier AWS Backup journal pour la gestion entre comptes

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et

l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateOrganizationalBackupPlan`action.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"},
    "eventTime": "2020-06-02T00:34:00Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "CreateOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
\"name\":\"hourly\",\"description\":null,\"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault\",
\"scheduleExpression\":\"cron(0 0/1 ? * * *)\",\"startWindow\":\"PT1H\",
\"completionWindow\":\"PT2H\",\"lifecycle\":{\"moveToColdStorageAfterDays\":null,
\"deleteAfterDays\":\"7\"},\"tags\":null,\"copyActions\":[]}]",
        "backupSelections": "[{\"name\":\"selectiondatatype\",\"arn\":
\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
\"resources\":[],\"notResources\":[],\"conditions\":[{\"type\":\"STRINGEQUALS\",\"key
\":\"dataType\",\"value\":\"PII\"},{\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",
\"value\":\"RED\"}],\"creationDate\":\"2020-06-02T00:34:00.695Z\",\"creatorRequestId
\":null}]",
```

```
        "creationDate": {
            "seconds": 1591058040,
            "nanos": 695000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`DeleteOrganizationalBackupPlan`action.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2020-06-02T00:34:25Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "deletionDate": {
            "seconds": 1591058065,
            "nanos": 519000000
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    }
```

```
}
```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'événement`InvalidOrganizationBackupPlan`, qui est envoyé lorsque vous AWS Backup recevez un plan de sauvegarde non valide de la part d'Organizations.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2022-06-11T13:29:23Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "InvalidOrganizationBackupPlan",
    "awsRegion": "Region",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "987654321098",
    "serviceEventDetails": {
        "effectivePolicyVersion": 7,
        "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
        "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
        "policyType": "BACKUP_POLICY",
        "effectiveBackupPlan": {
            "logicalName": "logical-name",
            "regions": [
                "Region"
            ],
            "rules": [
                {
                    "name": "test-orgs",
                    "targetBackupVaultName": "vault-name",
                    "ruleLifecycle": {
                        "deleteAfterDays": 100
                    },
                    "copyActions": [],
```

```
                    "enableContinuousBackup": true
                }
            ],
            "selections": {
                "tagSelections": [
                    {
                        "selectionName": "selection-name",
                        "iamRoleArn": "arn:aws:iam::$account:role/role",
                        "targetedTags": [
                            {
                                "tagKey": "key",
                                "tagValue": "value"
                            }
                        ]
                    }
                ]
            },
            "backupPlanTags": {
                "key": "value"
            }
        },
        "organizationId": "org-id",
        "accountId": "123456789012"
    },
    "eventCategory": "Management"
}
```

Options de notification avec AWS Backup

Il existe deux manières de recevoir des notifications concernant AWS Backup :

- AWS Les notifications utilisateur peuvent envoyer des notifications, notamment des CloudWatch alarmes Amazon et AWS Support des notifications relatives à d'autres services.
- Amazon Simple Notification Service peut vous informer des AWS Backup événements.

AWS Notifications aux utilisateurs et AWS Backup

AWS Backup prend en charge la gestion de vos notifications de sauvegarde à partir de la console de notifications AWS utilisateur. Grâce à AWS User Notifications, vous pouvez consulter la progression de vos tâches de sauvegarde, de copie et de restauration, ainsi que les modifications apportées à

vos politiques de sauvegarde, à vos coffres-forts, à vos points de récupération et à vos paramètres à partir du centre de notification User Notifications.

Amazon CloudWatch, les EventBridge alarmes Amazon et les mises à jour de AWS Support cas font partie des autres types de notifications que vous pouvez gérer depuis la console. En outre, vous pouvez configurer plusieurs options de livraison, notamment le courrier électronique, AWS Chatbot les notifications et les notifications AWS Console Mobile Application push.

Amazon SNS et événements AWS Backup

AWS Backup tire parti des notifications robustes fournies par Amazon Simple Notification Service (Amazon SNS). Vous pouvez configurer Amazon SNS pour qu'il vous informe des AWS Backup événements depuis la console Amazon SNS.

Limites

- Bien que le service Amazon SNS autorise les notifications entre comptes, il ne prend actuellement AWS Backup pas en charge cette fonctionnalité. Vous devez spécifier votre propre identifiant de AWS compte et l'ARN de la ressource de votre rubrique.
- AWS Backup prend en charge les rubriques standard pour la déduplication optimale via SNS, mais AWS Backup ne prend actuellement pas en charge les rubriques SNS FIFO pour la déduplication stricte.

Cas d’utilisation courants

- Configurez les notifications pour les tâches de sauvegarde ayant échoué en suivant les étapes décrites dans Comment puis-je recevoir des notifications pour les AWS Backup tâches qui ont échoué ? auprès de AWS Premium Support.
- Consultez des exemples de notifications JSON Amazon SNS pour les tâches de sauvegarde terminées, échouées ou expirées dans le tableau des exemples d'événements ci-dessous.

Pour plus d'informations sur Amazon SNS de façon générale, consultez Démarrage avec Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

AWS Backup API de notification

Après avoir créé vos rubriques à l'aide de la console Amazon SNS ou AWS Command Line Interface (AWS CLI), vous pouvez utiliser les opérations d' AWS Backup API suivantes pour gérer vos notifications de sauvegarde.

- DeleteBackupVaultNotifications : supprime les notifications d'événement SNS pour le coffre-fort de sauvegarde spécifié.
- GetBackupVaultNotifications : répertorie toutes les notifications d'événement SNS pour le coffre-fort de sauvegarde spécifié.
- PutBackupVaultNotifications : active les notifications pour la rubrique et les événements spécifiés.

AWS Backup prend en charge les événements suivants :

Type de tâche	Événement
Tâche de sauvegarde	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `CONTINUOUS_BACKUP_INTERRUPTED`
Tâche de copie	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
Tâche de restauration	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
Point de récupération	`RECOVERY_POINT_MODIFIED`

AWS Backup for S3 prend en charge deux événements supplémentaires :

- `S3_BACKUP_OBJECT_FAILED` vous informe de tout échec de la sauvegarde d'un objet S3 lors d'une tâche de sauvegarde avec AWS Backup .
- `S3_RESTORE_OBJECT_FAILED` vous informe de tout échec de la restauration d'un objet S3 lors d'une tâche de restauration avec AWS Backup .

Exemples d'événements

Example Exemple : tâche de sauvegarde terminée

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job was completed successfully. Recovery point
 ARN: arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012d. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"COMPLETED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example Exemple : échec de la tâche de sauvegarde

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
```

```
            "Message": "An AWS Backup job failed. Resource ARN : arn:aws:ec2:us-
west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID : 1b2345b2-
f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes": {
                "EventType": {"Type":"String","Value":"BACKUP_JOB"},
                "State": {"Type":"String","Value":"FAILED"},
                "AccountId": {"Type":"String","Value":"123456789012"},
                "Id": {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
                "StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
}
```

Example Exemple : la tâche de sauvegarde n'a pas pu être terminée pendant la fenêtre de sauvegarde

```
{
    "Records": [{
        "EventSource": "aws:sns",
        "EventVersion": "1.0",
        "EventSubscriptionArn": "arn:aws:sns:...-a3802aa1ed45",
        "Sns": {
            "Type": "Notification",
            "MessageId": "12345678-abcd-123a-def0-abcd1a234567",
            "TopicArn": "arn:aws:sns:us-west-1:123456789012:backup-2sqs-sns-topic",
            "Subject": "Notification from AWS Backup",
            "Message": "An AWS Backup job failed to complete in time. Resource ARN :
 arn:aws:ec2:us-west-1:123456789012:volume/vol-012f345df6789012e. BackupJob ID :
 1b2345b2-f22c-4dab-5eb6-bbc7890ed123",
            "Timestamp": "2019-08-02T18:46:02.788Z",
            ...
            "MessageAttributes" : {
              "EventType" : {"Type":"String","Value":"BACKUP_JOB"},
              "State" : {"Type":"String","Value":"EXPIRED"},
              "AccountId" : {"Type":"String","Value":"123456789012"},
              "Id" : {"Type":"String","Value":"1b2345b2-f22c-4dab-5eb6-bbc7890ed123"},
              "StartTime" : {"Type":"String","Value":"2019-09-02T13:48:52.226Z"}
            }
        }
    }]
```

```
}
```

AWS Backup exemples de commandes de notification

Vous pouvez utiliser des AWS CLI commandes pour vous abonner aux notifications Amazon SNS relatives à vos AWS Backup événements, les répertorier et les supprimer.

Exemple de notification de mise en place d'un coffre-fort de sauvegarde

La commande suivante s'abonne à une rubrique Amazon SNS pour le coffre-fort de sauvegarde spécifié qui vous avertit lorsqu'une tâche de restauration est lancée ou terminée, ou lorsqu'un point de récupération est modifié.

```
aws backup put-backup-vault-notifications
    --backup-vault-name myBackupVault
    --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
    --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
 RECOVERY_POINT_MODIFIED
```

Exemple de notification d'obtention d'un coffre-fort de sauvegarde

La commande suivante répertorie tous les événements actuellement abonnés à une rubrique Amazon SNS pour le coffre-fort de sauvegarde spécifié.

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

L'exemple de sortie se présente comme suit :

```
{
    "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
    "BackupVaultEvents": [
        "RESTORE_JOB_STARTED",
        "RESTORE_JOB_COMPLETED",
        "RECOVERY_POINT_MODIFIED"
    ],
    "BackupVaultName": "myVault",
    "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

Exemple de notification de suppression d'un coffre-fort de sauvegarde

La commande suivante se désabonne d'une rubrique Amazon SNS pour le coffre-fort de sauvegarde spécifié.

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

Spécification AWS Backup en tant que principal de service

> **Note**
>
> AWS Backup Pour autoriser la publication de sujets SNS en votre nom, vous devez le spécifier AWS Backup en tant que principal de service.

Incluez le code JSON suivant dans la politique d'accès de la rubrique Amazon SNS que vous utilisez pour suivre AWS Backup les événements. Vous devez spécifier l'Amazon Resource Name (ARN) de la ressource de votre rubrique.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Pour plus d'informations sur la spécification d'un principal de service dans une politique d'accès Amazon SNS, consultez la section Autoriser la publication d'une AWS ressource dans un sujet dans le guide du développeur Amazon Simple Notification Service.

> **Note**
>
> Si votre sujet est crypté, vous devez inclure des autorisations supplémentaires dans votre politique AWS Backup pour autoriser la publication sur celui-ci. Pour plus d'informations sur la possibilité pour les services de publier sur des sujets chiffrés, consultez la section Activer la

compatibilité entre les sources d'événements AWS des services et les sujets cryptés dans le guide du développeur Amazon Simple Notification Service.

Résolution des problèmes AWS Backup

Lors de l'utilisation AWS Backup, il est possible que vous rencontriez des problèmes. Les sections suivantes peuvent vous aider à résoudre les problèmes courants qui peuvent se poser.

Pour les questions d'ordre général AWS Backup, consultez la AWS Backup FAQ. Vous pouvez également rechercher des réponses et publier des questions dans le forum AWS Backup.

Rubriques

Dépannage de problèmes généraux

Lorsque vous sauvegardez et restaurez des ressources, vous devez être autorisé à utiliser AWS Backup et à accéder aux ressources que vous souhaitez protéger. Le moyen le plus simple d'obtenir les autorisations appropriées est de choisir le Rôle par défaut lorsque vous attribuez des ressources à un plan de sauvegarde. Pour plus d'informations sur le contrôle d'accès à l'aide de AWS Identity and Access Management (IAM) avec AWS Backup, consultezContrôle d’accès.

Si un `AccessDenied` message d'erreur s'affiche lorsque vous tentez d'accéder à une AWS Backup ressource, telle qu'un coffre de sauvegarde, cela signifie que la ressource n'existe pas ou que vous n'êtes pas autorisé à y accéder.

Si vous rencontrez des problèmes avec la sauvegarde et la restauration d'un type de ressource particulier, n'hésitez pas à consulter la rubrique de dépannage des sauvegardes et des restaurations relative à cette ressource. Pour plus d'informations, consultez les liens de la section Fonctionnement AWS Backup avec les AWS services pris en charge.

Si vous AWS Backup ne parvenez pas à créer ou à supprimer une ressource, vous pouvez en savoir plus sur le problème en consultant AWS CloudTrail les messages d'erreur ou les journaux. Pour plus d'informations sur l'utilisation CloudTrail avec AWS Backup, consultezJournalisation des appels d' AWS Backup API avec CloudTrail.

Résolution des problèmes liés à la création de ressources

Les informations suivantes peuvent vous aider à résoudre les problèmes que vous rencontrez lors de la création de sauvegardes.

- En général, les services de base de données AWS ne peuvent pas démarrer les sauvegardes 1 heure avant ou pendant leur fenêtre de maintenance ou leur fenêtre de sauvegarde automatique. Amazon FSx ne peut pas démarrer les sauvegardes 4 heures avant ou pendant la fenêtre de maintenance ou la fenêtre de sauvegarde automatique (Amazon Aurora est exempté de cette restriction de fenêtre de maintenance). Les sauvegardes d'instantanés planifiées pendant ces périodes échoueront. Une exception : lorsque vous choisissez d'utiliser AWS Backup à la fois des sauvegardes instantanées et des sauvegardes continues pour un service pris en charge, vous n'avez plus à vous soucier de ces fenêtres, car AWS Backup nous les planifierons pour vous. Consultez la section Point-in-Time Recovery pour obtenir une liste des services pris en charge et des instructions sur la manière de les utiliser AWS Backup pour effectuer des sauvegardes continues.
- La création de sauvegardes pour les tables DynamoDB échoue lors de la création de tables. La création d'une table DynamoDB prend généralement quelques minutes.
- La sauvegarde des systèmes de fichiers Amazon EFS peut prendre jusqu'à 7 jours lorsque les systèmes de fichiers sont très volumineux. Une seule sauvegarde simultanée à la fois peut être mise en file d'attente pour un système de fichiers Amazon EFS. Si une sauvegarde ultérieure est mise en file d'attente alors qu'une sauvegarde précédente est toujours en cours, la fenêtre de sauvegarde peut expirer et aucune sauvegarde n'est créée.
- Amazon EBS dispose d'un quota souple de 100 000 sauvegardes Région AWS par compte, et les sauvegardes supplémentaires échouent lorsque ce quota est atteint. Si vous atteignez ce quota, vous pouvez supprimer les sauvegardes excédentaires ou demander une augmentation du quota. Pour de plus amples informations sur la demande d'augmentation de quota, consultez Quotas de service AWS.
- Lorsque vous créez des sauvegardes Amazon Relational Database Service (RDS), tenez compte des points suivants :
  - Si vous ne gérez pas AWS Backup à la fois les instantanés Amazon RDS et les sauvegardes continues avec point-in-time restauration, vos sauvegardes échoueront si elles sont lancées si elles sont planifiées ou effectuées à la demande pendant la fenêtre de sauvegarde quotidienne de 30 minutes configurable par l'utilisateur. Pour plus d'informations sur les sauvegardes Amazon RDS automatiques, consultez Utilisation des sauvegardes dans le Guide de l'utilisateur

Amazon RDS. Vous pouvez éviter cette limitation en utilisant AWS Backup pour gérer à la fois les instantanés Amazon RDS et les sauvegardes continues avec point-in-time restauration.

- Si vous lancez une tâche de sauvegarde depuis la console Amazon RDS, elle peut entrer en conflit avec une tâche de sauvegarde des clusters Aurora, provoquant l'erreur `Backup job expired before completion.`. Si cela se produit, configurez une fenêtre de sauvegarde plus longue dans AWS Backup.
- AWS Backup ne transmet actuellement pas le groupe d'options TDE lorsqu'une tâche de copie est créée. Si vous avez l'intention d'utiliser ce groupe d'options pour créer des tâches de copie, vous devez utiliser la console Amazon RDS ou l'API Amazon RDS au lieu d'outils AWS Backup . Consultez Copie d'un groupe d'options dans le Manuel de l'utilisateur Amazon Relational Database Service pour plus d'informations.
- ERREUR : les sauvegardes à la demande sont terminées mais les sauvegardes planifiées échouent avec l'erreur « La clé KMS de l'instantané source n'existe pas, n'est pas activée ou vous n'êtes pas autorisé à y accéder ». La tâche à la demande est terminée, car elle utilise l'appel d'API `CopyDBSnapshot`, qui ne nécessite pas d'accès à la clé KMS.

  SOLUTION : ajoutez le rôle IAM à votre clé KMS. Cela peut être fait en autorisant le rôle dans votre stratégie de clé KMS.

  Pour modifier votre politique,

  1. Ouvrez la console KMS.
  2. Dans le panneau de navigation de gauche, sélectionnez Clés gérées par le client.
  3. Cliquez sur la clé gérée par le client que vous souhaitez modifier.
  4. Sous Stratégie de clé, cliquez sur Passer à la vue de stratégie.
  5. Cliquez sur Modifier.
  6. Ajoutez le rôle.

Résolution des problèmes liés à la suppression de ressources

Les points de restauration créés par AWS Backup ne peuvent pas être supprimés dans la fenêtre de console de la ressource protégée. Vous pouvez les supprimer sur la AWS Backup console en les sélectionnant dans le coffre où ils sont stockés, puis en choisissant Supprimer.

Pour supprimer un point de récupération ou un coffre-fort de sauvegarde, vous avez besoin des autorisations appropriées. Pour plus d'informations sur le contrôle d'accès à l'aide d'IAM avec AWS Backup, consultezContrôle d’accès.

Résolution des problèmes liés à la restauration de ressources

Restauration à l'aide de l'API

Pour restaurer une sauvegarde par programmation, utilisez l'opération d'API StartRestoreJob.

Pour obtenir les métadonnées de configuration avec lesquelles votre sauvegarde a été créée, vous pouvez appeler GetRecoveryPointRestoreMetadata.

Pour plus d'informations, consultez Restauration d'une sauvegarde.

Restauration avec la console

- Restauration de données Amazon S3
- Restauration d'une machine virtuelle
- Restauration d'un système de fichiers Amazon FSx
- Restauration d'un volume Amazon EBS
- Restauration d'un système de fichiers Amazon EFS
- Restauration d'une table Amazon DynamoDB
- Restauration d'une base de données Amazon RDS
- Restauration d'un cluster Aurora
- Restauration d'une instance Amazon EC2
- Restauration d'un volume Storage Gateway
- Restauration d'un cluster Amazon DocumentDB
- Restauration d'un cluster Neptune

Résolution des erreurs de formatage

Lorsqu'un caractère générique (*) est inclus pour la valeur d'un paramètre, le caractère générique est traité pour inclure des valeurs autres que des espaces. Les valeurs d'une paire clé-valeur contenant des espaces blancs ne seront pas incluses dans le caractère générique.

API AWS Backup

En plus de la console, vous pouvez utiliser les actions et les types de données de l'API AWS Backup pour configurer et gérer AWS Backup, ainsi que ses ressources, par programmation. Cette section décrit les actions et les types de données AWS Backup. Il contient la référence des API pour AWS Backup.

API AWS Backup

- Actions AWS Backup
- Types de données AWS Backup

Actions

Les actions suivantes sont prises en charge par AWS Backup :

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework

- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection

- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob

- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

Les actions suivantes sont prises en charge par AWS Backup gateway :

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource

- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AWS Backup

Les actions suivantes sont prises en charge par AWS Backup :

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications

- DeleteFramework
- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan

- GetRestoreTestingSelection
- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult

- StartBackupJob
- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

CancelLegalHold

Service : AWS Backup

Supprime le blocage légal spécifié sur un point de récupération. Cette action ne peut être effectuée que par un utilisateur disposant des autorisations suffisantes.

Syntaxe de la demande

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

CancelDescription

Chaîne qui décrit la raison pour laquelle la suspension légale a été supprimée.

Obligatoire : oui

legalHoldId

L'identifiant de la retenue légale.

Obligatoire : oui

RetainRecordInDays

Le montant entier, en jours, après lequel la suspension légale doit être supprimée.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 201
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidResourceStateException

AWS Backup exécute déjà une action sur ce point de récupération. Il ne peut pas exécuter l'action que vous avez demandée tant que la première action n'est pas terminée. Réessayez ultérieurement.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateBackupPlan

Service : AWS Backup

Crée un plan de sauvegarde à l'aide d'un nom de plan de sauvegarde et de règles de sauvegarde. Un plan de sauvegarde est un document qui contient des informations permettant de AWS Backup planifier des tâches qui créent des points de récupération pour les ressources.

Si vous appelez `CreateBackupPlan` avec un plan qui existe déjà, vous recevez une exception `AlreadyExistsException`.

Syntaxe de la demande

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
```

```
                "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
                "string" : "string"
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
        }
    ]
  },
  "BackupPlanTags": {
    "string" : "string"
  },
  "CreatorRequestId": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupPlan

Le corps d'un plan de secours. Comprend un `BackupPlanName` et un ou plusieurs ensembles de `Rules`.

Type : objet BackupPlanInput

Obligatoire : oui

BackupPlanTags

Les balises à attribuer au plan de sauvegarde.

Type : mappage chaîne/chaîne

Obligatoire : non

CreatorRequestId

Identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Si la demande inclut un `CreatorRequestId` qui correspond à un plan de sauvegarde existant, ce plan est renvoyé. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AdvancedBackupSettings

Les paramètres d'un type de ressource. Cette option est uniquement disponible pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Type : tableau d'objets AdvancedBackupSetting

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

BackupPlanId

ID du plan de sauvegarde.

Type : chaîne

CreationDate

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Ils ne peuvent pas être modifiés.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateBackupSelection

Service : AWS Backup

Crée un document JSON qui spécifie un ensemble de ressources à attribuer à un plan de sauvegarde. Pour des exemples, consultez Attribution de ressources par programmation.

Syntaxe de la demande

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
```

```
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreatorRequestId": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

ID du plan de sauvegarde.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupSelection

Le corps d'une demande visant à affecter un ensemble de ressources à un plan de sauvegarde.

Type : objet BackupSelection

Obligatoire : oui

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlanId

ID du plan de sauvegarde.

Type : chaîne

CreationDate

Date et heure de création d'une sélection de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

SelectionId

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateBackupVault

Service : AWS Backup

Crée un conteneur logique dans lequel sont stockées les sauvegardes. Une demande `CreateBackupVault` comprend un nom, éventuellement une ou plusieurs balises de ressource, une clé de chiffrement et un ID de demande.

> **Note**
>
> N'incluez pas de données sensibles, telles que des numéros de passeport, dans le nom d'un coffre-fort de sauvegarde.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés. Ces noms sont composés de lettres, de chiffres et de traits d'union.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupVaultTags

Les balises à attribuer au coffre de sauvegarde.

Type : mappage chaîne/chaîne

Obligatoire : non

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

EncryptionKeyArn

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
```

```
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés. Ces noms sont composés de lettres minuscules, des chiffres et de traits d'union.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Date et heure de création d'un coffre-fort de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateFramework

Service : AWS Backup

Crée un cadre avec un ou plusieurs contrôles. Un cadre est un ensemble de contrôles que vous pouvez utiliser pour évaluer vos pratiques de sauvegarde. En utilisant des contrôles personnalisables prédéfinis pour définir vos politiques, vous pouvez évaluer si vos pratiques de sauvegarde sont conformes à vos politiques et quelles ressources ne le sont pas encore.

Syntaxe de la demande

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkTags": {
      "string" : "string"
   },
   "IdempotencyToken": "string"
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

FrameworkControls

Les contrôles qui constituent le cadre. Chaque contrôle de la liste possède un nom, des paramètres d'entrée et une portée.

Type : tableau d'objets FrameworkControl

Obligatoire : oui

FrameworkDescription

Une description facultative du framework avec 1 024 caractères au maximum.

Type : chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

FrameworkName

Le nom unique du framework. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

FrameworkTags

Les balises à attribuer au framework.

Type : mappage chaîne/chaîne

Obligatoire : non

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `CreateFrameworkInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

FrameworkArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

FrameworkName

Le nom unique du framework. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS

- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLegalHold

Service : AWS Backup

Crée un blocage légal sur un point de récupération (sauvegarde). Une conservation légale est une restriction associée à la modification ou à la suppression d'une sauvegarde jusqu'à ce qu'un utilisateur autorisé annule la conservation légale. Toute action visant à supprimer ou dissocier un point de récupération échouera avec une erreur si une ou plusieurs conservations légales actives se trouvent sur le point de récupération.

Syntaxe de la demande

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
   "Description": "string",
   "IdempotencyToken": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Tags": {
      "string" : "string"
   },
   "Title": "string"
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Description

Description de la détention légale.

Type : chaîne

Obligatoire : oui

IdempotencyToken

Il s'agit d'une chaîne choisie par l'utilisateur utilisée pour faire la distinction entre des appels par ailleurs identiques. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

RecoveryPointSelection

Les critères d'attribution d'un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Type : objet RecoveryPointSelection

Obligatoire : non

Tags

Balises facultatives à inclure. Une balise est une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources. Les caractères autorisés incluent les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : /.

Type : mappage chaîne/chaîne

Obligatoire : non

Title

Titre de la retenue légale.

Type : chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Status": "string",
   "Title": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationDate

Heure à laquelle la mise en attente légale a été créée.

Type : Timestamp

Description

Description de la détention légale.

Type : chaîne

LegalHoldArn

L'Amazon Resource Name (ARN) de la conservation légale.

Type : chaîne

LegalHoldId

L'identifiant de la retenue légale.

Type : chaîne

RecoveryPointSelection

Les critères à attribuer à un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Type : objet RecoveryPointSelection

Status

Le statut de la mise en attente légale.

Type : chaîne

Valeurs valides : `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Titre de la retenue légale.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateLogicallyAirGappedBackupVault

Service : AWS Backup

Crée un conteneur logique dans lequel les sauvegardes peuvent être copiées.

Cette demande inclut un nom, la région, le nombre maximum de jours de rétention, le nombre minimum de jours de rétention et peut éventuellement inclure des balises et un ID de demande de créateur.

> **Note**
>
> N'incluez pas de données sensibles, telles que des numéros de passeport, dans le nom d'un coffre-fort de sauvegarde.

Syntaxe de la demande

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde logiquement cloisonnés sont identifiés par des noms uniques au compte utilisé pour les créer et la région dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupVaultTags

Les balises à attribuer au coffre.

Type : mappage chaîne/chaîne

Obligatoire : non

CreatorRequestId

ID de la demande de création.

Ce paramètre est facultatif. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

MaxRetentionDays

Période de conservation maximale pendant laquelle le coffre conserve ses points de récupération. Si ce paramètre n'est pas spécifié, AWS Backup n'applique pas de période de rétention maximale sur les points de récupération dans le coffre-fort (permettant un stockage indéfini).

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou inférieure à la période de rétention maximale. Si la période de rétention de la tâche est plus longue que cette période de rétention maximale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort.

Type : long

Obligatoire : oui

MinRetentionDays

Ce paramètre spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, aucune période de rétention minimale n'est appliquée.

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou supérieure à la période de rétention minimale. Si la période de rétention d'une tâche est plus courte que cette période de rétention minimale, la tâche de sauvegarde ou de copie du coffre-fort échoue et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort.

Type : long

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

L'ARN (Amazon Resource Name) du coffre.

Type : chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde logiquement cloisonnés sont identifiés par des noms uniques au compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Date et heure de la création du coffre-fort.

Cette valeur est au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

VaultState

État actuel du coffre.

Type : chaîne

Valeurs valides : `CREATING | AVAILABLE | FAILED`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d'état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateReportPlan

Service : AWS Backup

Crée un plan de rapport. Un plan de rapport est un document qui contient des informations sur le contenu du rapport et sur l'endroit où il AWS Backup sera livré.

Si vous appelez `CreateReportPlan` avec un plan qui existe déjà, vous recevez une exception `AlreadyExistsException`.

Syntaxe de la demande

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `CreateReportPlanInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

ReportDeliveryChannel

Une structure qui contient des informations sur où et comment livrer vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Type : objet ReportDeliveryChannel

Obligatoire : oui

ReportPlanDescription

Une description facultative du plan de rapport avec 1 024 caractères au maximum.

Type : chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

ReportPlanName

Le nom unique du plan de rapport. Ce nom doit contenir entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

ReportPlanTags

Les balises à attribuer au plan de rapport.

Type : mappage chaîne/chaîne

Obligatoire : non

ReportSetting

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Si le modèle de rapport est `RESOURCE_COMPLIANCE_REPORT` ou`CONTROL_COMPLIANCE_REPORT`, cette ressource d'API décrit également la couverture du rapport par Régions AWS et les frameworks.

Type : objet ReportSetting

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'un coffre-fort de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

ReportPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

ReportPlanName

Le nom unique du plan de rapport.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateRestoreTestingPlan

Service : AWS Backup

Crée un plan de test de restauration.

La première des deux étapes pour créer un plan de test de restauration. Une fois cette demande réussie, terminez la procédure en utilisant CreateRestoreTestingSelection.

Syntaxe de la demande

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   },
   "Tags": {
      "string" : "string"
   }
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

CreatorRequestId

Il s'agit d'une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

RestoreTestingPlan

Un plan de tests de la restauration doit contenir une chaîne `RestoreTestingPlanName` unique que vous créez et doit contenir un cron `ScheduleExpression`. Vous pouvez éventuellement inclure un nombre entier `StartWindowHours` et une chaîne `CreatorRequestId`.

`RestoreTestingPlanName` est une chaîne unique qui est le nom du plan de test de la restauration. Elle ne peut pas être modifiée après sa création et elle doit être composée uniquement de caractères alphanumériques et de traits de soulignement.

Type : objet RestoreTestingPlanForCreate

Obligatoire : oui

Tags

Les balises à attribuer au plan de test de restauration.

Type : mappage chaîne/chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d’un plan de test de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique le plan de test de la restauration créé.

Type : chaîne

RestoreTestingPlanName

Cette chaîne unique est le nom du plan de test de la restauration.

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d’état HTTP : 400

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateRestoreTestingSelection

Service : AWS Backup

Cette demande peut être envoyée une fois que la CreateRestoreTestingPlan demande a été renvoyée avec succès. Il s'agit de la deuxième partie de la création d'un plan de test des ressources, qui doit être réalisée de manière séquentielle.

Cela comprend `RestoreTestingSelectionName`, `ProtectedResourceType` et l'un des éléments suivants :

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Chaque type de ressource protégée peut avoir une seule valeur.

Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour `ProtectedResourceArns` avec `ProtectedResourceConditions`. Vous pouvez également inclure jusqu'à 30 ARN de ressources protégées spécifiques dans `ProtectedResourceArns`.

Impossible de sélectionner à la fois les types de ressources protégées ET les ARN spécifiques. La demande échouera si les deux sont inclus.

Syntaxe de la demande

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
```

```
                "Key": "string",
                "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Entrez le nom du plan de test de restauration renvoyé par la CreateRestoreTestingPlan demande correspondante.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

CreatorRequestId

Il s'agit d'une chaîne unique facultative qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

RestoreTestingSelection

Cela comprend `RestoreTestingSelectionName`, `ProtectedResourceType` et l'un des éléments suivants :

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Chaque type de ressource protégée peut avoir une seule valeur.

Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour `ProtectedResourceArns` avec `ProtectedResourceConditions`. Vous pouvez également inclure jusqu'à 30 ARN de ressources protégées spécifiques dans `ProtectedResourceArns`.

Type : objet RestoreTestingSelectionForCreate

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle la sélection des ressources testées a été créée.

Type : Timestamp

RestoreTestingPlanArn

L'ARN du plan de test de restauration auquel la sélection de test de restauration est associée.

Type : chaîne

RestoreTestingPlanName

Nom du plan de test de restauration.

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : chaîne

RestoreTestingSelectionName

Nom de la sélection de test de restauration pour le plan de test de restauration associé.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteBackupPlan

Service : AWS Backup

Supprime un plan de sauvegarde. Un plan de sauvegarde ne peut être supprimé qu'une fois que toutes les sélections de ressources associées ont été supprimées. La suppression d'un plan de sauvegarde supprime la version actuelle d'un plan de sauvegarde. Les versions précédentes, le cas échéant, existeront toujours.

Syntaxe de la demande

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

DeletionDate

Date et heure de suppression d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `DeletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Les ID de version ne peuvent pas être modifiés.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteBackupSelection

Service : AWS Backup

Supprime la sélection de ressources associée à un plan de sauvegarde spécifié par l'`SelectionId`.

Syntaxe de la demande

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

selectionId

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteBackupVault

Service : AWS Backup

Supprime le coffre-fort de sauvegarde identifié par son nom. Un coffre-fort ne peut être supprimé que s'il est vide.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteBackupVaultAccessPolicy

Service : AWS Backup

Supprime le document de politique qui gère les autorisations sur un coffre-fort de sauvegarde.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés. Ces noms sont composés de lettres minuscules, des chiffres et de traits d'union.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteBackupVaultLockConfiguration

Service : AWS Backup

Supprime AWS Backup Vault Lock d'un coffre-fort de sauvegarde spécifié par un nom de coffre-fort de sauvegarde.

Si la configuration de Vault Lock est immuable, vous ne pouvez pas supprimer Vault Lock à l'aide des opérations de l'API et vous recevrez une `InvalidRequestException` si vous essayez de le faire. Pour plus d'informations, consultez Vault Lock dans le guide du AWS Backup développeur.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Nom du coffre-fort de sauvegarde dans lequel vous souhaitez supprimer AWS Backup Vault Lock.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteBackupVaultNotifications

Service : AWS Backup

Supprime les notifications d'événement pour le coffre-fort de sauvegarde spécifié.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteFramework

Service : AWS Backup

Supprime le framework spécifié par un nom de framework.

Syntaxe de la demande

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

frameworkName

Le nom unique d'un cadre.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteRecoveryPoint

Service : AWS Backup

Supprime le point de récupération spécifié par un ID de point de récupération.

Si l'ID du point de récupération appartient à une sauvegarde continue, l'appel de ce point de terminaison supprime la sauvegarde continue existante et arrête la sauvegarde continue future.

Lorsque les autorisations d'un rôle IAM sont insuffisantes pour appeler cette API, le service renvoie une réponse HTTP 200 avec un corps HTTP vide, mais le point de récupération n'est pas supprimé. Au lieu de cela, il entre dans un état `EXPIRED`.

Les points de récupération `EXPIRED` peuvent être supprimés avec cette API une fois que le rôle IAM a activé l'action `iam:CreateServiceLinkedRole`. Pour en savoir plus sur l'ajout de ce rôle, consultez Résolution des problèmes liés aux suppressions manuelles.

Si l'utilisateur ou le rôle est supprimé ou si l'autorisation associée au rôle est supprimée, la suppression échouera et entrera dans un état `EXPIRED`.

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

InvalidResourceStateException

AWS Backup exécute déjà une action sur ce point de récupération. Il ne peut pas exécuter l'action que vous avez demandée tant que la première action n'est pas terminée. Réessayez ultérieurement.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteReportPlan

Service : AWS Backup

Supprime le plan de rapport spécifié par un nom de plan de rapport.

Syntaxe de la demande

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportPlanName

Le nom unique d'un plan de rapport.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteRestoreTestingPlan

Service : AWS Backup

Cette demande supprime le plan de test de la restauration spécifié.

La suppression ne peut réussir que si toutes les sélections de tests de la restauration associées sont d'abord supprimées.

Syntaxe de la demande

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration que vous souhaitez supprimer.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteRestoreTestingSelection

Service : AWS Backup

Entrez le nom du plan de test de la restauration et le nom de la sélection de tests de la restauration.

Toutes les sélections de tests associées à un plan de test de la restauration doivent être supprimées avant que le plan de test de la restauration ne puisse être supprimé.

Syntaxe de la demande

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration contenant la sélection de tests de la restauration que vous souhaitez supprimer.

Obligatoire : oui

RestoreTestingSelectionName

Nom unique obligatoire de la sélection de tests de la restauration que vous souhaitez supprimer.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeBackupJob

Service : AWS Backup

Renvoie les détails de la tâche de sauvegarde pour l'`BackupJobId` spécifié.

Syntaxe de la demande

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupJobId": "string",
   "BackupOptions": {
      "string" : "string"
   },
   "BackupSizeInBytes": number,
   "BackupType": "string",
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "BytesTransferred": number,
   "ChildJobsInState": {
      "string" : number
   },
```

```
   "CompletionDate": number,
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "ExpectedCompletionDate": number,
   "IamRoleArn": "string",
   "InitiationDate": number,
   "IsParent": boolean,
   "MessageCategory": "string",
   "NumberOfChildJobs": number,
   "ParentJobId": "string",
   "PercentDone": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "StartBy": number,
   "State": "string",
   "StatusMessage": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AccountId

Renvoie l'ID de compte du propriétaire de la tâche de sauvegarde.

Type : chaîne

Modèle : `^[0-9]{12}$`

BackupJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Type : chaîne

BackupOptions

Représente les options spécifiées dans le cadre du plan de sauvegarde ou de la tâche de sauvegarde à la demande.

Type : mappage chaîne/chaîne

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.]{1,50}$`

BackupSizeInBytes

Taille d'une sauvegarde, en octets.

Type : long

BackupType

Représente le type de sauvegarde réel sélectionné pour une tâche de sauvegarde. Par exemple, si une sauvegarde Windows Volume Shadow Copy Service (VSS) a bien été effectuée, `BackupType` renvoie `"WindowsVSS"`. Si `BackupType` est vide, le type de sauvegarde était une sauvegarde normale.

Type : chaîne

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

BytesTransferred

Taille en octets transférée vers un coffre-fort de sauvegarde au moment où le statut de la tâche a été demandé.

Type : long

ChildJobsInState

Cela renvoie les statistiques des tâches de sauvegarde enfant (imbriquées) incluses.

Type : mappage chaîne/long

Clés valides : `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

CompletionDate

Date et heure de fin d'une tâche de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche de sauvegarde, dont `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour la créer.

Type : objet RecoveryPointCreator

CreationDate

Date et heure de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

ExpectedCompletionDate

Date et heure de fin attendues d'une tâche de sauvegarde des ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `ExpectedCompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

InitiationDate

Date à laquelle une tâche de sauvegarde a été initiée.

Type : Timestamp

IsParent

Cela renvoie la valeur booléenne indiquant qu'une tâche de sauvegarde est une tâche parent (composite).

Type : booléen

MessageCategory

Nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes peuvent inclure `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` et `INVALIDPARAMETERS`. Consultez la section Surveillance pour obtenir la liste des MessageCategory chaînes acceptées.

Type : chaîne

NumberOfChildJobs

Cela renvoie le nombre de tâches de sauvegarde enfant (imbriquées).

Type : long

ParentJobId

Cela renvoie l'ID de la tâche de sauvegarde de la ressource parent (composite).

Type : chaîne

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : chaîne

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

ResourceArn

Un ARN qui identifie de façon unique une ressource enregistrée. Le format de l'ARN dépend du type de ressource.

Type : chaîne

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

ResourceType

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

Spécifie l'heure au format Unix et au format UTC (Coordinated Universal Time) quand une tâche de sauvegarde doit être démarrée avant d'être annulée. La valeur est calculée en ajoutant la fenêtre de démarrage à l'heure planifiée. Ainsi, si l'heure prévue était 18 h 00 et que la fenêtre de début était de 2 heures, l'heure `StartBy` serait 20 h 00 à la date spécifiée. La valeur de `StartBy` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

State

L'état actuel d'une tâche de sauvegarde.

Type : chaîne

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

Message détaillé expliquant le statut de la tâche de sauvegarde d'une ressource.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

DependencyFailureException

Un AWS service ou une ressource dépendant a renvoyé une erreur au AWS Backup service et l'action ne peut pas être terminée.

Code d’état HTTP : 500

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeBackupVault

Service : AWS Backup

Renvoie les métadonnées relatives à un coffre-fort de sauvegarde spécifié par son nom.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

ID de compte du coffre-fort de sauvegarde spécifié.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string",
   "LockDate": number,
```

```
    "Locked": boolean,
    "MaxRetentionDays": number,
    "MinRetentionDays": number,
    "NumberOfRecoveryPoints": number,
    "VaultType": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : chaîne

CreationDate

Date et heure de création d'un coffre-fort de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif. S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

EncryptionKeyArn

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : chaîne

LockDate

Date et heure auxquelles la configuration de AWS Backup Vault Lock ne peut pas être modifiée ou supprimée.

Si vous avez appliqué Vault Lock à votre coffre-fort sans spécifier de date de verrouillage, vous pouvez modifier les paramètres de Vault Lock ou supprimer complètement Vault Lock du coffre-fort à tout moment.

Cette valeur est au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Locked

Un booléen qui indique si AWS Backup Vault Lock protège actuellement le coffre-fort de sauvegarde. `True`signifie que Vault Lock entraîne l'échec des opérations de suppression ou de mise à jour sur les points de récupération stockés dans le coffre-fort.

Type : booléen

MaxRetentionDays

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention maximale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, Vault Lock n'applique pas de période de rétention maximale sur les points de récupération dans le coffre-fort (permettant un stockage indéfini).

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou inférieure à la période de rétention maximale. Si la période de conservation de la tâche est plus longue que cette période de conservation maximale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous

devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

MinRetentionDays

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, le verrouillage du coffre-fort n'appliquera pas de période de conservation minimale.

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou supérieure à la période de rétention minimale. Si la période de rétention de la tâche est plus courte que cette période de rétention minimale, la tâche de sauvegarde ou de copie du coffre-fort échoue et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

NumberOfRecoveryPoints

Nombre de points de récupération stockés dans un coffre-fort de sauvegarde.

Type : long

VaultType

Type de coffre décrit.

Type : chaîne

Valeurs valides : `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeCopyJob

Service : AWS Backup

Renvoie les métadonnées associées à la création d'une copie d'une ressource.

Syntaxe de la demande

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

copyJobId

Identifie de manière unique une tâche de copie.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJob": {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "ChildJobsInState": {
         "string" : number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
      "CopyJobId": "string",
      "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
```

```
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
        },
        "CreationDate": number,
        "DestinationBackupVaultArn": "string",
        "DestinationRecoveryPointArn": "string",
        "IamRoleArn": "string",
        "IsParent": boolean,
        "MessageCategory": "string",
        "NumberOfChildJobs": number,
        "ParentJobId": "string",
        "ResourceArn": "string",
        "ResourceName": "string",
        "ResourceType": "string",
        "SourceBackupVaultArn": "string",
        "SourceRecoveryPointArn": "string",
        "State": "string",
        "StatusMessage": "string"
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CopyJob

Contient des informations détaillées sur une tâche de copie.

Type : objet CopyJob

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeFramework

Service : AWS Backup

Renvoie les détails du framework pour le paramètre `FrameworkName` spécifié.

Syntaxe de la demande

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

frameworkName

Le nom unique d'un cadre.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "DeploymentStatus": "string",
   "FrameworkArn": "string",
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
```

```
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkStatus": "string",
   "IdempotencyToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'un framework, dans une représentation ISO 8601. La valeur de `CreationTime` est précise en millisecondes. Par exemple, 2020-07-10T15:00:00.000-08:00 représente le 10 juillet 2020 à 15 h 00 avec 8 heures de retard sur le temps UTC.

Type : Timestamp

DeploymentStatus

Le statut du déploiement d'un framework. Les statuts sont les suivants :

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Type : chaîne

FrameworkArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

FrameworkControls

Les contrôles qui constituent le cadre. Chaque contrôle de la liste possède un nom, des paramètres d'entrée et une portée.

Type : tableau d'objets FrameworkControl

FrameworkDescription

Description facultative du framework.

Type : chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

FrameworkName

Le nom unique d'un cadre.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

Un cadre est constitué d'un ou plusieurs contrôles. Chaque contrôle régit une ressource, telle que les plans de sauvegarde, les sélections de sauvegarde, les coffres-forts de sauvegarde ou les points de récupération. Vous pouvez également activer ou désactiver AWS Config l'enregistrement pour chaque ressource. Les statuts sont les suivants :

- `ACTIVE` lorsque l'enregistrement est activé pour toutes les ressources que le framework gouverne.
- `PARTIALLY_ACTIVE` lorsque l'enregistrement est désactivé pour au moins une ressource que le framework gouverne.
- `INACTIVE` lorsque l'enregistrement est désactivé pour toutes les ressources que le framework gouverne.
- `UNAVAILABLE`lorsqu'il n' AWS Backup est pas en mesure de valider le statut de l'enregistrement pour le moment.

Type : chaîne

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `DescribeFrameworkOutput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeGlobalSettings

Service : AWS Backup

Décrit si le AWS compte est activé pour la sauvegarde entre comptes. Renvoie une erreur si le compte n'est pas membre d'une organisation Organizations. Exemple : `describe-global-settings --region us-west-2`

Syntaxe de la demande

```
GET /global-settings HTTP/1.1
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GlobalSettings

Statut de l'indicateur `isCrossAccountBackupEnabled`.

Type : mappage chaîne/chaîne

LastUpdateTime

Date et heure de la dernière mise à jour de l'indicateur `isCrossAccountBackupEnabled`. Cette mise à jour est au format Unix et UTC (temps universel coordonné). La valeur de `LastUpdateTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeProtectedResource

Service : AWS Backup

Renvoie des informations sur une ressource enregistrée, notamment la dernière fois qu'elle a été sauvegardée, son Amazon Resource Name (ARN) et le type de AWS service de la ressource enregistrée.

Syntaxe de la demande

```
GET /resources/resourceArn HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

resourceArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "LastBackupTime": number,
   "LastBackupVaultArn": "string",
   "LastRecoveryPointArn": "string",
   "LatestRestoreExecutionTimeMinutes": number,
   "LatestRestoreJobCreationDate": number,
   "LatestRestoreRecoveryPointCreationDate": number,
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string"
```

```
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LastBackupTime

Date et heure de la dernière sauvegarde d'une ressource, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastBackupTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

LastBackupVaultArn

L'ARN (Amazon Resource Name) du coffre de sauvegarde qui contient le point de restauration de sauvegarde le plus récent.

Type : chaîne

LastRecoveryPointArn

L'ARN (Amazon Resource Name) du point de récupération le plus récent.

Type : chaîne

LatestRestoreExecutionTimeMinutes

Durée, en minutes, nécessaire à l'exécution de la tâche de restauration la plus récente.

Type : long

LatestRestoreJobCreationDate

Date de création de la tâche de restauration la plus récente.

Type : Timestamp

LatestRestoreRecoveryPointCreationDate

Date à laquelle le point de récupération le plus récent a été créé.

Type : Timestamp

ResourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

ResourceName

Nom de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

ResourceType

Type de AWS ressource enregistrée en tant que point de récupération ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeRecoveryPoint

Service : AWS Backup

Renvoie les métadonnées associées à un point de récupération, notamment l'ID, le statut, le chiffrement et le cycle de vie.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

ID de compte du coffre-fort de sauvegarde spécifié.

Modèle : `^[0-9]{12}$`

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupSizeInBytes": number,
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "CompletionDate": number,
   "CompositeMemberIdentifier": "string",
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "EncryptionKeyArn": "string",
   "IamRoleArn": "string",
   "IsEncrypted": boolean,
   "IsParent": boolean,
   "LastRestoreTime": number,
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "ParentRecoveryPointArn": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "SourceBackupVaultArn": "string",
   "Status": "string",
   "StatusMessage": "string",
   "StorageClass": "string",
   "VaultType": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupSizeInBytes

Taille d'une sauvegarde, en octets.

Type : long

BackupVaultArn

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

Un objet `CalculatedLifecycle` contenant des horodatages `DeleteAt` et `MoveToColdStorageAt`.

Type : objet CalculatedLifecycle

CompletionDate

Date et heure de fin d'une tâche de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CompositeMemberIdentifier

Identifiant d'une ressource au sein d'un groupe composite, tel qu'un point de récupération imbriqué (enfant) appartenant à une pile composite (parent). L'ID est transféré à partir de l'ID logique au sein d'une pile.

Type : chaîne

CreatedBy

Contient des informations d'identification relatives à la création d'un point de récupération, notamment les valeurs `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour le créer.

Type : objet RecoveryPointCreator

CreationDate

Date et heure de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

EncryptionKeyArn

Clé de chiffrement côté serveur utilisée pour protéger vos sauvegardes ; par exemple, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : chaîne

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

IsEncrypted

Valeur booléenne renvoyée comme `TRUE` si le point de récupération spécifié était chiffré ou `FALSE` s'il n'était pas chiffré.

Type : booléen

IsParent

Cela renvoie la valeur booléenne indiquant qu'un point de récupération est une tâche parent (composite).

Type : booléen

LastRestoreTime

Date et heure de la dernière restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastRestoreTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet Lifecycle

ParentRecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération parent (composite) ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

ResourceArn

Un ARN qui identifie de façon unique une ressource enregistrée. Le format de l'ARN dépend du type de ressource.

Type : chaîne

ResourceName

Nom de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

ResourceType

Type de AWS ressource à enregistrer comme point de récupération ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

Un Amazon Resource Name (ARN) qui identifie de façon unique le coffre-fort source dans lequel la ressource a été initialement sauvegardée ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`. Si la restauration est rétablie sur le même AWS compte ou la même région, cette valeur sera`null`.

Type : chaîne

Status

Code de statut spécifiant l'état du point de récupération.

`PARTIAL`le statut indique qu' AWS Backup il n'a pas été possible de créer le point de restauration avant la fermeture de la fenêtre de sauvegarde. Pour augmenter la fenêtre de votre plan de

sauvegarde à l'aide de l'API, consultez UpdateBackupPlan. Vous pouvez également augmenter la fenêtre de votre plan de sauvegarde à l'aide de la console en choisissant et en modifiant votre plan de sauvegarde.

`EXPIRED`le statut indique que le point de restauration a dépassé sa période de rétention, mais qu'il n'est AWS Backup pas autorisé ou qu'il est incapable de le supprimer pour une autre raison. Pour supprimer manuellement ces points de récupération, voir Étape 3 : Supprimer les points de récupération dans la section Nettoyage des ressources du guide Mise en route.

Le statut `STOPPED` apparaît lors d'une sauvegarde continue lorsqu'un utilisateur a effectué une action qui entraîne la désactivation de la sauvegarde continue. Cela peut être dû à la suppression des autorisations, à la désactivation de la gestion des versions, à la désactivation des événements envoyés ou à EventBridge la désactivation des EventBridge règles mises en place par. AWS Backup

Pour résoudre le statut `STOPPED`, assurez-vous que toutes les autorisations demandées sont en place et que la gestion des versions est activée sur le compartiment S3. Une fois ces conditions remplies, la prochaine instance d'une règle de sauvegarde exécutée entraînera la création d'un nouveau point de récupération continue. Les points de récupération ayant le statut ARRÊTÉ n'ont pas besoin d'être supprimés.

Pour SAP HANA sur Amazon EC2, le statut `STOPPED` est dû à une action de l'utilisateur, à une mauvaise configuration de l'application ou à un échec de sauvegarde. Pour garantir le succès des futures sauvegardes continues, reportez-vous au statut du point de récupération et consultez SAP HANA pour plus de détails.

Type : chaîne

Valeurs valides : `COMPLETED | PARTIAL | DELETING | EXPIRED`

StatusMessage

Message de statut expliquant le statut du point de récupération.

Type : chaîne

StorageClass

Spécifie la classe de stockage du point de récupération. Les valeurs valides sont `WARM` ou `COLD`.

Type : chaîne

Valeurs valides : `WARM | COLD | DELETED`

VaultType

Type de coffre-fort dans lequel le point de restauration décrit est stocké.

Type : chaîne

Valeurs valides : `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS

- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeRegionSettings

Service : AWS Backup

Renvoie les paramètres actuels d'activation du service pour la région. Si l'abonnement au service est activé pour un service, AWS Backup essaie de protéger les ressources de ce service dans cette région, lorsque la ressource est incluse dans une sauvegarde à la demande ou un plan de sauvegarde planifiée. Sinon, AWS Backup n'essaie pas de protéger les ressources de ce service dans cette région.

Syntaxe de la demande

```
GET /account-settings HTTP/1.1
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ResourceTypeManagementPreference

Indique si les sauvegardes d'un type de ressource sont AWS Backup entièrement gérées.

Pour connaître les avantages de la AWS Backup gestion complète, consultez la section AWS Backup Gestion complète.

Pour obtenir la liste des types de ressources et savoir si chacun prend en charge AWS Backup la gestion complète, consultez le tableau Disponibilité des fonctionnalités par ressource.

Si`"DynamoDB":false`, vous pouvez activer la AWS Backup gestion complète de la sauvegarde DynamoDB en activant les fonctionnalités avancées AWS Backup de sauvegarde DynamoDB.

Type : chaîne vers un mappage booléen

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

Les services ainsi que les préférences d'inscription dans la région.

Type : chaîne vers un mappage booléen

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS

- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeReportJob

Service : AWS Backup

Renvoie les détails associés à la création d'un rapport tel que spécifié par son `ReportJobId`.

Syntaxe de la demande

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportJobId

Identifiant de la tâche de rapport. Une chaîne codée en Unicode, UTF-8 unique et générée de façon aléatoire qui contiennent au maximum 1 024 octets. L'ID de tâche de rapport ne peut pas être modifié.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJob": {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
         "S3BucketName": "string",
         "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
```

```
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ReportJob

Les informations relatives à une tâche de rapport, notamment ses heures d'achèvement et de création, la destination du rapport, l'identifiant unique de la tâche de rapport, le nom de ressource Amazon (ARN), le modèle de rapport, le statut et le message de statut.

Type : objet ReportJob

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeReportPlan

Service : AWS Backup

Renvoie la liste de tous les plans de rapport pour un Compte AWS et Région AWS.

Syntaxe de la demande

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportPlanName

Le nom unique d'un plan de rapport.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
```

```
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "OrganizationUnits": [ "string" ],
         "Regions": [ "string" ],
         "ReportTemplate": "string"
      }
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ReportPlan

Renvoie des informations sur le plan de rapport spécifié par son nom. Ces informations incluent l'Amazon Resource Name (ARN), la description, les paramètres, le canal de livraison, le statut du déploiement, l'heure de création et les dernières tentatives d'exécution du plan de rapport ainsi que celles ayant réussi.

Type : objet ReportPlan

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DescribeRestoreJob

Service : AWS Backup

Renvoie les métadonnées associées à une tâche de restauration spécifiée par un ID de tâche.

Syntaxe de la demande

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

restoreJobId

Identifie de manière unique la tâche qui restaure un point de récupération.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupSizeInBytes": number,
   "CompletionDate": number,
   "CreatedBy": {
      "RestoreTestingPlanArn": "string"
   },
   "CreatedResourceArn": "string",
   "CreationDate": number,
   "DeletionStatus": "string",
   "DeletionStatusMessage": "string",
   "ExpectedCompletionTimeMinutes": number,
   "IamRoleArn": "string",
   "PercentDone": "string",
```

```
    "RecoveryPointArn": "string",
    "RecoveryPointCreationDate": number,
    "ResourceType": "string",
    "RestoreJobId": "string",
    "Status": "string",
    "StatusMessage": "string",
    "ValidationStatus": "string",
    "ValidationStatusMessage": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AccountId

Renvoie l'ID de compte du propriétaire de la tâche de restauration.

Type : chaîne

Modèle : `^[0-9]{12}$`

BackupSizeInBytes

Taille, en octets, de la ressource restaurée.

Type : long

CompletionDate

Date et heure de fin d'une tâche de restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche de restauration.

Type : objet RestoreJobCreator

CreatedResourceArn

Le nom de ressource Amazon (ARN) de la ressource créée par la tâche de restauration.

Le format de l'ARN dépend du type de ressource sauvegardée.

Type : chaîne

CreationDate

Date et heure de création d'une tâche de restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

DeletionStatus

État des données générées par le test de restauration.

Type : chaîne

Valeurs valides : `DELETING | FAILED | SUCCESSFUL`

DeletionStatusMessage

Cela décrit le statut de suppression de la tâche de restauration.

Type : chaîne

ExpectedCompletionTimeMinutes

Durée en minutes prévue d'une tâche de restauration d'un point de récupération.

Type : long

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : chaîne

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

RecoveryPointCreationDate

Date de création du point de restauration créé par la tâche de restauration spécifiée.

Type : Timestamp

ResourceType

Renvoie les métadonnées associées à une tâche de restauration répertoriées par type de ressource.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

Identifie de manière unique la tâche qui restaure un point de récupération.

Type : chaîne

Status

Code d'état spécifiant l'état de la tâche initiée AWS Backup pour restaurer un point de restauration.

Type : chaîne

Valeurs valides : `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

Message indiquant le statut d'une tâche de restauration d'un point de récupération.

Type : chaîne

ValidationStatus

État de la validation exécutée sur la tâche de restauration indiquée.

Type : chaîne

Valeurs valides : `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

Message d'état.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

DependencyFailureException

Un AWS service ou une ressource dépendant a renvoyé une erreur au AWS Backup service et l'action ne peut pas être terminée.

Code d’état HTTP : 500

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DisassociateRecoveryPoint

Service : AWS Backup

Supprime le point de restauration de sauvegarde continue spécifié AWS Backup et confie le contrôle de cette sauvegarde continue au service source, tel qu'Amazon RDS. Le service source continuera à créer et à conserver des sauvegardes continues en utilisant le cycle de vie que vous avez spécifié dans votre plan de sauvegarde d'origine.

Ne prend pas en charge les points de récupération des sauvegardes d'instantanés.

Syntaxe de la demande

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Nom unique d'un AWS Backup coffre-fort.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de manière unique un point AWS Backup de récupération.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

InvalidResourceStateException

AWS Backup exécute déjà une action sur ce point de récupération. Il ne peut pas exécuter l'action que vous avez demandée tant que la première action n'est pas terminée. Réessayez ultérieurement.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DisassociateRecoveryPointFromParent

Service : AWS Backup

Cette action sur un point de récupération enfant (imbriqué) spécifique supprime la relation entre le point de récupération spécifié et son point de récupération parent (composite).

Syntaxe de la demande

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Nom d'un conteneur logique dans lequel le point de récupération enfant (imbriqué) est stocké. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique le point de récupération enfant (imbriqué) ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 204
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ExportBackupPlanTemplate

Service : AWS Backup

Renvoie le plan de sauvegarde spécifié par l'ID du plan en tant que modèle de sauvegarde.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlanTemplateJson

Le corps d'un modèle de plan de sauvegarde au format JSON.

> **Note**
>
> Il s'agit d'un document JSON signé qui ne peut pas être modifié avant d'être transmis à `GetBackupPlanFromJSON`.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS

- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetBackupPlan

Service : AWS Backup

Renvoie les informations `BackupPlan` pour l'`BackupPlanId` spécifié. Les informations constituent le corps d'un plan de sauvegarde au format JSON, en plus des métadonnées.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Les ID de version ne peuvent pas être modifiés.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
```

```
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
```

```
    "CreatorRequestId": "string",
    "DeletionDate": number,
    "LastExecutionDate": number,
    "VersionId": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AdvancedBackupSettings

Contient une liste d'`BackupOptions` pour chaque type de ressource. La liste est renseignée uniquement si l'option avancée est définie pour le plan de sauvegarde.

Type : tableau d'objets AdvancedBackupSetting

BackupPlan

Spécifie le corps d'un plan de sauvegarde. Comprend un `BackupPlanName` et un ou plusieurs ensembles de `Rules`.

Type : objet BackupPlan

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

CreationDate

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois.

Type : chaîne

DeletionDate

Date et heure de suppression d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `DeletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

LastExecutionDate

La dernière fois que ce plan de sauvegarde a été exécuté. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de `LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Les ID de version ne peuvent pas être modifiés.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetBackupPlanFromJSON

Service : AWS Backup

Renvoie un document JSON valide spécifiant un plan de sauvegarde ou une erreur.

Syntaxe de la demande

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupPlanTemplateJson

Document de plan de sauvegarde fourni par le client au format JSON.

Type : chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
```

```
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlan

Spécifie le corps d'un plan de sauvegarde. Comprend un `BackupPlanName` et un ou plusieurs ensembles de `Rules`.

Type : objet BackupPlan

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetBackupPlanFromTemplate

Service : AWS Backup

Renvoie le modèle spécifié par son `templateId` en tant que plan de sauvegarde.

Syntaxe de la demande

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

templateId

Identifie de manière unique un modèle de plan de sauvegarde enregistré.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanDocument": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
```

```
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlanDocument

Renvoie le corps d'un plan de sauvegarde en fonction du modèle cible, y compris le nom, les règles et le coffre-fort de sauvegarde du plan.

Type : objet BackupPlan

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

GetBackupSelection

Service : AWS Backup

Renvoie les métadonnées de sélection et un document au format JSON qui spécifie une liste de ressources associées à un plan de sauvegarde.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

selectionId

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
```

```
                "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreationDate": number,
   "CreatorRequestId": "string",
   "SelectionId": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

BackupSelection

Spécifie le corps d'une demande pour attribuer un ensemble de ressources à un plan de secours.

Type : objet BackupSelection

CreationDate

Date et heure de création d'une sélection de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois.

Type : chaîne

SelectionId

Identifie de façon unique le corps d'une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetBackupVaultAccessPolicy

Service : AWS Backup

Renvoie le document de stratégie d'accès associé au coffre-fort de sauvegarde nommé.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Policy

Document de stratégie d'accès au coffre-fort de sauvegarde au format JSON.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetBackupVaultNotifications

Service : AWS Backup

Renvoie des notifications d'événement pour le coffre-fort de sauvegarde spécifié.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

BackupVaultEvents

Tableau d'événements qui indiquent le statut des tâches de sauvegarde des ressources dans le coffre-fort de sauvegarde.

Type : tableau de chaînes

Valeurs valides : `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED`

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

ARN qui identifie de façon unique une rubrique Amazon Simple Notification Service (Amazon SNS) ; par exemple, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

GetLegalHold

Service : AWS Backup

Cette action renvoie les détails d'une conservation légale spécifiée. Les détails constituent le corps d'une conservation légale au format JSON, en plus des métadonnées.

Syntaxe de la demande

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

legalHoldId

L'identifiant de la retenue légale.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CancelDescription": "string",
   "CancellationDate": number,
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
```

```
      "VaultNames": [ "string" ]
   },
   "RetainRecordUntil": number,
   "Status": "string",
   "Title": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CancelDescription

La raison de la levée de la suspension légale.

Type : chaîne

CancellationDate

Heure à laquelle le blocage légal a été annulé.

Type : Timestamp

CreationDate

Heure à laquelle la mise en attente légale a été créée.

Type : Timestamp

Description

Description de la détention légale.

Type : chaîne

LegalHoldArn

L'ARN du framework pour la conservation légale spécifiée. Le format de l'ARN dépend du type de ressource.

Type : chaîne

LegalHoldId

L'identifiant de la retenue légale.

Type : chaîne

RecoveryPointSelection

Les critères d'attribution d'un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Type : objet RecoveryPointSelection

RetainRecordUntil

Date et heure jusqu'à laquelle le dossier de conservation légal est conservé.

Type : Timestamp

Status

Le statut de la suspension légale.

Type : chaîne

Valeurs valides : `CREATING | ACTIVE | CANCELING | CANCELED`

Title

Titre de la retenue légale.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetRecoveryPointRestoreMetadata

Service : AWS Backup

Renvoie un ensemble de paires clé-valeur de métadonnées qui ont été utilisées pour créer la sauvegarde.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

ID de compte du coffre-fort de sauvegarde spécifié.

Modèle : `^[0-9]{12}$`

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

ResourceType

Type de ressource du point de récupération.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreMetadata

Ensemble de paires clé-valeur de métadonnées décrivant la configuration d'origine de la ressource sauvegardée. Ces valeurs varient en fonction du service restauré.

Type : mappage chaîne/chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetRestoreJobMetadata

Service : AWS Backup

Cette demande renvoie les métadonnées de la tâche de restauration spécifiée.

Syntaxe de la demande

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

restoreJobId

Il s'agit de l'identifiant unique d'une tâche de restauration intégrée AWS Backup.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Metadata

Cela contient les métadonnées de la tâche de sauvegarde spécifiée.

Type : mappage chaîne/chaîne

RestoreJobId

Il s'agit de l'identifiant unique d'une tâche de restauration intégrée AWS Backup.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetRestoreTestingInferredMetadata

Service : AWS Backup

Cette demande renvoie l'ensemble minimal de métadonnées requis pour démarrer une tâche de restauration avec des paramètres par défaut sécurisés. `BackupVaultName` et `RecoveryPointArn` sont des paramètres obligatoires. `BackupVaultAccountId` est un paramètre facultatif.

Syntaxe de la demande

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

ID de compte du coffre-fort de sauvegarde spécifié.

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés. Ces noms sont composés de lettres, de chiffres et de traits d'union.

Obligatoire : oui

RecoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

InferredMetadata

Il s'agit d'une carte de chaînes des métadonnées déduites de la demande.

Type : mappage chaîne/chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetRestoreTestingPlan

Service : AWS Backup

Renvoie les informations `RestoreTestingPlan` pour l'`RestoreTestingPlanName` spécifié. Les informations constituent le corps d'un plan de test de la restauration au format JSON, en plus des métadonnées.

Syntaxe de la demande

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingPlan": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
```

```
      },
      "RestoreTestingPlanArn": "string",
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

RestoreTestingPlan

Spécifie le corps d'un plan de test de la restauration. Inclut `RestoreTestingPlanName`.

Type : objet RestoreTestingPlanForGet

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetRestoreTestingSelection

Service : AWS Backup

Renvoie RestoreTestingSelection, qui affiche les ressources et les éléments du plan de test de restauration.

Syntaxe de la demande

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom unique obligatoire du plan de test de la restauration.

Obligatoire : oui

RestoreTestingSelectionName

Nom unique obligatoire de la sélection de tests de la restauration.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingSelection": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
```

```
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingPlanName": "string",
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

RestoreTestingSelection

Nom unique de la sélection de tests de la restauration.

Type : objet RestoreTestingSelectionForGet

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetSupportedResourceTypes

Service : AWS Backup

Renvoie les types de AWS ressources pris en charge par AWS Backup.

Syntaxe de la demande

```
GET /supported-resource-types HTTP/1.1
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ResourceTypes

Contient une chaîne avec les types de AWS ressources pris en charge :

- `Aurora` pour Amazon Aurora
- `CloudFormation`pour AWS CloudFormation
- `DocumentDB` pour Amazon DocumentDB (compatible avec MongoDB)
- `DynamoDB` pour Amazon DynamoDB
- `EBS` pour Amazon Elastic Block Store

- `EC2` pour Amazon Elastic Compute Cloud
- `EFS` pour Amazon Elastic File System
- `FSX` pour Amazon FSx
- `Neptune` pour Amazon Neptune
- `RDS` pour Amazon Relational Database Service
- `Redshift` pour Amazon Redshift
- `SAP HANA on Amazon EC2`pour les bases de données SAP HANA sur les instances Amazon Elastic Compute Cloud
- `S3`pour Amazon Simple Storage Service (Amazon S3)
- `Storage Gateway`pour AWS Storage Gateway
- `Timestream` pour Amazon Timestream
- `VirtualMachine`pour les machines virtuelles VMware

Type : tableau de chaînes

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++

- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListBackupJobs

Service : AWS Backup

Renvoie la liste des tâches de sauvegarde existantes pour un compte authentifié au cours des 30 derniers jours. Envisagez d'utiliser ces outils de surveillance pendant une période plus longue.

Syntaxe de la demande

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ByAccountId

L'ID du compte à partir duquel répertorier les tâches. Renvoie uniquement les tâches de sauvegarde associées à l'ID de compte spécifié.

S'il est utilisé à partir d'un compte de AWS Organizations gestion, le transfert * renvoie tous les emplois de l'organisation.

Modèle : `^[0-9]{12}$`

ByBackupVaultName

Renvoie uniquement les tâches de sauvegarde qui seront stockées dans le coffre-fort de sauvegarde spécifié. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

Renvoie uniquement les tâches de sauvegarde terminées après une date exprimée au format Unix et au format UTC (temps universel coordonné).

ByCompleteBefore

Renvoie uniquement les tâches de sauvegarde terminées avant une date exprimée au format Unix et au format UTC (temps universel coordonné).

ByCreatedAfter

Renvoie uniquement les tâches de sauvegarde créées après la date spécifiée.

ByCreatedBefore

Renvoie uniquement les tâches de sauvegarde créées avant la date spécifiée.

ByMessageCategory

Il s'agit d'un paramètre facultatif qui peut être utilisé pour filtrer les tâches MessageCategory dont la valeur correspond à la valeur que vous avez saisie.

Les exemples de chaînes peuvent inclure `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` et `InvalidParameters`.

Consultez Surveillance

Le caractère générique () renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

ByParentJobId

Il s'agit d'un filtre permettant de répertorier les tâches enfants (imbriquées) en fonction de l'ID de tâche parent.

ByResourceArn

Renvoie uniquement les tâches de sauvegarde qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

ByResourceType

Renvoie uniquement les tâches de sauvegarde pour les ressources spécifiées :

- `Aurora` pour Amazon Aurora
- `CloudFormation`pour AWS CloudFormation
- `DocumentDB` pour Amazon DocumentDB (compatible avec MongoDB)
- `DynamoDB` pour Amazon DynamoDB
- `EBS` pour Amazon Elastic Block Store
- `EC2` pour Amazon Elastic Compute Cloud
- `EFS` pour Amazon Elastic File System

- FSx pour Amazon FSx
- Neptune pour Amazon Neptune
- Redshift pour Amazon Redshift
- RDS pour Amazon Relational Database Service
- SAP HANA on Amazon EC2 pour les bases de données SAP HANA
- Storage Gatewaypour AWS Storage Gateway
- S3 pour Simple Storage Service (Amazon S3)
- Timestream pour Amazon Timestream
- VirtualMachine pour les machines virtuelles

Modèle : ^[a-zA-Z0-9\-_\.]{1,50}$

ByState

Renvoie uniquement les tâches de sauvegarde qui sont dans l'état spécifié.

Completed with issues est un statut présent uniquement dans la console AWS Backup . Pour l'API, ce statut fait référence aux tâches avec un état COMPLETED et MessageCategory avec une valeur différente de SUCCESS ; c'est-à-dire que le statut est terminé mais qu'il est accompagné d'un message de statut.

Pour obtenir le nombre de tâches pour Completed with issues, exécutez deux requêtes GET et soustrayez le deuxième plus petit nombre :

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

Valeurs valides : CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer MaxResults éléments, NextToken vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobs": [
      {
         "AccountId": "string",
         "BackupJobId": "string",
         "BackupOptions": {
            "string" : "string"
         },
         "BackupSizeInBytes": number,
         "BackupType": "string",
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "BytesTransferred": number,
         "CompletionDate": number,
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "ExpectedCompletionDate": number,
         "IamRoleArn": "string",
         "InitiationDate": number,
         "IsParent": boolean,
         "MessageCategory": "string",
         "ParentJobId": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "StartBy": number,
         "State": "string",
         "StatusMessage": "string"
```

```
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupJobs

Tableau de structures contenant des métadonnées relatives à vos tâches de sauvegarde renvoyées au format JSON.

Type : tableau d'objets BackupJob

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListBackupJobSummaries

Service : AWS Backup

Il s'agit d'une demande pour un résumé des tâches de sauvegarde créées ou en cours d'exécution au cours des 30 derniers jours. Vous pouvez inclure les paramètres AccountID, State,, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken ou pour filtrer les résultats.

Cette demande renvoie un résumé contenant la région, le compte, l'état ResourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Syntaxe de la demande

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccountId

Renvoie le nombre de tâches pour le compte spécifié.

Si la demande est envoyée depuis un compte membre ou un compte ne faisant pas partie d' AWS Organizations, les offres d'emploi enregistrées dans le compte du demandeur seront renvoyées.

Les comptes root, administrateur et administrateur délégué peuvent utiliser la valeur ANY pour renvoyer le nombre de tâches de chaque compte de l'organisation.

`AGGREGATE_ALL` agrège le nombre de tâches provenant de tous les comptes de l'organisation authentifiée, puis renvoie la somme.

Modèle : `^[0-9]{12}$`

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- `ONE_DAY`- Le nombre de tâches quotidiennes effectuées au cours des 14 jours précédents.
- `SEVEN_DAYS`- Le nombre de tâches agrégé pour les 7 jours précédents.

- `FOURTEEN_DAYS`- Le nombre de tâches agrégé pour les 14 jours précédents.

Valeurs valides : `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Le nombre maximum d'éléments à renvoyer.

La valeur est un nombre entier. La plage de valeurs acceptées est comprise entre 1 et 500.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

MessageCategory

Ce paramètre renvoie le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes acceptées incluent `AccessDenied`, `Success` et `InvalidParameters`. Voir Surveillance pour une liste des MessageCategory chaînes acceptées.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

ResourceType

Renvoie le nombre de tâches pour le type de ressource spécifié. Utilisez la demande `GetSupportedResourceTypes` pour obtenir des chaînes pour les types de ressources pris en charge.

La valeur ANY renvoie le nombre de tous les types de ressources.

`AGGREGATE_ALL` agrège le nombre de tâches pour tous les types de ressources et renvoie la somme.

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Ce paramètre renvoie le nombre de tâches pour les tâches dans l'état spécifié.

La valeur ANY renvoie le nombre de tous les états.

`AGGREGATE_ALL` agrège le nombre de tâches pour tous les états et renvoie la somme.

`Completed with issues` est un statut présent uniquement dans la console AWS Backup . Pour l'API, ce statut fait référence aux tâches avec un état `COMPLETED` et `MessageCategory` avec une valeur différente de `SUCCESS` ; c'est-à-dire que le statut est terminé mais qu'il est accompagné d'un message de statut. Pour obtenir le nombre de tâches pour `Completed with issues`, exécutez deux requêtes GET et soustrayez le deuxième plus petit nombre :

OBTENIR /audit/ ? backup-job-summaries AggregationPeriod=Quatorteen_days&state=Terminé

OBTENIR /audit/ ? backup-job-summaries AggregationPeriod=QUATORTE_DAYS& =Success&State=Terminé MessageCategory

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "BackupJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
```

```
            "ResourceType": "string",
            "StartTime": number,
            "State": "string"
        }
    ],
    "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- ONE_DAY- Le nombre de tâches quotidiennes effectuées au cours des 14 jours précédents.
- SEVEN_DAYS- Le nombre de tâches agrégé pour les 7 jours précédents.
- FOURTEEN_DAYS- Le nombre de tâches agrégé pour les 14 jours précédents.

Type : chaîne

BackupJobSummaries

Les informations récapitulatives.

Type : tableau d'objets BackupJobSummary

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListBackupPlans

Service : AWS Backup

Répertorie les plans de sauvegarde actifs pour le compte.

Syntaxe de la demande

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

IncludeDeleted

Une valeur booléenne dont la valeur par défaut est `FALSE`, qui renvoie les plans de sauvegarde supprimés lorsqu'elle est définie sur `TRUE`.

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlansList": [
      {
         "AdvancedBackupSettings": [
```

```
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlansList

Informations sur les plans de sauvegarde.

Type : tableau d'objets BackupPlansListMember

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListBackupPlanTemplates

Service : AWS Backup

Répertorie les modèles de plan de sauvegarde.

Syntaxe de la demande

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre maximum d'articles à retourner.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlanTemplatesList

Un tableau d'éléments de liste de modèles contenant des métadonnées relatives à vos modèles enregistrés.

Type : tableau d’objets BackupPlanTemplatesListMember

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListBackupPlanVersions

Service : AWS Backup

Renvoie les métadonnées de version de vos plans de sauvegarde, notamment les Amazon Resource Name (ARN), les ID des plans de sauvegarde, les dates de création et de suppression, les noms des plans et les ID de version.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupPlanVersionsList": [
      {
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupPlanVersionsList

Un tableau de versions répertorie les éléments contenant des métadonnées relatives à vos plans de sauvegarde.

Type : tableau d'objets BackupPlansListMember

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

ListBackupSelections

Service : AWS Backup

Renvoie un tableau contenant les métadonnées des ressources associées au plan de sauvegarde cible.

Syntaxe de la demande

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

Identifie de façon unique un plan de secours.

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "BackupSelectionsList": [
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupSelectionsList

Un tableau de sélection de sauvegardes répertorie les éléments contenant des métadonnées relatives à chaque ressource de la liste.

Type : tableau d'objets BackupSelectionsListMember

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListBackupVaults

Service : AWS Backup

Renvoie une liste des conteneurs de stockage de points de récupération ainsi que des informations les concernant.

Syntaxe de la demande

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ByShared

Ce paramètre triera la liste des coffres-forts par coffres-forts partagés.

ByVaultType

Ce paramètre triera la liste des coffres-forts par type de coffre-fort.

Valeurs valides : `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultList": [
      {
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "EncryptionKeyArn": "string",
         "LockDate": number,
         "Locked": boolean,
         "MaxRetentionDays": number,
         "MinRetentionDays": number,
         "NumberOfRecoveryPoints": number
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultList

Un tableau des membres du coffre-fort de sauvegarde contenant les métadonnées du coffre-fort, notamment l'Amazon Resource Name (ARN), le nom d'affichage, la date de création, le nombre de points de récupération enregistrés et les informations de chiffrement si les ressources enregistrées dans le coffre-fort de sauvegarde sont chiffrées.

Type : tableau d'objets BackupVaultListMember

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript

- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListCopyJobs

Service : AWS Backup

Renvoie les métadonnées relatives à vos tâches de copie.

Syntaxe de la demande

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ByAccountId

L'ID du compte à partir duquel répertorier les tâches. Renvoie uniquement les tâches de copie associées à l'ID de compte spécifié.

Modèle : `^[0-9]{12}$`

ByCompleteAfter

Renvoie uniquement les tâches de copie terminées après une date exprimée au format Unix et au format UTC (temps universel coordonné).

ByCompleteBefore

Renvoie uniquement les tâches de copie terminées avant une date exprimée au format Unix et au format UTC (temps universel coordonné).

ByCreatedAfter

Renvoie uniquement les tâches de copie créées après la date spécifiée.

ByCreatedBefore

Renvoie uniquement les tâches de copie créées avant la date spécifiée.

ByDestinationVaultArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde source à partir duquel copier ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

ByMessageCategory

Il s'agit d'un paramètre facultatif qui peut être utilisé pour filtrer les tâches MessageCategory dont la valeur correspond à la valeur que vous avez saisie.

Les exemples de chaînes peuvent inclure `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` et `INVALIDPARAMETERS`.

Consultez Surveillance pour obtenir la liste des chaînes acceptées.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

ByParentJobId

Il s'agit d'un filtre permettant de répertorier les tâches enfants (imbriquées) en fonction de l'ID de tâche parent.

ByResourceArn

Renvoie uniquement les tâches de copie qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

ByResourceType

Renvoie uniquement les tâches de sauvegarde pour les ressources spécifiées :

- `Aurora` pour Amazon Aurora
- `CloudFormation`pour AWS CloudFormation
- `DocumentDB` pour Amazon DocumentDB (compatible avec MongoDB)
- `DynamoDB` pour Amazon DynamoDB
- `EBS` pour Amazon Elastic Block Store
- `EC2` pour Amazon Elastic Compute Cloud
- `EFS` pour Amazon Elastic File System
- `FSx` pour Amazon FSx
- `Neptune` pour Amazon Neptune
- `Redshift` pour Amazon Redshift
- `RDS` pour Amazon Relational Database Service

- `SAP HANA on Amazon EC2` pour les bases de données SAP HANA
- `Storage Gatewaypour` AWS Storage Gateway
- `S3` pour Simple Storage Service (Amazon S3)
- `Timestream` pour Amazon Timestream
- `VirtualMachine` pour les machines virtuelles

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Renvoie uniquement les tâches de copie qui sont dans l'état spécifié.

Valeurs valides : `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer un MaxResults certain nombre d'articles, cela vous NextToken permet de renvoyer d'autres articles dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
```

```
         "ChildJobsInState": {
            "string" : number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CopyJobId": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "DestinationBackupVaultArn": "string",
         "DestinationRecoveryPointArn": "string",
         "IamRoleArn": "string",
         "IsParent": boolean,
         "MessageCategory": "string",
         "NumberOfChildJobs": number,
         "ParentJobId": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "SourceBackupVaultArn": "string",
         "SourceRecoveryPointArn": "string",
         "State": "string",
         "StatusMessage": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CopyJobs

Tableau de structures contenant des métadonnées relatives à vos tâches de copie renvoyées au format JSON.

Type : tableau d'objets CopyJob

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer un MaxResults certain nombre d'articles, cela vous NextToken permet de renvoyer d'autres articles dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

ListCopyJobSummaries

Service : AWS Backup

Cette demande obtient une liste des tâches de copie créées ou en cours d'exécution au cours des 30 derniers jours. Vous pouvez inclure les paramètres AccountID, State,, ResourceType, MessageCategory AggregationPeriod MaxResults, NextToken ou pour filtrer les résultats.

Cette demande renvoie un résumé contenant la région, le compte, l'état RestourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Syntaxe de la demande

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccountId

Renvoie le nombre de tâches pour le compte spécifié.

Si la demande est envoyée depuis un compte membre ou un compte ne faisant pas partie d' AWS Organizations, les offres d'emploi enregistrées dans le compte du demandeur seront renvoyées.

Les comptes root, administrateur et administrateur délégué peuvent utiliser la valeur ANY pour renvoyer le nombre de tâches de chaque compte de l'organisation.

`AGGREGATE_ALL` agrège le nombre de tâches provenant de tous les comptes de l'organisation authentifiée, puis renvoie la somme.

Modèle : `^[0-9]{12}$`

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- `ONE_DAY`- Le nombre de tâches quotidiennes effectuées au cours des 14 jours précédents.
- `SEVEN_DAYS`- Le nombre de tâches agrégé pour les 7 jours précédents.

- FOURTEEN_DAYS- Le nombre de tâches agrégé pour les 14 jours précédents.

Valeurs valides : ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Ce paramètre définit le nombre maximum d'éléments à renvoyer.

La valeur est un nombre entier. La plage de valeurs acceptées est comprise entre 1 et 500.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

MessageCategory

Ce paramètre renvoie le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes acceptées incluent `AccessDenied`, `Success` et `InvalidParameters`. Voir Surveillance pour une liste des MessageCategory chaînes acceptées.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

ResourceType

Renvoie le nombre de tâches pour le type de ressource spécifié. Utilisez la demande `GetSupportedResourceTypes` pour obtenir des chaînes pour les types de ressources pris en charge.

La valeur ANY renvoie le nombre de tous les types de ressources.

`AGGREGATE_ALL` agrège le nombre de tâches pour tous les types de ressources et renvoie la somme.

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Ce paramètre renvoie le nombre de tâches pour les tâches dans l'état spécifié.

La valeur ANY renvoie le nombre de tous les états.

`AGGREGATE_ALL` agrège le nombre de tâches pour tous les états et renvoie la somme.

Valeurs valides : `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "CopyJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- `ONE_DAY`- Le nombre de tâches quotidiennes effectuées au cours des 14 jours précédents.
- `SEVEN_DAYS`- Le nombre de tâches agrégé pour les 7 jours précédents.
- `FOURTEEN_DAYS`- Le nombre de tâches agrégé pour les 14 jours précédents.

Type : chaîne

CopyJobSummaries

Ce retour affiche un résumé contenant la région, le compte, l'état ResourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Type : tableau d’objets CopyJobSummary

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListFrameworks

Service : AWS Backup

Renvoie une liste de tous les frameworks pour un Compte AWS et Région AWS.

Syntaxe de la demande

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre de résultats souhaités est compris entre 1 et 1 000. Facultatif. Si ce n'est pas spécifié, la requête renverra 1 Mo de données.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
         "FrameworkName": "string",
```

```
            "NumberOfControls": number
        }
    ],
    "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Frameworks

Les frameworks avec les détails de chaque framework, y compris le nom du framework, le nom de ressource Amazon (ARN), la description, le nombre de contrôles, l'heure de création et l'état du déploiement.

Type : tableau d'objets Framework

NextToken

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListLegalHolds

Service : AWS Backup

Cette action renvoie des métadonnées concernant les mises en suspens juridiques actives et antérieures.

Syntaxe de la demande

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "LegalHolds": [
      {
         "CancellationDate": number,
         "CreationDate": number,
         "Description": "string",
         "LegalHoldArn": "string",
```

```
            "LegalHoldId": "string",
            "Status": "string",
            "Title": "string"
        }
    ],
    "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

LegalHolds

Il s'agit d'un ensemble de mises en suspens juridiques retournées, actives et antérieures.

Type : tableau d'objets LegalHold

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListProtectedResources

Service : AWS Backup

Renvoie un tableau de ressources sauvegardées avec succès AWS Backup, y compris l'heure à laquelle la ressource a été enregistrée, un Amazon Resource Name (ARN) de la ressource et un type de ressource.

Syntaxe de la demande

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
```

```
            "LastRecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string"
        }
    ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Results

Tableau de ressources sauvegardé avec succès en AWS Backup indiquant l'heure à laquelle la ressource a été enregistrée, le nom de ressource Amazon (ARN) de la ressource et un type de ressource.

Type : tableau d'objets ProtectedResource

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListProtectedResourcesByBackupVault

Service : AWS Backup

Cette demande répertorie les ressources protégées correspondant à chaque coffre-fort de sauvegarde.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

La liste des ressources protégées par coffre-fort de sauvegarde dans le ou les coffres que vous spécifiez par identifiant de compte.

Modèle : `^[0-9]{12}$`

backupVaultName

La liste des ressources protégées par coffre-fort de sauvegarde dans le ou les coffres que vous spécifiez par nom.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Results

Il s'agit des résultats renvoyés pour la demande ListProtectedResourcesByBackupVault.

Type : tableau d’objets ProtectedResource

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRecoveryPointsByBackupVault

Service : AWS Backup

Renvoie des informations détaillées sur les points de récupération stockés dans un coffre-fort de sauvegarde.

Syntaxe de la demande

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

BackupVaultAccountId

Ce paramètre triera la liste des points de récupération par ID de compte.

Modèle : `^[0-9]{12}$`

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

> **Note**
>
> Le nom du coffre-fort de sauvegarde peut ne pas être disponible lorsqu'un service pris en charge crée la sauvegarde.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

ByBackupPlanId

Renvoie uniquement les points de récupération correspondant à l'ID du plan de sauvegarde spécifié.

ByCreatedAfter

Renvoie uniquement les points de récupération créés après l'horodatage spécifié.

ByCreatedBefore

Renvoie uniquement les points de récupération créés après l'horodatage spécifié.

ByParentRecoveryPointArn

Cela renvoie uniquement les points de récupération qui correspondent au point de récupération parent (composite) spécifié (Amazon Resource Name (ARN).

ByResourceArn

Renvoie uniquement les points de récupération qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

ByResourceType

Renvoie uniquement les points de récupération qui correspondent au(x) type(s) de ressources spécifié(s) :

- `Aurora` pour Amazon Aurora
- `CloudFormation`pour AWS CloudFormation
- `DocumentDB` pour Amazon DocumentDB (compatible avec MongoDB)
- `DynamoDB` pour Amazon DynamoDB
- `EBS` pour Amazon Elastic Block Store
- `EC2` pour Amazon Elastic Compute Cloud
- `EFS` pour Amazon Elastic File System
- `FSx` pour Amazon FSx
- `Neptune` pour Amazon Neptune
- `Redshift` pour Amazon Redshift
- `RDS` pour Amazon Relational Database Service
- `SAP HANA on Amazon EC2` pour les bases de données SAP HANA
- `Storage Gateway`pour AWS Storage Gateway
- `S3` pour Simple Storage Service (Amazon S3)
- `Timestream` pour Amazon Timestream

- `VirtualMachine` pour les machines virtuelles

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeInBytes": number,
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CalculatedLifecycle": {
            "DeleteAt": number,
            "MoveToColdStorageAt": number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
```

```
            "CreationDate": number,
            "EncryptionKeyArn": "string",
            "IamRoleArn": "string",
            "IsEncrypted": boolean,
            "IsParent": boolean,
            "LastRestoreTime": number,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "ParentRecoveryPointArn": "string",
            "RecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string",
            "SourceBackupVaultArn": "string",
            "Status": "string",
            "StatusMessage": "string",
            "VaultType": "string"
         }
      ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

RecoveryPoints

Ensemble d'objets contenant des informations détaillées sur les points de récupération enregistrés dans un coffre-fort de sauvegarde.

Type : tableau d'objets RecoveryPointByBackupVault

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

ListRecoveryPointsByLegalHold

Service : AWS Backup

Cette action renvoie les ARN du point de récupération (Amazon Resource Names) correspondant à la mise en suspens juridique spécifiée.

Syntaxe de la demande

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

legalHoldId

L'identifiant de la retenue légale.

Obligatoire : oui

MaxResults

Le nombre maximum d'éléments de la liste de ressources à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées.

Type : chaîne

RecoveryPoints

Les points de récupération.

Type : tableau d'objets RecoveryPointMember

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRecoveryPointsByResource

Service : AWS Backup

Les informations sur les points de récupération du type spécifié par le nom de ressource Amazon (ARN) d'une ressource.

> **Note**
>
> Pour Amazon EFS et Amazon EC2, cette action répertorie uniquement les points de récupération créés par AWS Backup.

Syntaxe de la demande

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ManagedByAWSBackupOnly

Cet attribut filtre les points de récupération en fonction de leur propriétaire.

Si ce paramètre est défini sur`TRUE`, la réponse contiendra les points de récupération associés aux ressources sélectionnées gérées par AWS Backup.

Si ce paramètre est défini sur`FALSE`, la réponse contiendra tous les points de récupération associés à la ressource sélectionnée.

Type : booléen

MaxResults

Le nombre maximum d'éléments à renvoyer.

> **Note**
>
> Amazon RDS nécessite une valeur d'au moins 20.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

resourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeBytes": number,
         "BackupVaultName": "string",
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IsParent": boolean,
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceName": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

RecoveryPoints

Tableau d'objets contenant des informations détaillées sur les points de récupération du type de ressource spécifié.

> **Note**
>
> Seuls les points de récupération Amazon EFS et Amazon EC2 sont renvoyés.
> BackupVaultName

Type : tableau d’objets RecoveryPointByResource

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListReportJobs

Service : AWS Backup

Renvoie des informations sur vos tâches de rapport.

Syntaxe de la demande

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ByCreationAfter

Renvoie uniquement les tâches de rapport créées après la date et l'heure spécifiées au format Unix et au format UTC (temps universel coordonné). Par exemple, la valeur 1516925490 représente le vendredi 26 janvier 2018 à 00 h 11 m 30 s.

ByCreationBefore

Renvoie uniquement les tâches de rapport créées avant la date et l'heure spécifiées au format Unix et au format UTC (temps universel coordonné). Par exemple, la valeur 1516925490 représente le vendredi 26 janvier 2018 à 00 h 11 m 30 s.

ByReportPlanName

Renvoie uniquement les tâches de rapport portant le nom du plan de rapport spécifié.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

Renvoie uniquement les tâches de rapport qui sont dans le statut spécifié. Les statuts sont les suivants :

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

Le nombre de résultats souhaités est compris entre 1 et 1 000. Facultatif. Si ce n'est pas spécifié, la requête renverra 1 Mo de données.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportJobs": [
      {
         "CompletionTime": number,
         "CreationTime": number,
         "ReportDestination": {
            "S3BucketName": "string",
            "S3Keys": [ "string" ]
         },
         "ReportJobId": "string",
         "ReportPlanArn": "string",
         "ReportTemplate": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Type : chaîne

ReportJobs

Détails de vos tâches de rapports au format JSON.

Type : tableau d’objets ReportJob

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListReportPlans

Service : AWS Backup

Renvoie une liste de vos plans de rapport. Pour obtenir des informations détaillées sur un plan de rapport unique, utilisez `DescribeReportPlan`.

Syntaxe de la demande

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre de résultats souhaités est compris entre 1 et 1 000. Facultatif. Si ce n'est pas spécifié, la requête renverra 1 Mo de données.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportPlans": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
```

```
         "LastAttemptedExecutionTime": number,
         "LastSuccessfulExecutionTime": number,
         "ReportDeliveryChannel": {
            "Formats": [ "string" ],
            "S3BucketName": "string",
            "S3KeyPrefix": "string"
         },
         "ReportPlanArn": "string",
         "ReportPlanDescription": "string",
         "ReportPlanName": "string",
         "ReportSetting": {
            "Accounts": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "ReportTemplate": "string"
         }
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

Identifiant renvoyé lors de l'appel précédent cette opération, qui peut être utilisé pour renvoyer le prochain ensemble d'éléments de la liste.

Type : chaîne

ReportPlans

Le rapport planifie avec des informations détaillées pour chaque plan. Ces informations incluent l'Amazon Resource Name (ARN), le nom du plan de rapport, la description, les paramètres, le canal de livraison, le statut du déploiement, l'heure de création et les dernières tentatives d'exécution du plan de rapport ainsi que celles ayant réussi.

Type : tableau d'objets ReportPlan

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRestoreJobs

Service : AWS Backup

Renvoie la liste des tâches AWS Backup initiées pour restaurer une ressource enregistrée, y compris des détails sur le processus de restauration.

Syntaxe de la demande

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ByAccountId

L'ID du compte à partir duquel répertorier les tâches. Renvoie uniquement les tâches de restauration associées à l'ID de compte spécifié.

Modèle : `^[0-9]{12}$`

ByCompleteAfter

Renvoie uniquement les tâches de copie terminées après une date exprimée au format Unix et au format UTC (temps universel coordonné).

ByCompleteBefore

Renvoie uniquement les tâches de copie terminées avant une date exprimée au format Unix et au format UTC (temps universel coordonné).

ByCreatedAfter

Renvoie uniquement les tâches de restauration créées après la date spécifiée.

ByCreatedBefore

Renvoie uniquement les tâches de restauration créées avant la date spécifiée.

ByResourceType

Incluez ce paramètre pour renvoyer uniquement les tâches de restauration pour les ressources spécifiées :

- `Aurora` pour Amazon Aurora

- `CloudFormation`pour AWS CloudFormation
- `DocumentDB` pour Amazon DocumentDB (compatible avec MongoDB)
- `DynamoDB` pour Amazon DynamoDB
- `EBS` pour Amazon Elastic Block Store
- `EC2` pour Amazon Elastic Compute Cloud
- `EFS` pour Amazon Elastic File System
- `FSx` pour Amazon FSx
- `Neptune` pour Amazon Neptune
- `Redshift` pour Amazon Redshift
- `RDS` pour Amazon Relational Database Service
- `SAP HANA on Amazon EC2` pour les bases de données SAP HANA
- `Storage Gateway`pour AWS Storage Gateway
- `S3` pour Simple Storage Service (Amazon S3)
- `Timestream` pour Amazon Timestream
- `VirtualMachine` pour les machines virtuelles

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByRestoreTestingPlanArn

Cela renvoie uniquement les tâches de test de la restauration qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

ByStatus

Renvoie uniquement les tâches de restauration associées au statut de tâche spécifié.

Valeurs valides : `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

RestoreJobs

Tableau d'objets contenant des informations détaillées sur les tâches de restauration des ressources enregistrées.

Type : tableau d’objets RestoreJobsListMember

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRestoreJobsByProtectedResource

Service : AWS Backup

Cela renvoie les tâches de restauration contenant la ressource protégée spécifiée.

Vous devez inclure `ResourceArn`. Vous pouvez éventuellement inclure `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` et `ByRecoveryPointCreationDateBefore`.

Syntaxe de la demande

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

ByRecoveryPointCreationDateAfter

Renvoie uniquement les tâches de restauration des points de récupération créées après la date spécifiée.

ByRecoveryPointCreationDateBefore

Renvoie uniquement les tâches de restauration des points de récupération créées avant la date spécifiée.

ByStatus

Renvoie uniquement les tâches de restauration associées au statut de tâche spécifié.

Valeurs valides : `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d’autres éléments dans votre liste en commençant par l’emplacement indiqué par le jeton suivant.

resourceArn

Renvoie uniquement les tâches de restauration qui correspondent à l'Amazon Resource Name (ARN) des ressources spécifié.

Obligatoire : oui

Corps de la demande

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
```

```
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d’autres éléments dans votre liste en commençant par l’emplacement indiqué par le jeton suivant.

Type : chaîne

RestoreJobs

Tableau d’objets contenant des informations détaillées sur les tâches de restauration des ressources enregistrées.

Type : tableau d’objets RestoreJobsListMember

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRestoreJobSummaries

Service : AWS Backup

Cette demande obtient un résumé des tâches de restauration créées ou en cours d'exécution au cours des 30 derniers jours. Vous pouvez inclure les paramètres AccountID, State,, ResourceType AggregationPeriod MaxResults, NextToken ou pour filtrer les résultats.

Cette demande renvoie un résumé contenant la région, le compte, l'état RestourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Syntaxe de la demande

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

AccountId

Renvoie le nombre de tâches pour le compte spécifié.

Si la demande est envoyée depuis un compte membre ou un compte ne faisant pas partie d' AWS Organizations, les offres d'emploi enregistrées dans le compte du demandeur seront renvoyées.

Les comptes root, administrateur et administrateur délégué peuvent utiliser la valeur ANY pour renvoyer le nombre de tâches de chaque compte de l'organisation.

`AGGREGATE_ALL` agrège le nombre de tâches provenant de tous les comptes de l'organisation authentifiée, puis renvoie la somme.

Modèle : `^[0-9]{12}$`

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- `ONE_DAY`- Le nombre de tâches quotidiennes des 14 jours précédents.
- `SEVEN_DAYS`- Le nombre de tâches agrégé pour les 7 jours précédents.
- `FOURTEEN_DAYS`- Le nombre de tâches agrégé pour les 14 jours précédents.

Valeurs valides : `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Ce paramètre définit le nombre maximum d'éléments à renvoyer.

La valeur est un nombre entier. La plage de valeurs acceptées est comprise entre 1 et 500.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

ResourceType

Renvoie le nombre de tâches pour le type de ressource spécifié. Utilisez la demande `GetSupportedResourceTypes` pour obtenir des chaînes pour les types de ressources pris en charge.

La valeur ANY renvoie le nombre de tous les types de ressources.

`AGGREGATE_ALL` agrège le nombre de tâches pour tous les types de ressources et renvoie la somme.

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Ce paramètre renvoie le nombre de tâches pour les tâches dans l'état spécifié.

La valeur ANY renvoie le nombre de tous les états.

`AGGREGATE_ALL` agrège le nombre de tâches pour tous les états et renvoie la somme.

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Corps de la requête

La demande n'a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "NextToken": "string",
   "RestoreJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AggregationPeriod

Période pendant laquelle les résultats sont renvoyés.

- `ONE_DAY`- Le nombre de tâches quotidiennes des 14 jours précédents.
- `SEVEN_DAYS`- Le nombre de tâches agrégé pour les 7 jours précédents.
- `FOURTEEN_DAYS`- Le nombre de tâches agrégé pour les 14 jours précédents.

Type : chaîne

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

RestoreJobSummaries

Ce retour contient un résumé qui contient la région, le compte, l'état ResourceType, MessageCategory, StartTime, EndTime, et le nombre de tâches incluses.

Type : tableau d'objets RestoreJobSummary

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRestoreTestingPlans

Service : AWS Backup

Renvoie une liste de plans de test de la restauration.

Syntaxe de la demande

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d’autres éléments dans votre liste en commençant par l’emplacement indiqué par le jeton suivant.

Corps de la requête

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreTestingPlans": [
      {
         "CreationTime": number,
         "LastExecutionTime": number,
         "LastUpdateTime": number,
         "RestoreTestingPlanArn": "string",
```

```
            "RestoreTestingPlanName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowHours": number
        }
    ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

RestoreTestingPlans

Il s'agit d'une liste renvoyée de plans de test de la restauration.

Type : tableau d'objets RestoreTestingPlanForList

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListRestoreTestingSelections

Service : AWS Backup

Renvoie une liste de sélections de tests de la restauration. Peut être filtrée par `MaxResults` et `RestoreTestingPlanName`.

Syntaxe de la demande

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d’autres éléments dans votre liste en commençant par l’emplacement indiqué par le jeton suivant.

RestoreTestingPlanName

Renvoie les sélections de tests de la restauration en fonction du nom du plan de tests de la restauration spécifié.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

RestoreTestingSelections

Les sélections de tests de la restauration renvoyées associées au plan de test de la restauration.

Type : tableau d'objets RestoreTestingSelectionForList

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListTags

Service : AWS Backup

Renvoie les balises attribuées à la ressource, telles qu'un point de restauration cible, un plan de sauvegarde ou un coffre de sauvegarde.

`ListTags` ne fonctionne que pour les types de ressources qui prennent en charge la gestion complète d' AWS Backup de leurs sauvegardes. Ces types de ressources sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource.

Syntaxe de la demande

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

MaxResults

Le nombre maximum d'éléments à renvoyer.

Plage valide : valeur minimum de 1. La valeur maximale est 1 000.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

resourceArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource. Les cibles valides pour `ListTags` sont les points de récupération, les plans de sauvegarde et les coffres-forts de sauvegarde.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des éléments renvoyés. Par exemple, si une demande est faite pour renvoyer `MaxResults` éléments, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Tags

Informations sur les tags.

Type : mappage chaîne/chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutBackupVaultAccessPolicy

Service : AWS Backup

Définit une politique basée sur les ressources qui est utilisée pour gérer les autorisations d'accès au coffre-fort de sauvegarde sur la cible. Nécessite un nom de coffre-fort de sauvegarde et un document de stratégie d'accès au format JSON.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Policy

Document de stratégie d'accès au coffre-fort de sauvegarde au format JSON.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutBackupVaultLockConfiguration

Service : AWS Backup

Applique AWS Backup Vault Lock à un coffre-fort de sauvegarde, empêchant ainsi les tentatives de suppression de tout point de récupération stocké ou créé dans un coffre-fort de sauvegarde. Vault Lock empêche également les tentatives de mise à jour de la politique de cycle de vie qui contrôle la période de rétention de tout point de récupération actuellement stocké dans un coffre-fort de sauvegarde. Si cela est spécifié, Vault Lock applique une période de rétention minimale et maximale pour les futures tâches de sauvegarde et de copie ciblant un coffre-fort de sauvegarde.

> **Note**
>
> AWS Backup Vault Lock a été évalué par Cohasset Associates pour une utilisation dans des environnements soumis aux réglementations SEC 17a-4, CFTC et FINRA. Pour plus d'informations sur le lien entre AWS Backup Vault Lock et ces réglementations, consultez l'évaluation de conformité de Cohasset Associates.

Pour plus d'informations, consultez la page AWS Backup Vault Lock.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

La configuration AWS Backup Vault Lock qui indique le nom du coffre de sauvegarde qu'il protège.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

ChangeableForDays

La configuration AWS Backup Vault Lock qui indique le nombre de jours avant la date de verrouillage. Par exemple, définir `ChangeableForDays` sur 30 le 1er janvier 2022 à 20 h UTC fixera la date de verrouillage au 31 janvier 2022 à 20 h UTC.

AWS Backup impose une période de réflexion de 72 heures avant que Vault Lock n'entre en vigueur et ne devienne immuable. Vous devez donc définir `ChangeableForDays` sur 3 ou plus.

Avant la date de verrouillage, vous pouvez supprimer le verrouillage du coffre-fort à l'aide de `DeleteBackupVaultLockConfiguration` ou modifier la configuration du verrouillage du coffre-fort en utilisant `PutBackupVaultLockConfiguration`. À compter de la date de verrouillage, le verrouillage du coffre-fort devient immuable et ne peut être ni modifié ni supprimé.

Si ce paramètre n'est pas spécifié, vous pouvez supprimer le verrouillage du coffre-fort à l'aide de `DeleteBackupVaultLockConfiguration` ou modifier la configuration du verrouillage du coffre-fort en utilisant `PutBackupVaultLockConfiguration` à tout moment.

Type : long

Obligatoire : non

MaxRetentionDays

La configuration AWS Backup Vault Lock qui spécifie la période de rétention maximale pendant laquelle le coffre-fort conserve ses points de restauration. Ce paramètre peut être utile si, par exemple, les politiques de votre organisation vous obligent à détruire certaines données après les avoir conservées pendant quatre ans (1 460 jours).

Si ce paramètre n'est pas inclus, le verrouillage du coffre-fort n'applique pas de période de conservation maximale sur les points de récupération dans le coffre-fort. Si ce paramètre est inclus sans valeur, le verrouillage du coffre-fort n'appliquera pas de période de conservation maximale.

Si ce paramètre est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de conservation égale ou inférieure à la période

de conservation maximale. Si la période de conservation de la tâche est plus longue que cette période de conservation maximale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. La période de rétention maximale la plus longue que vous puissiez spécifier est de 36 500 jours (environ 100 ans). Les points de récupération déjà enregistrés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

Obligatoire : non

MinRetentionDays

La configuration AWS Backup Vault Lock qui spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de restauration. Ce paramètre peut être utile si, par exemple, les politiques de votre organisation vous obligent à conserver certaines données pendant au moins sept ans (2 555 jours).

Ce paramètre est obligatoire lors de la création d'un verrou de coffre-fort AWS CloudFormation ; dans le cas contraire, ce paramètre est facultatif. Si ce paramètre n'est pas spécifié, le verrouillage du coffre-fort n'appliquera pas de période de conservation minimale.

Si ce paramètre est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de conservation égale ou supérieure à la période de conservation minimale. Si la période de conservation de la tâche est plus courte que cette période de conservation minimale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. La période de rétention minimale la plus courte que vous puissiez spécifier est d'un jour. Les points de récupération déjà enregistrés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++

- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutBackupVaultNotifications

Service : AWS Backup

Active les notifications sur un coffre-fort de sauvegarde pour la rubrique et les événements spécifiés.

Syntaxe de la demande

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupVaultEvents

Tableau d'événements qui indiquent le statut des tâches de sauvegarde des ressources dans le coffre-fort de sauvegarde.

Pour les cas d'utilisation courants et les exemples de code, consultez la section Utilisation d'Amazon SNS pour suivre AWS Backup les événements.

Les événements suivants sont pris en charge :

- `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED`
- `COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED`
- `RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RECOVERY_POINT_MODIFIED`
- `S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED`

> **Note**
>
> La liste ci-dessous inclut à la fois les événements pris en charge et les événements obsolètes qui ne sont plus utilisés (à titre de référence). Les événements déconseillés ne renvoient ni statuts ni notifications. Reportez-vous à la liste ci-dessus pour connaître les événements pris en charge.

Type : tableau de chaînes

Valeurs valides : `BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED`

Obligatoire : oui

SNSTopicArn

L'Amazon Resource Name (ARN) qui spécifie la rubrique des événements d'un coffre-fort de secours ; par exemple, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Type : chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2

- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutRestoreValidationResult

Service : AWS Backup

Cette demande vous permet d'envoyer les résultats de validation de votre test de la restauration autonome indépendant. `RestoreJobId` et `ValidationStatus` sont obligatoires. Vous pouvez éventuellement saisir un `ValidationStatusMessage`.

Syntaxe de la demande

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

restoreJobId

Il s'agit de l'identifiant unique d'une tâche de restauration intégrée AWS Backup.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

ValidationStatus

État de la validation de votre restauration.

Type : chaîne

Valeurs valides : `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Obligatoire : oui

ValidationStatusMessage

Il s’agit d’une chaîne de message facultative que vous pouvez saisir pour décrire le statut de validation du test de la restauration.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 204
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

StartBackupJob

Service : AWS Backup

Démarre une tâche de sauvegarde à la demande pour la ressource spécifiée.

Syntaxe de la demande

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
   "BackupOptions": {
      "string" : "string"
   },
   "BackupVaultName": "string",
   "CompleteWindowMinutes": number,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointTags": {
      "string" : "string"
   },
   "ResourceArn": "string",
   "StartWindowMinutes": number
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupOptions

L'option de sauvegarde pour une ressource sélectionnée. Cette option est uniquement disponible pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Valeurs valides : définissez sur `"WindowsVSS":"enabled"` pour activer l'option de sauvegarde `WindowsVSS` et créer une sauvegarde Windows VSS. Définissez sur `"WindowsVSS""disabled"` pour créer une sauvegarde régulière. L'option `WindowsVSS` n'est pas activée par défaut.

Type : mappage chaîne/chaîne

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

CompleteWindowMinutes

Valeur en minutes pendant laquelle une sauvegarde démarrée avec succès doit se terminer, faute de quoi AWS Backup annule la tâche. Cette valeur est facultative. Cette valeur commence le compte à rebours à partir du moment auquel la sauvegarde a été planifiée. Cela n'ajoute pas de temps supplémentaire pour `StartWindowMinutes`, ni si la sauvegarde a démarré plus tard que prévu.

Comme `StartWindowMinutes`, ce paramètre a une valeur maximale de 100 ans (52 560 000 minutes).

Type : long

Obligatoire : non

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : oui

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartBackupJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup fera automatiquement la transition et expirera les sauvegardes en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Ce paramètre a une valeur maximale de 100 ans (36 500 jours).

Type : objet Lifecycle

Obligatoire : non

RecoveryPointTags

Les balises à attribuer aux ressources.

Type : mappage chaîne/chaîne

Obligatoire : non

ResourceArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : oui

StartWindowMinutes

Valeur en minutes après la planification d'une sauvegarde avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative et elle est de 8 heures par défaut. Si cette valeur est incluse, elle doit être d'au moins 60 minutes pour éviter les erreurs.

Ce paramètre a une valeur maximale de 100 ans (52 560 000 minutes).

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste `CREATED` jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à`RUNNING`) ou jusqu'à ce que le statut de la tâche passe à `EXPIRED` (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Type : long

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Type : chaîne

CreationDate

Date et heure de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

IsParent

Il s'agit d'une valeur booléenne renvoyée indiquant qu'il s'agit d'une tâche de sauvegarde parent (composite).

Type : booléen

RecoveryPointArn

Remarque : ce champ n'est renvoyé que pour les ressources Amazon EFS et Advanced DynamoDB.

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

StartCopyJob

Service : AWS Backup

Démarre une tâche pour créer une copie unique de la ressource spécifiée.

Ne prend pas en charge les sauvegardes continues.

Syntaxe de la demande

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
   "DestinationBackupVaultArn": "string",
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string",
   "SourceBackupVaultName": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

DestinationBackupVaultArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de destination sur lequel effectuer la copie ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : oui

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour copier le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : oui

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartCopyJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Lifecycle

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et`DeleteAfterDays`.

Type : objet Lifecycle

Obligatoire : non

RecoveryPointArn

Un ARN qui identifie de manière unique un point de récupération à utiliser pour la tâche de copie ; par exemple, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Type : chaîne

Obligatoire : oui

SourceBackupVaultName

Le nom d'un conteneur source logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms propres au compte utilisé pour les créer et à la AWS région dans laquelle ils ont été créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CopyJobId

Identifie de manière unique une tâche de copie.

Type : chaîne

CreationDate

Date et heure de création d'une tâche de copie, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

IsParent

Il s'agit d'une valeur booléenne renvoyée indiquant qu'il s'agit d'une tâche de copie parent (composite).

Type : booléen

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

StartReportJob

Service : AWS Backup

Démarre une tâche de rapport à la demande pour le plan de rapport spécifié.

Syntaxe de la demande

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportPlanName

Le nom unique d'un plan de rapport.

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartReportJobInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ReportJobId

Identifiant de la tâche de rapport. Une chaîne codée en Unicode, UTF-8 unique et générée de façon aléatoire qui contiennent au maximum 1 024 octets. L'ID de tâche de rapport ne peut pas être modifié.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

StartRestoreJob

Service : AWS Backup

Récupère la ressource enregistrée identifiée par un Amazon Resource Name (ARN).

Syntaxe de la demande

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

CopySourceTagsToRestoredResource

Ce paramètre est facultatif. S'il est égal à `True`, les balises incluses dans la sauvegarde seront copiées sur la ressource restaurée.

Cela ne peut être appliqué qu'aux sauvegardes créées via AWS Backup.

Type : booléen

Obligatoire : non

IamRoleArn

Le nom de ressource Amazon (ARN) du rôle IAM AWS Backup utilisé pour créer la ressource cible ; par exemple :`arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `StartRestoreJob`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Metadata

Un ensemble de paires clé-valeur de métadonnées.

Vous pouvez obtenir les métadonnées de configuration relatives à une ressource au moment de sa sauvegarde en appelant `GetRecoveryPointRestoreMetadata`. Cependant, des valeurs autres que celles fournies par `GetRecoveryPointRestoreMetadata` peuvent être nécessaires pour restaurer une ressource. Par exemple, vous devrez peut-être fournir un nouveau nom de ressource si l'original existe déjà.

Pour plus d'informations sur les métadonnées de chaque ressource, consultez les rubriques suivantes :

- Métadonnées pour Amazon Aurora
- Métadonnées pour Amazon DocumentDB
- Métadonnées pour AWS CloudFormation
- Métadonnées pour Amazon DynamoDB
- Métadonnées pour Amazon EBS
- Métadonnées pour Amazon EC2
- Métadonnées pour Amazon EFS
- Métadonnées pour Amazon FSx
- Métadonnées pour Amazon Neptune
- Métadonnées pour Amazon RDS
- Métadonnées pour Amazon Redshift
- Métadonnées pour AWS Storage Gateway

- Métadonnées pour Amazon S3
- Métadonnées pour Amazon Timestream
- Métadonnées pour les machines virtuelles

Type : mappage chaîne/chaîne

Obligatoire : oui

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : oui

ResourceType

Démarre une tâche visant à restaurer un point de récupération pour l'une des ressources suivantes :

- `Aurora`- Amazon Aurora
- `DocumentDB`- Amazon DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`- Amazon DynamoDB
- `EBS`- Boutique Amazon Elastic Block
- `EC2`- Amazon Elastic Compute Cloud
- `EFS`- Amazon Elastic File System
- `FSx`- Amazon FSx
- `Neptune`- Amazon Neptune
- `RDS`- Amazon Relational Database Service
- `Redshift`- Amazon Redshift
- `Storage Gateway` - AWS Storage Gateway
- `S3`- Amazon Simple Storage Service
- `Timestream`- Amazon Timestream
- `VirtualMachine`- Machines virtuelles

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

RestoreJobId

Identifie de manière unique la tâche qui restaure un point de récupération.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

StopBackupJob

Service : AWS Backup

Tente d'annuler une tâche afin de créer une sauvegarde unique d'une ressource.

Cette action n'est pas prise en charge pour les services suivants : Amazon FSx pour Windows File Server, Amazon FSx pour Lustre, Amazon FSx pour NetApp ONTAP, Amazon FSx pour OpenZFS, Amazon DocumentDB (compatible avec MongoDB), Amazon RDS, Amazon Aurora et Amazon Neptune.

Syntaxe de la demande

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Obligatoire : oui

Corps de la demande

La demande n’a pas de corps de requête.

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

TagResource

Service : AWS Backup

Attribue un ensemble de paires clé-valeur à un point de récupération, à un plan de sauvegarde ou à un coffre-fort de sauvegarde identifié par un Amazon Resource Name (ARN).

Cette API est prise en charge pour les points de récupération pour les types de ressources tels qu'Aurora et Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune et Amazon RDS.

Syntaxe de la demande

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

resourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource balisée.

Les ARN non inclus `backup` sont incompatibles avec le balisage. `TagResource`et `UntagResource` avec des ARN non valides, une erreur se produira. Le contenu ARN acceptable peut inclure`arn:aws:backup:us-east`. Un contenu ARN non valide peut ressembler à`arn:aws:ec2:us-east`.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Tags

Des paires clé-valeur utilisées pour vous aider à organiser vos ressources. Vous pouvez attribuer vos propres métadonnées aux ressources que vous créez. Pour plus de clarté, voici la structure pour attribuer des balises : `[{"Key":"string","Value":"string"}]`.

Type : mappage chaîne/chaîne

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UntagResource

Service : AWS Backup

Supprime un ensemble de paires clé-valeur d'un point de récupération, d'un plan de sauvegarde ou d'un coffre-fort de sauvegarde identifié par un Amazon Resource Name (ARN)

Cette API n'est pas prise en charge pour les points de récupération pour les types de ressources tels qu'Aurora et Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune et Amazon RDS.

Syntaxe de la demande

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

resourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource balisée.

Les ARN non inclus `backup` sont incompatibles avec le balisage. `TagResource`et si `UntagResource` les ARN ne sont pas valides, une erreur se produira. Le contenu ARN acceptable peut inclure`arn:aws:backup:us-east`. Un contenu ARN non valide peut ressembler à`arn:aws:ec2:us-east`.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

TagKeyList

Les clés permettant d'identifier les balises clé-valeur à supprimer d'une ressource.

Type : tableau de chaînes

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d'état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateBackupPlan

Service : AWS Backup

Met à jour le plan de sauvegarde spécifié. La nouvelle version est identifiée de manière unique par son identifiant.

Syntaxe de la demande

```
POST /backup/plans/backupPlanId HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
```

```
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupPlanId

L'ID du plan de sauvegarde.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

BackupPlan

Le corps d'un plan de secours. Comprend un `BackupPlanName` et un ou plusieurs ensembles de `Rules`.

Type : objet BackupPlanInput

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
```

```
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "CreationDate": number,
      "VersionId": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

AdvancedBackupSettings

Contient une liste d'`BackupOptions` pour chaque type de ressource.

Type : tableau d'objets AdvancedBackupSetting

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

CreationDate

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Les ID de version ne peuvent pas être modifiés.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateFramework

Service : AWS Backup

Met à jour le framework spécifié.

Syntaxe de la demande

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "IdempotencyToken": "string"
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

frameworkName

Le nom unique d'un cadre. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

FrameworkControls

Les contrôles qui constituent le cadre. Chaque contrôle de la liste possède un nom, des paramètres d'entrée et une portée.

Type : tableau d'objets FrameworkControl

Obligatoire : non

FrameworkDescription

Une description facultative du cadre avec 1 024 caractères au maximum.

Type : chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `UpdateFrameworkInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'un framework, dans une représentation ISO 8601. La valeur de `CreationTime` est précise en millisecondes. Par exemple, 2020-07-10T15:00:00.000-08:00 représente le 10 juillet 2020 à 15 h 00 avec 8 heures de retard sur le temps UTC.

Type : Timestamp

FrameworkArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

FrameworkName

Le nom unique d'un cadre. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AlreadyExistsException

La ressource demandée existe déjà.

Code d’état HTTP : 400

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

LimitExceededException

Une limite de la demande a été dépassée ; par exemple, le nombre maximum d'éléments autorisés dans une demande.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateGlobalSettings

Service : AWS Backup

Indique si le AWS compte est activé pour la sauvegarde entre comptes. Renvoie une erreur si le compte n'est pas un compte de gestion Organizations. Utilisez l'API `DescribeGlobalSettings` pour déterminer les paramètres actuels.

Syntaxe de la demande

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

Paramètres de demande URI

La demande n’utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

GlobalSettings

Une valeur pour `isCrossAccountBackupEnabled` et une région. Exemple: `update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Type : mappage chaîne/chaîne

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2

- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateRecoveryPointLifecycle

Service : AWS Backup

Définit le cycle de vie de transition d'un point de récupération.

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Cette opération ne prend pas en charge les sauvegardes continues.

Syntaxe de la demande

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

backupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

recoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Type : objet Lifecycle

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BackupVaultArn

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

CalculatedLifecycle

Un objet `CalculatedLifecycle` contenant des horodatages `DeleteAt` et `MoveToColdStorageAt`.

Type : objet CalculatedLifecycle

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur

de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet Lifecycle

RecoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

InvalidRequestException

Indique une erreur dans la saisie de la demande. Par exemple, un paramètre n'est pas du bon type.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateRegionSettings

Service : AWS Backup

Met à jour les paramètres actuels d'activation du service pour la région.

Utilisez l'API `DescribeRegionSettings` pour déterminer les types de ressources pris en charge.

Syntaxe de la demande

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Paramètres de demande URI

La demande n'utilise pas de paramètres URI.

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

ResourceTypeManagementPreference

Active ou désactive AWS Backup la gestion complète des sauvegardes pour un type de ressource. Pour activer AWS Backup la gestion complète de DynamoDB ainsi que les fonctionnalités avancées AWS Backup de sauvegarde DynamoDB, suivez la procédure pour activer la sauvegarde DynamoDB avancée par programmation.

Type : chaîne vers un mappage booléen

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

ResourceTypeOptInPreference

Met à jour la liste des services ainsi que les préférences d'activation pour la région.

Si les attributions de ressources sont uniquement basées sur des balises, les paramètres d'acceptation du service sont appliqués. Si un type de ressource est explicitement attribué à un plan de sauvegarde, tel qu'Amazon S3, Amazon EC2 ou Amazon RDS, il sera inclus dans la sauvegarde même s'il n'est pas activé pour ce service en particulier. Si un type de ressource et des balises sont spécifiés dans une attribution de ressource, le type de ressource spécifié dans le plan de sauvegarde est prioritaire par rapport à la condition de balise. Les paramètres d'activation du service ne sont pas pris en compte dans ce cas.

Type : chaîne vers un mappage booléen

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d'état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d'état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateReportPlan

Service : AWS Backup

Met à jour le plan de rapport spécifié.

Syntaxe de la demande

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

reportPlanName

Le nom unique du plan de rapport. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

IdempotencyToken

Chaîne choisie par le client que vous pouvez utiliser pour faire la distinction entre des appels par ailleurs identiques à `UpdateReportPlanInput`. Toute nouvelle tentative d'une demande réussie avec le même jeton d'idempotence entraîne un message de réussite sans qu'aucune action ne soit entreprise.

Type : chaîne

Obligatoire : non

ReportDeliveryChannel

Les informations sur l'endroit où envoyer vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Type : objet ReportDeliveryChannel

Obligatoire : non

ReportPlanDescription

Une description facultative du plan de rapport avec 1 024 caractères au maximum.

Type : chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

ReportSetting

Modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Si le modèle de rapport est `RESOURCE_COMPLIANCE_REPORT` ou`CONTROL_COMPLIANCE_REPORT`, cette ressource d'API décrit également la couverture du rapport par Régions AWS et les frameworks.

Type : objet ReportSetting

Obligatoire : non

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Date et heure de création d'un plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

ReportPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

ReportPlanName

Le nom unique du plan de rapport.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateRestoreTestingPlan

Service : AWS Backup

Cette demande enverra des modifications au plan de test de la restauration que vous avez spécifié. `RestoreTestingPlanName` ne peut pas être mis à jour après sa création.

`RecoveryPointSelection` peut contenir :

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Syntaxe de la demande

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Nom du plan de test de restauration.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

RestoreTestingPlan

Spécifie le corps d'un plan de test de la restauration.

Type : objet RestoreTestingPlanForUpdate

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle le plan de test des ressources a été créé.

Type : Timestamp

RestoreTestingPlanArn

ARN (Amazon Resource Name) unique du plan de test de la restauration.

Type : chaîne

RestoreTestingPlanName

Le nom ne peut pas être modifié après la création. Le nom comprend uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : chaîne

UpdateTime

Heure à laquelle la mise à jour s'est terminée pour le plan de test de restauration.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateRestoreTestingSelection

Service : AWS Backup

Met à jour la sélection de test de restauration spécifiée.

La plupart des éléments, à l'exception de `RestoreTestingSelectionName`, peuvent être mis à jour avec cette demande.

Vous pouvez utiliser des ARN ou des conditions de ressources protégées, mais pas les deux.

Syntaxe de la demande

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "ValidationWindowHours": number
   }
}
```

Paramètres de demande URI

La demande utilise les paramètres URI suivants.

RestoreTestingPlanName

Le nom du plan de test de la restauration est requis pour mettre à jour le plan de test indiqué.

Obligatoire : oui

RestoreTestingSelectionName

Nom de la sélection de test de restauration requise de la sélection de test de restauration que vous souhaitez mettre à jour.

Obligatoire : oui

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

RestoreTestingSelection

Pour mettre à jour votre sélection de tests de la restauration, vous pouvez utiliser des ARN ou des conditions de ressources protégées, mais pas les deux. En d'autres termes, si votre sélection a `ProtectedResourceArns`, la demande de mise à jour avec le paramètre `ProtectedResourceConditions` échouera.

Type : objet RestoreTestingSelectionForUpdate

Obligatoire : oui

Syntaxe de la réponse

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string",
```

```
    "UpdateTime": number
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

CreationTime

Heure à laquelle la sélection des ressources testées a été mise à jour avec succès.

Type : Timestamp

RestoreTestingPlanArn

Chaîne unique qui est le nom du plan de test de la restauration.

Type : chaîne

RestoreTestingPlanName

Le plan de test de restauration auquel la sélection de test de restauration mise à jour est associée.

Type : chaîne

RestoreTestingSelectionName

Nom de la sélection de test de restauration renvoyé.

Type : chaîne

UpdateTime

Heure à laquelle la mise à jour s'est terminée pour la sélection du test de restauration.

Type : Timestamp

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

AWS Backup ne peut pas exécuter l'action que vous avez demandée tant qu'il n'a pas terminé d'exécuter une action précédente. Réessayez ultérieurement.

Code d’état HTTP : 400

InvalidParameterValueException

Indique une erreur avec la valeur d'un paramètre. Par exemple, la valeur est hors de portée.

Code d’état HTTP : 400

MissingParameterValueException

Indique qu'un paramètre obligatoire est manquant.

Code d’état HTTP : 400

ResourceNotFoundException

Aucune ressource requise pour l'action n'existe.

Code d’état HTTP : 400

ServiceUnavailableException

La demande a échoué en raison d'une défaillance temporaire du serveur.

Code d’état HTTP : 500

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

AWS Backup gateway

Les actions suivantes sont prises en charge par AWS Backup gateway :

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AssociateGatewayToServer

Service : AWS Backup gateway

Associe une passerelle de sauvegarde à votre serveur. Une fois le processus d'association terminé, vous pouvez sauvegarder et restaurer vos machines virtuelles via la passerelle.

Syntaxe de la requête

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette `ListGateways` opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

ServerArn

Amazon Resource Name (ARN) du serveur qui héberge vos machines virtuelles.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) d'une passerelle.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

CreateGateway

Service : AWS Backup gateway

Crée une passerelle de sauvegarde. Une fois la passerelle créée, vous pouvez l'associer à un serveur à l'aide de l'opération `AssociateGatewayToServer`.

Syntaxe de la requête

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

ActivationKey

La clé d'activation de la passerelle créée.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 50.

Modèle : `^[0-9a-zA-Z\-]+$`

Obligatoire : oui

GatewayDisplayName

Le nom d'affichage de la passerelle créée.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : oui

GatewayType

Type de passerelle créée.

Type : chaîne

Valeurs valides : `BACKUP_VM`

Obligatoire : oui

Tags

Liste jusqu'à 50 balises à attribuer à la passerelle. Chaque balise est une paire clés-valeurs.

Type : tableau d'objets Tag

Obligatoire : non

Syntaxe de la réponse

```
{
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous créez.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python

- AWS SDK pour Ruby V3

DeleteGateway

Service : AWS Backup gateway

Supprime une passerelle de sauvegarde.

Syntaxe de la requête

```
{
   "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle à supprimer.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous avez supprimée.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DeleteHypervisor

Service : AWS Backup gateway

Supprime un hyperviseur.

Syntaxe de la requête

```
{
   "HypervisorArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur à supprimer.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "HypervisorArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur que vous avez supprimé.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

DisassociateGatewayFromServer

Service : AWS Backup gateway

Dissocie une passerelle de sauvegarde du serveur spécifié. Une fois le processus de dissociation terminé, la passerelle ne peut plus accéder aux machines virtuelles du serveur.

Syntaxe de la requête

```
{
   "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle à dissocier.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous avez dissociée.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d’état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetBandwidthRateLimitSchedule

Service : AWS Backup gateway

Récupère la planification de limite de débit de la bande passante pour une passerelle spécifiée. Par défaut, les passerelles n'ont pas de planification de limite de débit de la bande passante, ce qui signifie qu'aucune limitation de débit de bande passante n'est en vigueur. Utilisez ceci pour obtenir la planification de limite de débit de la bande passante d'une passerelle.

Syntaxe de la requête

```
{
   "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette ListGatewaysopération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
```

```
            "DaysOfWeek": [ number ],
            "EndHourOfDay": number,
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
        }
    ],
    "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

BandwidthRateLimitIntervals

Un tableau contenant les intervalles de planification de limite de débit de la bande passante pour une passerelle. Lorsqu'aucun intervalle de limite de débit de bande passante n'a été planifié, le tableau est vide.

Type : tableau d'objets BandwidthRateLimitInterval

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 20 éléments.

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette `ListGateways`opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetGateway

Service : AWS Backup gateway

En fournissant l'ARN (Amazon Resource Name), cette API renvoie la passerelle.

Syntaxe de la requête

```
{
   "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
```

```
            "DayOfWeek": number,
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Gateway

En fournissant l'ARN (Amazon Resource Name), cette API renvoie la passerelle.

Type : objet GatewayDetails

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetHypervisor

Service : AWS Backup gateway

Cette action demande des informations sur l'hyperviseur spécifié auquel la passerelle va se connecter. Un hyperviseur est un matériel, un logiciel ou un microprogramme qui crée et gère des machines virtuelles et leur alloue des ressources.

Syntaxe de la requête

```
{
   "HypervisorArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
```

```
        "LatestMetadataSyncStatus": "string",
        "LatestMetadataSyncStatusMessage": "string",
        "LogGroupArn": "string",
        "Name": "string",
        "State": "string"
    }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Hypervisor

Détails sur l'hyperviseur demandé.

Type : objet HypervisorDetails

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetHypervisorPropertyMappings

Service : AWS Backup gateway

Cette action récupère les mappages de propriétés pour l'hyperviseur spécifié. Un mappage de propriétés d'hyperviseur affiche la relation entre les propriétés d'entité disponibles dans l'hyperviseur et les propriétés disponibles dans. AWS

Syntaxe de la requête

```
{
   "HypervisorArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
```

```
            "AwsTagValue": "string",
            "VmwareCategory": "string",
            "VmwareTagName": "string"
        }
    ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM.

Type : chaîne

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

Il s'agit d'un affichage des mappages entre les balises VMware et les balises AWS .

Type : tableau d'objets VmwareToAwsTagMapping

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

GetVirtualMachine

Service : AWS Backup gateway

En fournissant l'ARN (Amazon Resource Name), cette API renvoie la machine virtuelle.

Syntaxe de la requête

```
{
   "ResourceArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

ResourceArn

Amazon Resource Name (ARN) de la machine virtuelle.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
```

```
            {
               "VmwareCategory": "string",
               "VmwareTagDescription": "string",
               "VmwareTagName": "string"
            }
         ]
      }
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

VirtualMachine

Cet objet contient les attributs de base de la `VirtualMachine` contenus dans la sortie de `GetVirtualMachine`

Type : objet VirtualMachineDetails

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ImportHypervisorConfiguration

Service : AWS Backup gateway

Se connecte à un hyperviseur en important sa configuration.

Syntaxe de la requête

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Host

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : chaîne

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : ^.+$

Obligatoire : oui

KmsKeyArn

Le AWS Key Management Service pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obligatoire : non

Name

Le nom de l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : oui

Password

Le mot de passe pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[ -~]+$`

Obligatoire : non

Tags

Les balises de la configuration de l'hyperviseur à importer.

Type : tableau d’objets Tag

Obligatoire : non

Username

Le nom d'utilisateur pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "HypervisorArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur que vous avez dissocié.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListGateways

Service : AWS Backup gateway

Répertorie les passerelles de sauvegarde détenues par un Compte AWS dans un Région AWS. La liste renvoyée est classée par Amazon Resource Name (ARN) de passerelle.

Syntaxe de la requête

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

MaxResults

Nombre maximum de passerelles à répertorier.

Type : entier

Plage valide : Valeur minimum de 1.

Obligatoire : non

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `MaxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : `^.+$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Gateways

Une liste de vos passerelles.

Type : tableau d'objets Gateway

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : `^.+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListHypervisors

Service : AWS Backup gateway

Répertorie vos hyperviseurs.

Syntaxe de la requête

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

MaxResults

Nombre maximal d'hyperviseurs à répertorier.

Type : entier

Plage valide : Valeur minimum de 1.

Obligatoire : non

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : `^.+$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Hypervisors

List de vos objets `Hypervisor`, classés par Amazon Resource Name (ARN).

Type : tableau d'objets Hypervisor

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : `^.+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListTagsForResource

Service : AWS Backup gateway

Répertorie les balises appliquées à la ressource identifiée par son Amazon Resource Name (ARN).

Syntaxe de la requête

```
{
   "ResourceArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

ResourceArn

Amazon Resource Name (ARN) des balises de la ressource à répertorier.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ResourceArn

Amazon Resource Name (ARN) des balises de la ressource que vous avez répertoriée.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

Liste des balises de la ressource.

Type : tableau d'objets Tag

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

ListVirtualMachines

Service : AWS Backup gateway

Répertorie vos machines virtuelles.

Syntaxe de la requête

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur connecté à votre machine virtuelle.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : non

MaxResults

Le nombre maximal de machines virtuelles à répertorier.

Type : entier

Plage valide : Valeur minimum de 1.

Obligatoire : non

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : `^.+$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

NextToken

L'élément suivant selon une liste partielle des ressources renvoyées. Par exemple, si une demande est faite pour renvoyer `maxResults` ressources, `NextToken` vous permet de renvoyer d'autres éléments dans votre liste en commençant par l'emplacement indiqué par le jeton suivant.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 1 000.

Modèle : `^.+$`

VirtualMachines

List de vos objets `VirtualMachine`, classés par Amazon Resource Name (ARN).

Type : tableau d'objets VirtualMachine

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutBandwidthRateLimitSchedule

Service : AWS Backup gateway

Cette action définit la planification de limite de débit de la bande passante pour une passerelle spécifiée. Par défaut, les passerelles n'ont pas de planification de limite de débit de la bande passante, ce qui signifie qu'aucune limitation de débit de bande passante n'est en vigueur. Utilisez-le pour lancer la planification de limite de débit de la bande passante d'une passerelle.

Syntaxe de la requête

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

BandwidthRateLimitIntervals

Un tableau contenant les intervalles de planification de limite de débit de la bande passante pour une passerelle. Lorsqu'aucun intervalle de limite de débit de bande passante n'a été planifié, le tableau est vide.

Type : tableau d’objets BandwidthRateLimitInterval

Membres du tableau : nombre minimum de 0 élément. Nombre maximum de 20 éléments.

Obligatoire : oui

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette ListGatewaysopération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette ListGatewaysopération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutHypervisorPropertyMappings

Service : AWS Backup gateway

Cette action définit les mappages de propriétés pour l'hyperviseur spécifié. Un mappage de propriétés d'hyperviseur affiche la relation entre les propriétés d'entité disponibles dans l'hyperviseur et les propriétés disponibles dans. AWS

Syntaxe de la requête

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM.

Type : chaîne

Contraintes de longueur : longueur minimale de 20. Longueur maximale de 2048.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

Obligatoire : oui

VmwareToAwsTagMappings

Cette action demande le mappage des balises VMware avec les balises AWS .

Type : tableau d'objets VmwareToAwsTagMapping

Obligatoire : oui

Syntaxe de la réponse

```
{
   "HypervisorArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

Code d’état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d’état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

PutMaintenanceStartTime

Service : AWS Backup gateway

Définissez l'heure de début de la maintenance pour une passerelle.

Syntaxe de la requête

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

DayOfMonth

Le jour du mois auquel commencer la maintenance d'une passerelle.

La plage des valeurs valides s'étend de `Sunday` à `Saturday`.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 31.

Obligatoire : non

DayOfWeek

Le jour de la semaine auquel commencer la maintenance d'une passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 6.

Obligatoire : non

GatewayArn

Amazon Resource Name (ARN) de la passerelle, utilisé pour spécifier l'heure de début de la maintenance.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

HourOfDay

L'heure de la journée à laquelle commencer la maintenance d'une passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

MinuteOfHour

La minute de l'heure à laquelle commencer la maintenance d'une passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

Syntaxe de la réponse

```
{
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) d'une passerelle pour laquelle vous définissez l'heure de début de la maintenance.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d’état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

StartVirtualMachinesMetadataSync

Service : AWS Backup gateway

Cette action envoie une demande de synchronisation des métadonnées entre les machines virtuelles spécifiées.

Syntaxe de la requête

```
{
   "HypervisorArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "HypervisorArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

Code d’état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

TagResource

Service : AWS Backup gateway

Balise la ressource.

Syntaxe de la requête

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

ResourceARN

Amazon Resource Name (ARN) de la ressource à baliser.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Tags

Liste des balises à attribuer à la ressource.

Type : tableau d’objets Tag

Obligatoire : oui

Syntaxe de la réponse

```
{
   "ResourceARN": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ResourceARN

Amazon Resource Name (ARN) de la ressource que vous avez balisée.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

TestHypervisorConfiguration

Service : AWS Backup gateway

Teste la configuration de votre hyperviseur pour vérifier que la passerelle de sauvegarde peut se connecter à l'hyperviseur et à ses ressources.

Syntaxe de la requête

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle de l'hyperviseur à tester.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Host

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : chaîne

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : `^.+$`

Obligatoire : oui

Password

Le mot de passe pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[ -~]+$`

Obligatoire : non

Username

Le nom d'utilisateur pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200 avec un corps HTTP vide.

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d’état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UntagResource

Service : AWS Backup gateway

Supprime des balises de la ressource.

Syntaxe de la requête

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

ResourceARN

Amazon Resource Name (ARN) de la ressource pour laquelle supprimer des balises.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

TagKeys

La liste des clés de balise spécifiant les balises à supprimer.

Type : tableau de chaînes

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatoire : oui

Syntaxe de la réponse

```
{
   "ResourceARN": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

ResourceARN

Amazon Resource Name (ARN) de la ressource pour laquelle vous avez supprimé des balises.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateGatewayInformation

Service : AWS Backup gateway

Met à jour le nom d'une passerelle. Spécifiez la passerelle à mettre à jour en utilisant l'Amazon Resource Name (ARN) de la passerelle dans votre demande.

Syntaxe de la requête

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle à mettre à jour.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

GatewayDisplayName

Le nom d'affichage mis à jour de la passerelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous avez mis à jour.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d’état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d’état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateGatewaySoftwareNow

Service : AWS Backup gateway

Met à jour le logiciel d'une machine virtuelle (VM) de passerelle. La demande déclenche immédiatement la mise à jour logicielle.

> **Note**
>
> Lorsque vous effectuez cette demande, vous obtenez immédiatement une réponse `200 OK` positive. La mise à jour peut toutefois prendre un certain temps.

Syntaxe de la requête

```
{
   "GatewayArn": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

GatewayArn

Amazon Resource Name (ARN) de la passerelle à mettre à jour.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

Syntaxe de la réponse

```
{
```

```
   "GatewayArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

GatewayArn

Amazon Resource Name (ARN) de la passerelle que vous avez mis à jour.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d’état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3
- AWS SDK pour Python
- AWS SDK pour Ruby V3

UpdateHypervisor

Service : AWS Backup gateway

Met à jour les métadonnées d'un hyperviseur, notamment son hôte, son nom d'utilisateur et son mot de passe. Spécifiez l'hyperviseur à mettre à jour en utilisant l'Amazon Resource Name (ARN) de l'hyperviseur dans votre demande.

Syntaxe de la requête

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

Paramètres de demande

Pour plus d'informations sur les paramètres courants pour toutes les actions, consultez Paramètres courants.

Cette demande accepte les données suivantes au format JSON.

Host

L'hôte mis à jour de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : chaîne

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : ^.+$

Obligatoire : non

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur à mettre à jour.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : oui

LogGroupArn

Amazon Resource Name (ARN) du groupe de passerelles dans le journal demandé.

Type : chaîne

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Modèle : `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Obligatoire : non

Name

Le nom mis à jour pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

Password

Le mot de passe mis à jour pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[ -~]+$`

Obligatoire : non

Username

Le nom d'utilisateur mis à jour pour l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obligatoire : non

Syntaxe de la réponse

```
{
   "HypervisorArn": "string"
}
```

Eléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur que vous avez mis à jour.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Erreurs

Pour plus d'informations sur les erreurs courantes pour toutes les actions, consultez Erreurs courantes.

AccessDeniedException

L'opération ne peut pas se poursuivre, car vous ne disposez pas d'autorisations suffisantes.

Code d'état HTTP : 400

ConflictException

L'opération ne peut pas se poursuivre, car elle n'est pas prise en charge.

Code d'état HTTP : 400

InternalServerException

L'opération n'a pas réussi, car une erreur interne s'est produite. Réessayez ultérieurement.

Code d'état HTTP : 500

ResourceNotFoundException

Une ressource requise pour l'action n'a pas été trouvée.

Code d'état HTTP : 400

ThrottlingException

Le TPS a été limité pour protéger contre les volumes de demandes élevés intentionnels ou involontaires.

Code d'état HTTP : 400

ValidationException

L'opération n'a pas réussi, car une erreur de validation s'est produite.

Code d'état HTTP : 400

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- Interface de ligne de commande AWS
- AWS SDK pour .NET
- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK pour Java V2
- AWS SDK pour V3 JavaScript
- AWS SDK pour PHP V3

- AWS SDK pour Python
- AWS SDK pour Ruby V3

Types de données

Les types de données suivants sont pris en charge par AWS Backup :

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl

- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

Les types de données suivants sont pris en charge par AWS Backup gateway :

- BandwidthRateLimitInterval

- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

Les types de données suivants sont pris en charge par AWS Backup :

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter

- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection

- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AdvancedBackupSetting

Service : AWS Backup

Les options de sauvegarde pour chaque type de ressource.

Table des matières

BackupOptions

Spécifie l'option de sauvegarde pour une ressource sélectionnée. Cette option est uniquement disponible pour les tâches de sauvegarde Windows VSS.

Valeurs valides :

Définissez sur `"WindowsVSS":"enabled"` pour activer l'option de sauvegarde `WindowsVSS` et créer une sauvegarde Windows VSS.

Définissez sur `"WindowsVSS":"disabled"` pour créer une sauvegarde régulière. L'option `WindowsVSS` n'est pas activée par défaut.

Si vous spécifiez une option non valide, vous obtenez une exception `InvalidParameterValueException`.

Pour plus d'informations sur les sauvegardes Windows VSS, consultez Création d'une sauvegarde Windows avec VSS.

Type : mappage chaîne/chaîne

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

ResourceType

Spécifie un objet contenant le type de ressource et les options de sauvegarde. Le seul type de ressource pris en charge est celui des instances Amazon EC2 avec Windows Volume Shadow Copy Service (VSS). Pour un CloudFormation exemple, consultez l'exemple de CloudFormation modèle pour activer Windows VSS dans le Guide de l' AWS Backup utilisateur.

Valeurs valides : `EC2`.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupJob

Service : AWS Backup

Contient des informations détaillées sur une tâche de sauvegarde.

Table des matières

AccountId

ID de compte du propriétaire de la tâche de sauvegarde.

Type : chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

BackupJobId

Identifie de manière unique une demande AWS Backup de sauvegarde d'une ressource.

Type : chaîne

Obligatoire : non

BackupOptions

Spécifie l'option de sauvegarde pour une ressource sélectionnée. Cette option est uniquement disponible pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Valeurs valides : définissez sur `"WindowsVSS":"enabled"` pour activer l'option de sauvegarde `WindowsVSS` et créer une sauvegarde Windows VSS. Définissez sur `"WindowsVSS":"disabled"` pour créer une sauvegarde régulière. Si vous spécifiez une option non valide, vous obtenez une exception `InvalidParameterValueException`.

Type : mappage chaîne/chaîne

Modèle de clé :`^[a-zA-Z0-9\-\_\.]{1,50}$`

Modèle de valeur : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

BackupSizeInBytes

Taille d'une sauvegarde, en octets.

Type : long

Obligatoire : non

BackupType

Représente le type de sauvegarde pour une tâche de sauvegarde.

Type : chaîne

Obligatoire : non

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : non

BytesTransferred

Taille en octets transférée vers un coffre-fort de sauvegarde au moment où le statut de la tâche a été demandé.

Type : long

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en

millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatedBy

Contient des informations d'identification relatives à la création d'une tâche de sauvegarde, dont `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour la créer.

Type : objet RecoveryPointCreator

Obligatoire : non

CreationDate

Date et heure de création d'une tâche de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ExpectedCompletionDate

Date et heure de fin attendues d'une tâche de sauvegarde des ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `ExpectedCompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible. Les rôles IAM autres que le rôle par défaut doivent inclure `AWSBackup` ou `AwsBackup` dans le nom du rôle. Par exemple, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Les noms de rôles dépourvus de ces chaînes ne sont pas autorisés à effectuer des tâches de sauvegarde.

Type : chaîne

Obligatoire : non

InitiationDate

Date à laquelle la tâche de sauvegarde a été lancée.

Type : Timestamp

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'une tâche de sauvegarde parent (composite).

Type : booléen

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes peuvent inclure `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` et `INVALIDPARAMETERS`. Voir Surveillance pour une liste de MessageCategory chaînes.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

Type : chaîne

Obligatoire : non

ParentJobId

Cela identifie de manière unique une demande vers AWS Backup pour sauvegarder une ressource. Le retour sera l'ID de tâche parent (composite).

Type : chaîne

Obligatoire : non

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

ResourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource à sauvegarder ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

StartBy

Spécifie l'heure au format Unix et au format UTC (Coordinated Universal Time) quand une tâche de sauvegarde doit être démarrée avant d'être annulée. La valeur est calculée en ajoutant la fenêtre de démarrage à l'heure planifiée. Ainsi, si l'heure prévue était 18 h 00 et que la fenêtre de début était de 2 heures, l'heure `StartBy` serait 20 h 00 à la date spécifiée. La valeur de `StartBy` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

L'état actuel d'une tâche de sauvegarde.

Type : chaîne

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

Obligatoire : non

StatusMessage

Message détaillé expliquant le statut de la tâche de sauvegarde d'une ressource.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2

- AWS SDK pour Ruby V3

BackupJobSummary

Service : AWS Backup

Il s'agit d'un résumé des tâches créées ou en cours d'exécution au cours des 30 derniers jours.

Le résumé renvoyé peut contenir les éléments suivants : région, compte, État RestourceType, MessageCategory, StartTime, EndTime, et nombre de tâches incluses.

Table des matières

AccountId

L'ID de compte qui possède les tâches figurant dans le résumé.

Type : chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

Count

La valeur du nombre de tâches dans un résumé des tâches.

Type : entier

Obligatoire : non

EndTime

La valeur de l'heure au format numérique de l'heure de fin d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes incluent `AccessDenied`, `Success` et `InvalidParameters`. Voir Surveillance pour une liste de MessageCategory chaînes.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

AGGREGATE_ALL agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

Type : chaîne

Obligatoire : non

Region

Les AWS régions figurant dans le résumé du poste.

Type : chaîne

Obligatoire : non

ResourceType

Cette valeur est le nombre de tâches pour le type de ressource spécifié. La demande GetSupportedResourceTypes renvoie des chaînes pour les types de ressources pris en charge.

Type : chaîne

Modèle : ^[a-zA-Z0-9\-_\.]{1,50}$

Obligatoire : non

StartTime

La valeur de l'heure au format numérique de l'heure de début d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

Cette valeur est le nombre de tâches pour les tâches ayant l'état spécifié.

Type : chaîne

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupPlan

Service : AWS Backup

Contient un nom d'affichage de plan de sauvegarde facultatif et un tableau d'objets `BackupRule`, chaque objet spécifiant une règle de sauvegarde. Dans un plan de sauvegarde, chaque règle est une tâche planifiée distincte et peut sauvegarder une sélection différente de ressources AWS .

Table des matières

BackupPlanName

Nom complet d'un plan de sauvegarde. Doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : oui

Rules

Tableau d'objets `BackupRule`, dont chacun spécifie une tâche planifiée qui est utilisée pour sauvegarder une sélection de ressources.

Type : tableau d’objets BackupRule

Obligatoire : oui

AdvancedBackupSettings

Contient une liste d'`BackupOptions` pour chaque type de ressource.

Type : tableau d’objets AdvancedBackupSetting

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2

- AWS SDK pour Ruby V3

BackupPlanInput

Service : AWS Backup

Contient un nom d'affichage de plan de sauvegarde facultatif et un tableau d'objets `BackupRule`, chaque objet spécifiant une règle de sauvegarde. Dans un plan de sauvegarde, chaque règle est une tâche planifiée distincte.

Table des matières

BackupPlanName

Nom complet d'un plan de sauvegarde. Doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : oui

Rules

Tableau d'objets `BackupRule`, dont chacun spécifie une tâche planifiée qui est utilisée pour sauvegarder une sélection de ressources.

Type : tableau d’objets BackupRuleInput

Obligatoire : oui

AdvancedBackupSettings

Spécifie une liste d'`BackupOptions` pour chaque type de ressource. Ces paramètres sont uniquement disponibles pour les tâches de sauvegarde Windows Volume Shadow Copy Service (VSS).

Type : tableau d’objets AdvancedBackupSetting

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++

- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupPlansListMember

Service : AWS Backup

Contient des métadonnées relatives à un plan de sauvegarde.

Table des matières

AdvancedBackupSettings

Contient une liste d'`BackupOptions` pour un type de ressource.

Type : tableau d’objets AdvancedBackupSetting

Obligatoire : non

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

Obligatoire : non

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

Obligatoire : non

BackupPlanName

Nom complet d'un plan de sauvegarde enregistré.

Type : chaîne

Obligatoire : non

CreationDate

Date et heure de création d'un plan de sauvegarde de ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

DeletionDate

Date et heure de suppression d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `DeletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastExecutionDate

La dernière fois que ce plan de sauvegarde a été exécuté. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de `LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

VersionId

Chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Les ID de version ne peuvent pas être modifiés.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupPlanTemplatesListMember

Service : AWS Backup

Objet spécifiant les métadonnées associées à un modèle de plan de sauvegarde.

Table des matières

BackupPlanTemplateId

Identifie de manière unique un modèle de plan de sauvegarde enregistré.

Type : chaîne

Obligatoire : non

BackupPlanTemplateName

Nom d'affichage facultatif d'un modèle de plan de sauvegarde.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupRule

Service : AWS Backup

Spécifie une tâche planifiée utilisée pour sauvegarder une sélection de ressources.

Table des matières

RuleName

Nom d'affichage d'une règle de sauvegarde. Doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : oui

TargetBackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

CompletionWindowMinutes

Une valeur en minutes après le démarrage réussi d'une tâche de sauvegarde et avant qu'elle doive être terminée ou qu'elle soit annulée par AWS Backup. Cette valeur est facultative.

Type : long

Obligatoire : non

CopyActions

Tableau d'objets `CopyAction`, qui contient les détails de l'opération de copie.

Type : tableau d’objets CopyAction

Obligatoire : non

EnableContinuousBackup

Spécifie s'il AWS Backup crée des sauvegardes continues. De véritables raisons AWS Backup de créer des sauvegardes continues capables de point-in-time restauration (PITR). Faux (ou non spécifié) entraîne AWS Backup la création de sauvegardes instantanées.

Type : booléen

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet Lifecycle

Obligatoire : non

RecoveryPointTags

Les balises attribuées aux ressources associées à cette règle lors de la restauration à partir d'une sauvegarde.

Type : mappage chaîne/chaîne

Obligatoire : non

RuleId

Identifie de manière unique une règle utilisée pour planifier la sauvegarde d'une sélection de ressources.

Type : chaîne

Obligatoire : non

ScheduleExpression

Expression cron en UTC indiquant à quel moment une tâche de sauvegarde est AWS Backup initiée. Pour plus d'informations sur les expressions AWS cron, consultez la section Schedule Expressions for Rules dans le guide de l'utilisateur Amazon CloudWatch Events. . Deux exemples d'expressions AWS cron sont `15 * ? * * *` (effectuer une sauvegarde toutes les heures 15 minutes après l'heure) et `0 12 * * ? *` (effectuer une sauvegarde tous les jours à midi UTC). Pour consulter un tableau d'exemples, cliquez sur le lien précédent et faites défiler la page vers le bas.

Type : chaîne

Obligatoire : non

ScheduleExpressionTimezone

Fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowMinutes

Valeur en minutes après la planification d'une sauvegarde avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, elle doit être d'au moins 60 minutes pour éviter les erreurs.

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste `CREATED` jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à`RUNNING`) ou jusqu'à ce que le statut de la tâche passe à `EXPIRED` (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Type : long

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupRuleInput

Service : AWS Backup

Spécifie une tâche planifiée utilisée pour sauvegarder une sélection de ressources.

Table des matières

RuleName

Nom d'affichage d'une règle de sauvegarde. Doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : oui

TargetBackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : oui

CompletionWindowMinutes

Une valeur en minutes après le démarrage réussi d'une tâche de sauvegarde et avant qu'elle doive être terminée ou qu'elle soit annulée par AWS Backup. Cette valeur est facultative.

Type : long

Obligatoire : non

CopyActions

Tableau d'objets `CopyAction`, qui contient les détails de l'opération de copie.

Type : tableau d’objets CopyAction

Obligatoire : non

EnableContinuousBackup

Spécifie s'il AWS Backup crée des sauvegardes continues. Les vraies raisons AWS Backup de créer des sauvegardes continues capables de point-in-time restauration (PITR). Faux (ou non spécifié) entraîne AWS Backup la création de sauvegardes instantanées.

Type : booléen

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup fera automatiquement la transition et expirera les sauvegardes en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition vers le froid après plusieurs jours » ne peut pas être modifié une fois qu'une sauvegarde a été transférée vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Ce paramètre a une valeur maximale de 100 ans (36 500 jours).

Type : objet Lifecycle

Obligatoire : non

RecoveryPointTags

Les balises à attribuer aux ressources.

Type : mappage chaîne/chaîne

Obligatoire : non

ScheduleExpression

Expression CRON en UTC indiquant à quel moment une tâche de sauvegarde est AWS Backup initiée.

Type : chaîne

Obligatoire : non

ScheduleExpressionTimezone

Fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowMinutes

Valeur en minutes après la planification d'une sauvegarde avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, elle doit être d'au moins 60 minutes pour éviter les erreurs.

Ce paramètre a une valeur maximale de 100 ans (52 560 000 minutes).

Pendant la fenêtre de démarrage, le statut de la tâche de sauvegarde reste `CREATED` jusqu'à ce qu'elle ait démarré ou jusqu'à ce que le délai de la fenêtre de démarrage soit écoulé. Si, dans la fenêtre de démarrage, time AWS Backup reçoit une erreur autorisant une nouvelle tentative de la tâche, elle AWS Backup réessaiera automatiquement de recommencer la tâche au moins toutes les 10 minutes jusqu'à ce que la sauvegarde commence avec succès (le statut de la tâche passe à`RUNNING`) ou jusqu'à ce que le statut de la tâche passe à `EXPIRED` (ce qui devrait se produire une fois la fenêtre de démarrage terminée).

Type : long

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupSelection

Service : AWS Backup

Utilisez pour spécifier un ensemble de ressources à un plan de sauvegarde.

Nous vous recommandons de spécifier les conditions, les balises ou les ressources à inclure ou à exclure. Dans le cas contraire, Backup tente de sélectionner toutes les ressources de stockage prises en charge et acceptées, ce qui peut avoir des conséquences financières imprévues.

Pour plus d'informations, consultez la section Affectation de ressources par programmation.

Table des matières

IamRoleArn

L'ARN du rôle IAM AWS Backup utilisé pour s'authentifier lors de la sauvegarde de la ressource cible ; par exemple,. `arn:aws:iam::123456789012:role/S3Access`

Type : chaîne

Obligatoire : oui

SelectionName

Nom complet d'un document de sélection de ressource. Doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : oui

Conditions

Les conditions que vous définissez pour affecter des ressources à vos plans de sauvegarde à l'aide de balises. Par exemple, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`.

`Conditions`soutient `StringEquals`,`StringLike`,`StringNotEquals`, et`StringNotLike`. Les opérateurs de condition sont sensibles à la casse.

Si vous spécifiez plusieurs conditions, les ressources doivent répondre à toutes les conditions (logique ET).

Type : objet Conditions

Obligatoire : non

ListOfTags

Les conditions que vous définissez pour affecter des ressources à vos plans de sauvegarde à l'aide de balises. Par exemple, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`.

`ListOfTags`supports uniquement`StringEquals`. Les opérateurs de condition sont sensibles à la casse.

Si vous spécifiez plusieurs conditions, les ressources doivent correspondre à n'importe laquelle des conditions (logique OR).

Type : tableau d’objets Condition

Obligatoire : non

NotResources

Les Amazon Resource Names (ARN) des ressources à exclure d'un plan de sauvegarde. Le nombre maximal d'ARN est de 500 sans caractères génériques, ou de 30 ARN avec caractères génériques.

Si vous devez exclure de nombreuses ressources d'un plan de sauvegarde, envisagez une stratégie de sélection de ressources différente, comme l'attribution d'un seul ou de quelques types de ressource, ou l'affinement de votre sélection de ressources à l'aide de balises.

Type : tableau de chaînes

Obligatoire : non

Resources

Les Amazon Resource Names (ARN) des ressources à attribuer à un plan de sauvegarde. Le nombre maximal d'ARN est de 500 sans caractères génériques, ou de 30 ARN avec caractères génériques.

Si vous devez attribuer de nombreuses ressources à un plan de sauvegarde, envisagez une stratégie de sélection de ressources différente, comme l'attribution de toutes les ressources d'un type de ressource, ou l'affinement de votre sélection de ressources à l'aide de balises.

Si vous spécifiez plusieurs ARN, les ressources doivent correspondre à n'importe lequel des ARN (logique OR).

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupSelectionsListMember

Service : AWS Backup

Contient des métadonnées relatives à un objet `BackupSelection`.

Table des matières

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

Obligatoire : non

CreationDate

Date et heure de création d'un plan de sauvegarde, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

IamRoleArn

Spécifie l'Amazon Resource Name (ARN) du rôle IAM pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

SelectionId

Identifie de façon unique une demande d'attribution d'un ensemble de ressources à un plan de sauvegarde.

Type : chaîne

Obligatoire : non

SelectionName

Nom complet d'un document de sélection de ressource.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

BackupVaultListMember

Service : AWS Backup

Contient des métadonnées relatives à un coffre-fort de sauvegarde.

Table des matières

BackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : non

CreationDate

Date et heure de création d'une sauvegarde de ressources, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatorRequestId

Une chaîne unique qui identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

EncryptionKeyArn

Une clé de chiffrement côté serveur que vous pouvez spécifier pour chiffrer vos sauvegardes à partir de services prenant en charge la AWS Backup gestion complète, par exemple,. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Si vous spécifiez une clé, vous devez indiquer son ARN et non son alias. Si vous ne spécifiez aucune clé, AWS Backup crée une clé KMS pour vous par défaut.

Pour savoir quels AWS Backup services prennent en charge AWS Backup la gestion complète et comment AWS Backup gère le chiffrement des sauvegardes provenant de services qui ne le sont pas encore AWS Backup, voir Chiffrement des sauvegardes dans AWS Backup

Type : chaîne

Obligatoire : non

LockDate

Date et heure auxquelles la configuration de AWS Backup Vault Lock devient immuable, ce qui signifie qu'elle ne peut être ni modifiée ni supprimée.

Si vous avez appliqué Vault Lock à votre coffre-fort sans spécifier de date de verrouillage, vous pouvez modifier les paramètres de Vault Lock ou supprimer complètement Vault Lock du coffre-fort à tout moment.

Cette valeur est au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

Locked

Valeur booléenne qui indique si AWS Backup Vault Lock s'applique au coffre-fort de sauvegarde sélectionné. Si `true`, Vault Lock empêche les opérations de suppression et de mise à jour sur les points de récupération du coffre-fort sélectionné.

Type : booléen

Obligatoire : non

MaxRetentionDays

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention maximale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, Vault Lock n'applique pas de période de rétention maximale sur les points de récupération dans le coffre-fort (permettant un stockage indéfini).

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou inférieure à la période de rétention maximale. Si la période de conservation de la tâche est plus longue que cette période de conservation maximale, la tâche de sauvegarde ou de copie du coffre-fort échoue, et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

Obligatoire : non

MinRetentionDays

Le paramètre AWS Backup Vault Lock qui spécifie la période de rétention minimale pendant laquelle le coffre-fort conserve ses points de récupération. Si ce paramètre n'est pas spécifié, le verrouillage du coffre-fort n'applique pas de période de rétention minimale.

S'il est spécifié, toute tâche de sauvegarde ou de copie vers le coffre-fort doit avoir une politique de cycle de vie avec une période de rétention égale ou supérieure à la période de rétention minimale. Si la période de rétention de la tâche est plus courte que cette période de rétention minimale, la tâche de sauvegarde ou de copie du coffre-fort échoue et vous devez soit modifier vos paramètres de cycle de vie, soit utiliser un autre coffre-fort. Les points de récupération déjà stockés dans le coffre-fort avant Vault Lock ne sont pas affectés.

Type : long

Obligatoire : non

NumberOfRecoveryPoints

Nombre de points de récupération stockés dans un coffre-fort de sauvegarde.

Type : long

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

CalculatedLifecycle

Service : AWS Backup

Contient des horodatages `DeleteAt` et `MoveToColdStorageAt`, qui sont utilisés pour spécifier le cycle de vie d'un point de récupération.

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Table des matières

DeleteAt

Un horodatage qui indique quand supprimer un point de récupération.

Type : Timestamp

Obligatoire : non

MoveToColdStorageAt

Horodatage qui indique à quel moment il faut passer d'un point de récupération à un stockage à froid.

Type : Timestamp

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Condition

Service : AWS Backup

Contient un tableau de triplets composé d'un type de condition (par exemple, `StringEquals`), d'une clé et d'une valeur. Utilisé pour filtrer les ressources à l'aide de leurs balises et les attribuer à un plan de sauvegarde. Sensible à la casse.

Table des matières

ConditionKey

Clé dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Department` est la clé.

Type : chaîne

Obligatoire : oui

ConditionType

Opération appliquée à une paire clé-valeur utilisée pour attribuer des ressources à votre plan de sauvegarde. Condition prenant en charge uniquement `StringEquals`. Pour des options d'attribution plus flexibles, notamment `StringLike` et la possibilité d'exclure des ressources de votre plan de sauvegarde, utilisez `Conditions` (avec un « s » à la fin) pour votre `BackupSelection`.

Type : chaîne

Valeurs valides : `STRINGEQUALS`

Obligatoire : oui

ConditionValue

Valeur dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Accounting` est la valeur.

Type : chaîne

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ConditionParameter

Service : AWS Backup

Inclut des informations sur les balises que vous définissez pour attribuer des ressources balisées à un plan de sauvegarde.

Incluez le préfixe `aws:ResourceTag` dans vos balises. Par exemple, `"aws:ResourceTag/TagKey1": "Value1"`.

Table des matières

ConditionKey

Clé dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Department` est la clé.

Type : chaîne

Obligatoire : non

ConditionValue

Valeur dans une paire clé-valeur. Par exemple, dans la balise `Department: Accounting`, `Accounting` est la valeur.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Conditions

Service : AWS Backup

Contient des informations sur les ressources à inclure ou à exclure d'un plan de sauvegarde à l'aide de leurs balises. Les conditions sont sensibles à la casse.

Table des matières

StringEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées avec la même valeur. Également appelé « correspondance exacte ».

Type : tableau d’objets ConditionParameter

Obligatoire : non

StringLike

Filtre les valeurs de vos ressources balisées pour faire correspondre les valeurs des balises à l'aide d'un caractère générique (*) n'importe où dans la chaîne. Par exemple, « prod* » ou « *rod* » correspond à la valeur de balise « production ».

Type : tableau d’objets ConditionParameter

Obligatoire : non

StringNotEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées qui n'ont pas la même valeur. Également appelé « correspondance négative ».

Type : tableau d’objets ConditionParameter

Obligatoire : non

StringNotLike

Filtre les valeurs de vos ressources balisées pour détecter les valeurs de balise non correspondantes à l'aide d'un caractère générique (*) n'importe où dans la chaîne.

Type : tableau d’objets ConditionParameter

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ControlInputParameter

Service : AWS Backup

Les paramètres d'un contrôle. Un contrôle peut comporter aucun, un ou plusieurs paramètres. Un exemple de contrôle avec deux paramètres : « la fréquence du plan de sauvegarde est d'au moins `daily` et la période de conservation est d'au moins `1 year` ». Le premier paramètre est `daily`. Le second paramètre est `1 year`.

Table des matières

ParameterName

Le nom d'un paramètre, par exemple `BackupPlanFrequency`.

Type : chaîne

Obligatoire : non

ParameterValue

La valeur d'un paramètre, par exemple `hourly`.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ControlScope

Service : AWS Backup

Un cadre est constitué d'un ou plusieurs contrôles. Chaque contrôle possède sa propre portée de contrôle. La portée de contrôle peut s'appliquer à un ou plusieurs types de ressource, à une combinaison de clé et de valeur de balise ou à une combinaison de type de ressource et d'ID de ressource. Si aucune portée n'est spécifiée, les évaluations de la règle sont déclenchées lorsque n'importe quelle ressource de votre groupe d'enregistrement change dans la configuration.

> **Note**
>
> Pour définir une portée de contrôle qui inclut l'ensemble d'une ressource donnée, laissez `ControlScope` vide ou ne le transmettez pas lors de l'appel de `CreateFramework`.

Table des matières

ComplianceResourceIds

L'ID de la seule AWS ressource que vous souhaitez que votre étendue de contrôle contienne.

Type : tableau de chaînes

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 100 éléments.

Obligatoire : non

ComplianceResourceTypes

Indique si la portée de contrôle inclut un ou plusieurs types de ressources, tels que `EFS` ou `RDS`.

Type : tableau de chaînes

Obligatoire : non

Tags

La paire clé-valeur de balise appliquée aux AWS ressources pour lesquelles vous souhaitez déclencher l'évaluation d'une règle. Une seule paire clé-valeur peut être fournie. La valeur de la balise est facultative, mais elle ne peut pas être une chaîne vide si vous créez ou modifiez un framework à partir de la console (bien que la valeur puisse être une chaîne vide lorsqu'elle est incluse dans un CloudFormation modèle).

La structure pour attribuer une étiquette est la suivante : `[{"Key":"string","Value":"string"}]`.

Type : mappage chaîne/chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

CopyAction

Service : AWS Backup

Les détails de l'opération de copie.

Table des matières

DestinationBackupVaultArn

Un nom de ressource Amazon (ARN) qui identifie de manière unique le coffre-fort de sauvegarde de destination pour la sauvegarde copiée. Par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : oui

Lifecycle

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et`DeleteAfterDays`.

Type : objet Lifecycle

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

CopyJob

Service : AWS Backup

Contient des informations détaillées sur une tâche de copie.

Table des matières

AccountId

ID de compte du propriétaire de la tâche de copie.

Type : chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

BackupSizeInBytes

Taille, en octets, d'une tâche de copie.

Type : long

Obligatoire : non

ChildJobsInState

Cela renvoie les statistiques des tâches de copie enfant (imbriquées) incluses.

Type : mappage chaîne/long

Clés valides : `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de copie, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CompositeMemberIdentifier

Identifiant d'une ressource au sein d'un groupe composite, tel qu'un point de récupération imbriqué (enfant) appartenant à une pile composite (parent). L'ID est transféré à partir de l'ID logique au sein d'une pile.

Type : chaîne

Obligatoire : non

CopyJobId

Identifie de manière unique une tâche de copie.

Type : chaîne

Obligatoire : non

CreatedBy

Contient des informations sur le plan de sauvegarde et la règle AWS Backup utilisés pour lancer la sauvegarde du point de restauration.

Type : objet RecoveryPointCreator

Obligatoire : non

CreationDate

Date et heure de création d'une tâche de copie, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

DestinationBackupVaultArn

Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de copie de destination ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

DestinationRecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération de destination ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour copier le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'une tâche de copie parent (composite).

Type : booléen

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes peuvent inclure `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` et `InvalidParameters`. Voir Surveillance pour une liste de MessageCategory chaînes.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme

Type : chaîne

Obligatoire : non

NumberOfChildJobs

Le nombre de tâches de copie secondaires (imbriquées).

Type : long

Obligatoire : non

ParentJobId

Cela identifie de manière unique une demande vers AWS Backup pour copier une ressource. Le retour sera l'ID de tâche parent (composite).

Type : chaîne

Obligatoire : non

ResourceArn

La AWS ressource à copier ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource à copier ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS).

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

SourceBackupVaultArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un coffre-fort de copie source ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

SourceRecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération source ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

State

L'état actuel d'une tâche de copie.

Type : chaîne

Valeurs valides : `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Obligatoire : non

StatusMessage

Message détaillé expliquant le statut de la tâche de copie d'une ressource.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

CopyJobSummary

Service : AWS Backup

Il s’agit d’un résumé des tâches de copie créées ou en cours d’exécution au cours des 30 derniers jours.

Le résumé renvoyé peut contenir les éléments suivants : région, compte, État RestourceType, MessageCategory, StartTime, EndTime, et nombre de tâches incluses.

Table des matières

AccountId

L’ID de compte qui possède les tâches figurant dans le résumé.

Type : chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

Count

La valeur du nombre de tâches dans un résumé des tâches.

Type : entier

Obligatoire : non

EndTime

La valeur de l’heure au format numérique de l’heure de fin d’une tâche.

Cette valeur est l’heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

MessageCategory

Ce paramètre est le nombre de tâches pour la catégorie de message spécifiée.

Les exemples de chaînes incluent `AccessDenied`, `Success` et `InvalidParameters`. Voir Surveillance pour une liste de MessageCategory chaînes.

La valeur ANY renvoie le nombre de toutes les catégories de messages.

`AGGREGATE_ALL` agrège le nombre de tâches pour toutes les catégories de messages et renvoie la somme.

Type : chaîne

Obligatoire : non

Region

Les AWS régions figurant dans le résumé du poste.

Type : chaîne

Obligatoire : non

ResourceType

Cette valeur est le nombre de tâches pour le type de ressource spécifié. La demande `GetSupportedResourceTypes` renvoie des chaînes pour les types de ressources pris en charge

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

StartTime

La valeur de l'heure au format numérique de l'heure de début d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

Cette valeur est le nombre de tâches pour les tâches ayant l'état spécifié.

Type : chaîne

Valeurs valides : `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

DateRange

Service : AWS Backup

Il s'agit d'un filtre de ressources contenant FromDate : DateTime et ToDate : DateTime. Les deux valeurs sont requises. Les DateTime valeurs futures ne sont pas autorisées.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives). Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Table des matières

FromDate

Cette valeur est la date de début incluse.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives).

Type : Timestamp

Obligatoire : oui

ToDate

Cette valeur est la date de fin incluse.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives).

Type : Timestamp

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Framework

Service : AWS Backup

Contient des informations détaillées sur un framework. Les frameworks contiennent des contrôles qui évaluent vos événements et ressources de sauvegarde et établissent des rapports. Les frameworks génèrent des résultats quotidiens en matière de conformité.

Table des matières

CreationTime

Date et heure de création d'un framework, dans une représentation ISO 8601. La valeur de `CreationTime` est précise en millisecondes. Par exemple, 2020-07-10T15:00:00.000-08:00 représente le 10 juillet 2020 à 15 h 00 avec 8 heures de retard sur le temps UTC.

Type : Timestamp

Obligatoire : non

DeploymentStatus

Le statut du déploiement d'un framework. Les statuts sont les suivants :

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Type : chaîne

Obligatoire : non

FrameworkArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

FrameworkDescription

Une description facultative du cadre avec 1 024 caractères au maximum.

Type : chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

FrameworkName

Le nom unique d'un cadre. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : non

NumberOfControls

Le nombre de contrôles contenus dans le framework.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

FrameworkControl

Service : AWS Backup

Contient des informations détaillées sur tous les contrôles d'un cadre. Chaque cadre doit contenir au moins un contrôle.

Table des matières

ControlName

Le nom d'un contrôle. Ce nom contient de 1 à 256 caractères.

Type : chaîne

Obligatoire : oui

ControlInputParameters

Les paires nom/valeur.

Type : tableau d’objets ControlInputParameter

Obligatoire : non

ControlScope

La portée d'un contrôle. La portée du contrôle définit ce que le contrôle va évaluer. Trois exemples de portées de contrôle sont : un plan de sauvegarde spécifique, tous les plans de sauvegarde avec une balise spécifique ou tous les plans de sauvegarde.

Pour de plus amples informations, veuillez consulter `ControlScope.`

Type : objet ControlScope

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2

- AWS SDK pour Ruby V3

KeyValue

Service : AWS Backup

Pair of two related strings. Les caractères autorisés sont les lettres, les espaces et les chiffres qui peuvent être représentés au format UTF-8, ainsi que les caractères suivants : `+ - = . _ : /`

Table des matières

Key

Clé de la balise (chaîne). La clé ne peut pas commencer par `aws:`.

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 128.

Modèle : `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Type : chaîne

Obligatoire : oui

Value

Valeur de la clé.

Contraintes de longueur : longueur maximale de 256.

Modèle : `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Type : chaîne

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

LegalHold

Service : AWS Backup

Une conservation légale est un outil administratif qui permet d'empêcher la suppression de sauvegardes pendant une conservation. Tant que la conservation est en place, les sauvegardes sous conservation ne peuvent pas être supprimées et les politiques de cycle de vie susceptibles de modifier le statut des sauvegardes (comme le passage à un stockage à froid) sont retardées jusqu'à ce que la conservation légale soit levée. Une sauvegarde peut avoir plusieurs conservations légales. Des conservations légales sont appliquées à une ou plusieurs sauvegardes (également appelées points de récupération). Ces sauvegardes peuvent être filtrées par type de ressource et par ID de ressource.

Table des matières

CancellationDate

Heure à laquelle le blocage légal a été annulé.

Type : Timestamp

Obligatoire : non

CreationDate

Heure à laquelle le blocage légal a été créé.

Type : Timestamp

Obligatoire : non

Description

Description d'une détention légale.

Type : chaîne

Obligatoire : non

LegalHoldArn

L'Amazon Resource Name (ARN) du support légal ; par exemple,`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

LegalHoldId

L'identifiant de la retenue légale.

Type : chaîne

Obligatoire : non

Status

État de la suspension légale.

Type : chaîne

Valeurs valides : `CREATING | ACTIVE | CANCELING | CANCELED`

Obligatoire : non

Title

Titre d'une détention légale.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Lifecycle

Service : AWS Backup

Spécifie la période, en jours, avant qu'un point de restauration ne passe en stockage à froid ou ne soit supprimé.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, sur la console, le paramètre de rétention doit être supérieur de 90 jours au réglage de transition vers le froid après plusieurs jours. Le paramètre de transition vers le froid après plusieurs jours ne peut pas être modifié une fois qu'une sauvegarde est passée au mode froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Pour supprimer le cycle de vie et les périodes de rétention existants et conserver vos points de restauration indéfiniment, spécifiez -1 pour `MoveToColdStorageAfterDays` et`DeleteAfterDays`.

Table des matières

DeleteAfterDays

Nombre de jours après sa création pendant lesquels un point de récupération est supprimé. Cette valeur doit être postérieure d'au moins 90 jours au nombre de jours spécifié dans`MoveToColdStorageAfterDays`.

Type : long

Obligatoire : non

MoveToColdStorageAfterDays

Nombre de jours après sa création pendant lesquels un point de récupération est déplacé vers une chambre froide.

Type : long

Obligatoire : non

OptInToArchiveForSupportedResources

Si la valeur est vraie, votre plan de sauvegarde fait passer les ressources prises en charge au niveau de stockage d'archivage (froid) conformément à vos paramètres de cycle de vie.

Type : booléen

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ProtectedResource

Service : AWS Backup

Structure contenant des informations sur une ressource sauvegardée.

Table des matières

LastBackupTime

Date et heure de la dernière sauvegarde d'une ressource, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastBackupTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastBackupVaultArn

L'ARN (Amazon Resource Name) du coffre de sauvegarde qui contient le point de restauration de sauvegarde le plus récent.

Type : chaîne

Obligatoire : non

LastRecoveryPointArn

L'ARN (Amazon Resource Name) du point de récupération le plus récent.

Type : chaîne

Obligatoire : non

ResourceArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ProtectedResourceConditions

Service : AWS Backup

Les conditions que vous définissez pour les ressources dans votre plan de test de restauration à l'aide de balises.

Par exemple, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Les opérateurs de condition sont sensibles à la casse.

Table des matières

StringEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées avec la même valeur. Également appelé « correspondance exacte ».

Type : tableau d'objets KeyValue

Obligatoire : non

StringNotEquals

Filtre les valeurs de vos ressources balisées uniquement pour les ressources que vous avez balisées qui n'ont pas la même valeur. Également appelé « correspondance négative ».

Type : tableau d'objets KeyValue

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RecoveryPointByBackupVault

Service : AWS Backup

Contient des informations détaillées sur les points de récupération stockés dans un coffre-fort de sauvegarde.

Table des matières

BackupSizeInBytes

Taille d'une sauvegarde, en octets.

Type : long

Obligatoire : non

BackupVaultArn

Un ARN qui identifie de façon unique un coffre-fort de sauvegarde ; par exemple, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Type : chaîne

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : non

CalculatedLifecycle

Un objet `CalculatedLifecycle` contenant des horodatages `DeleteAt` et `MoveToColdStorageAt`.

Type : objet CalculatedLifecycle

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CompositeMemberIdentifier

Identifiant d'une ressource au sein d'un groupe composite, tel qu'un point de récupération imbriqué (enfant) appartenant à une pile composite (parent). L'ID est transféré à partir de l'ID logique au sein d'une pile.

Type : chaîne

Obligatoire : non

CreatedBy

Contient des informations d'identification relatives à la création d'un point de récupération, dont les `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` et `BackupRuleId` du plan de sauvegarde utilisé pour le créer.

Type : objet RecoveryPointCreator

Obligatoire : non

CreationDate

Date et heure de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

EncryptionKeyArn

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : chaîne

Obligatoire : non

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

IsEncrypted

Valeur booléenne renvoyée comme `TRUE` si le point de récupération spécifié était chiffré ou `FALSE` s'il n'était pas chiffré.

Type : booléen

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'un point de récupération parent (composite).

Type : booléen

Obligatoire : non

LastRestoreTime

Date et heure de la dernière restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastRestoreTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

Lifecycle

Le cycle de vie définit le moment où une ressource protégée est transférée vers le stockage à froid et sa date d'expiration. AWS Backup effectue la transition et fait expirer les sauvegardes automatiquement en fonction du cycle de vie que vous définissez.

Les sauvegardes transférées vers un stockage à froid doivent être stockées dans le stockage à froid pendant au moins 90 jours. Par conséquent, le paramètre « rétention » doit être supérieur de 90 jours au paramètre « nombre de jours avant transfert vers stockage à froid ». Le paramètre « transition to cold after days (nombre de jours avant transfert vers stockage à froid) » ne peut pas être modifié après le transfert d'une sauvegarde vers un stockage à froid.

Les types de ressources pouvant passer au stockage à froid sont répertoriés dans le tableau Disponibilité des fonctionnalités par ressource. AWS Backup ignore cette expression pour les autres types de ressources.

Type : objet Lifecycle

Obligatoire : non

ParentRecoveryPointArn

Le nom de ressource Amazon (ARN) du point de récupération parent (composite).

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

ResourceArn

Un ARN qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource enregistrée comme point de récupération ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

SourceBackupVaultArn

Le coffre-fort de sauvegarde à partir duquel le point de récupération a été initialement copié. Si le point de récupération est restauré sur le même compte, cette valeur sera `null`.

Type : chaîne

Obligatoire : non

Status

Code de statut spécifiant l'état du point de récupération.

Type : chaîne

Valeurs valides : `COMPLETED | PARTIAL | DELETING | EXPIRED`

Obligatoire : non

StatusMessage

Un message expliquant l'état actuel du point de récupération.

Type : chaîne

Obligatoire : non

VaultType

Type de coffre-fort dans lequel le point de restauration décrit est stocké.

Type : chaîne

Valeurs valides : `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RecoveryPointByResource

Service : AWS Backup

Contient des informations détaillées sur un point de récupération enregistré.

Table des matières

BackupSizeBytes

Taille d'une sauvegarde, en octets.

Type : long

Obligatoire : non

BackupVaultName

Le nom d'un conteneur logique où les sauvegardes sont stockées. Les coffres-forts de sauvegarde sont identifiés par des noms spécifiques pour le compte utilisé pour les créer et la région AWS dans laquelle ils sont créés.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : non

CreationDate

Date et heure de création d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

EncryptionKeyArn

Chiffrement côté serveur utilisé pour protéger vos sauvegardes ; par exemple, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Type : chaîne

Obligatoire : non

IsParent

Il s'agit d'une valeur booléenne indiquant qu'il s'agit d'un point de récupération parent (composite).

Type : booléen

Obligatoire : non

ParentRecoveryPointArn

Le nom de ressource Amazon (ARN) du point de récupération parent (composite).

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

ResourceName

Nom non unique de la ressource appartenant à la sauvegarde spécifiée.

Type : chaîne

Obligatoire : non

Status

Code de statut spécifiant l'état du point de récupération.

Type : chaîne

Valeurs valides : `COMPLETED | PARTIAL | DELETING | EXPIRED`

Obligatoire : non

StatusMessage

Un message expliquant l'état actuel du point de récupération.

Type : chaîne

Obligatoire : non

VaultType

Type de coffre-fort dans lequel le point de restauration décrit est stocké.

Type : chaîne

Valeurs valides : `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RecoveryPointCreator

Service : AWS Backup

Contient des informations sur le plan de sauvegarde et la règle AWS Backup utilisés pour lancer la sauvegarde du point de restauration.

Table des matières

BackupPlanArn

Amazon Resource Name (ARN) qui identifie de façon unique un plan de secours ; par exemple, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Type : chaîne

Obligatoire : non

BackupPlanId

Identifie de façon unique un plan de secours.

Type : chaîne

Obligatoire : non

BackupPlanVersion

Les ID de version sont des chaînes codées en Unicode, UTF-8 et générées de façon aléatoire qui contiennent au maximum 1 024 octets. Ils ne peuvent pas être modifiés.

Type : chaîne

Obligatoire : non

BackupRuleId

Identifie de manière unique une règle utilisée pour planifier la sauvegarde d'une sélection de ressources.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RecoveryPointMember

Service : AWS Backup

Il s'agit d'un point de récupération qui est un point de récupération enfant (imbriqué) d'un point de récupération parent (composite). Ces points de récupération peuvent être dissociés de leur point de récupération parent (composite), auquel cas ils n'en seront plus membres.

Table des matières

BackupVaultName

Le nom du coffre de sauvegarde (le conteneur logique dans lequel les sauvegardes sont stockées).

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatoire : non

RecoveryPointArn

Le nom de ressource Amazon (ARN) du point de récupération parent (composite).

Type : chaîne

Obligatoire : non

ResourceArn

Le nom de ressource Amazon (ARN) qui identifie de manière unique une ressource enregistrée.

Type : chaîne

Obligatoire : non

ResourceType

Type de AWS ressource enregistré en tant que point de récupération.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RecoveryPointSelection

Service : AWS Backup

Cela spécifie les critères d'attribution d'un ensemble de ressources, tels que les types de ressources ou les coffres-forts de sauvegarde.

Table des matières

DateRange

Il s'agit d'un filtre de ressources contenant FromDate : DateTime et ToDate : DateTime. Les deux valeurs sont requises. Les DateTime valeurs futures ne sont pas autorisées.

La date et l'heure sont au format Unix et au temps universel coordonné (UTC), et leur précision est de l'ordre de la milliseconde (les millisecondes sont facultatives). Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : objet DateRange

Obligatoire : non

ResourceIdentifiers

Il s'agit des ressources incluses dans la sélection des ressources (y compris le type de ressources et les coffres).

Type : tableau de chaînes

Obligatoire : non

VaultNames

Il s'agit des noms des coffres-forts dans lesquels sont contenus les points de récupération sélectionnés.

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportDeliveryChannel

Service : AWS Backup

Contient des informations issues de votre plan de rapport sur l'endroit et la manière de diffuser vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Table des matières

S3BucketName

Nom unique du compartiment S3 dans lequel se trouvent vos rapports.

Type : chaîne

Obligatoire : oui

Formats

Le format de vos rapports : `CSV`, `JSON`, ou les deux. Si aucune valeur n'est spécifiée, le format par défaut est `CSV`.

Type : tableau de chaînes

Obligatoire : non

S3KeyPrefix

Le préfixe indiquant où AWS Backup Audit Manager envoie vos rapports à Amazon S3. Le préfixe est cette partie du chemin suivant : s3 ://your-bucket-name/`prefix`/backup/us-west-2/year/month/day/report-Name. S'il n'est pas spécifié, il n'y a pas de préfixe.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2

- AWS SDK pour Ruby V3

ReportDestination

Service : AWS Backup

Contient des informations issues de votre tâche de rapport concernant la destination de votre rapport.

Table des matières

S3BucketName

Nom unique du compartiment Amazon S3 qui reçoit vos rapports.

Type : chaîne

Obligatoire : non

S3Keys

Clé d'objet qui identifie de façon unique vos rapports dans votre compartiment S3.

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportJob

Service : AWS Backup

Contient des informations détaillées sur une tâche de rapport. Une tâche de rapport compile un rapport sur la base d'un plan de rapport et le publie sur Amazon S3.

Table des matières

CompletionTime

Date et heure de fin d'une tâche de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreationTime

Date et heure de création d'une tâche de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ReportDestination

Le nom du compartiment S3 et les clés S3 de la destination où la tâche de rapport publie le rapport.

Type : objet ReportDestination

Obligatoire : non

ReportJobId

Identifiant de la tâche de rapport. Une chaîne codée en Unicode, UTF-8 unique et générée de façon aléatoire qui contiennent au maximum 1 024 octets. Les ID de tâche de rapport ne peuvent pas être modifiés.

Type : chaîne

Obligatoire : non

ReportPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ReportTemplate

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Type : chaîne

Obligatoire : non

Status

Statut d'une tâche de rapports. Les statuts sont les suivants :

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` signifie que le rapport est disponible pour examen à la destination que vous avez désignée. Si le statut est `FAILED`, examinez le `StatusMessage` pour en connaître la raison.

Type : chaîne

Obligatoire : non

StatusMessage

Un message expliquant le statut de la tâche de rapport.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportPlan

Service : AWS Backup

Contient des informations détaillées sur un plan de rapport.

Table des matières

CreationTime

Date et heure de création d'un plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

DeploymentStatus

Le statut de déploiement d'un plan de rapport. Les statuts sont les suivants :

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED`

Type : chaîne

Obligatoire : non

LastAttemptedExecutionTime

Date et heure de la dernière tentative d'exécution d'une tâche de rapport associée à ce plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastAttemptedExecutionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastSuccessfulExecutionTime

Date et heure de la dernière exécution réussie d'une tâche de rapport associée à ce plan de rapport, au format Unix et au format UTC (temps universel coordonné). La valeur de `LastSuccessfulExecutionTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ReportDeliveryChannel

Contient des informations sur l'endroit et la manière de diffuser vos rapports, en particulier le nom de votre compartiment Amazon S3, le préfixe de clé S3 et les formats de vos rapports.

Type : objet ReportDeliveryChannel

Obligatoire : non

ReportPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

ReportPlanDescription

Une description facultative du plan de rapport avec 1 024 caractères au maximum.

Type : chaîne

Contraintes de longueur : longueur minimum de 0. Longueur maximum de 1024.

Modèle : `.*\S.*`

Obligatoire : non

ReportPlanName

Le nom unique du plan de rapport. Ce nom contient entre 1 et 256 caractères, commence par une lettre et est composé de lettres (a à z, A à Z), de chiffres (0 à 9) et de traits de soulignement (_).

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 256.

Modèle : `[a-zA-Z][_a-zA-Z0-9]*`

Obligatoire : non

ReportSetting

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Si le modèle de rapport est `RESOURCE_COMPLIANCE_REPORT` ou`CONTROL_COMPLIANCE_REPORT`, cette ressource d'API décrit également la couverture du rapport par Régions AWS et les frameworks.

Type : objet ReportSetting

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

ReportSetting

Service : AWS Backup

Contient des informations détaillées sur un paramètre de rapport.

Table des matières

ReportTemplate

Identifie le modèle de rapport pour le rapport. Les rapports sont créés à l'aide d'un modèle de rapport. Les modèles de rapport sont les suivants :

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Type : chaîne

Obligatoire : oui

Accounts

Il s'agit des comptes à inclure dans le rapport.

Utilisez la valeur de chaîne de `ROOT` pour inclure toutes les unités organisationnelles.

Type : tableau de chaînes

Obligatoire : non

FrameworkArns

Amazon Resource Name (ARN) des cadres couverts par un rapport.

Type : tableau de chaînes

Obligatoire : non

NumberOfFrameworks

Le nombre de frameworks couverts par un rapport.

Type : entier

Obligatoire : non

OrganizationUnits

Il s'agit des unités organisationnelles à inclure dans le rapport.

Type : tableau de chaînes

Obligatoire : non

Regions

Il s'agit des régions qui seront incluses dans le rapport.

Utilisez le caractère générique comme valeur de chaîne pour inclure toutes les régions.

Type : tableau de chaînes

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreJobCreator

Service : AWS Backup

Contient des informations sur le plan de test de la restauration utilisé par AWS Backup pour lancer la tâche de restauration.

Table des matières

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un plan de test de la restauration.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreJobsListMember

Service : AWS Backup

Contient des métadonnées relatives à une tâche de restauration.

Table des matières

AccountId

ID de compte du propriétaire de la tâche de restauration.

Type : chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

BackupSizeInBytes

Taille, en octets, de la ressource restaurée.

Type : long

Obligatoire : non

CompletionDate

Date et heure de fin d'une tâche de restauration d'un point de récupération, au format Unix et au format UTC (temps universel coordonné). La valeur de `CompletionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

CreatedBy

Contient des informations d’identification relatives à la création d’une tâche de restauration.

Type : objet RestoreJobCreator

Obligatoire : non

CreatedResourceArn

Un Amazon Resource Name (ARN) qui identifie de façon unique une ressource. Le format de l'ARN dépend du type de ressource.

Type : chaîne

Obligatoire : non

CreationDate

Date et heure de création d'une tâche de restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

DeletionStatus

Cela indique le statut des données générées par le test de la restauration. Le statut peut être `Deleting`, `Failed` ou `Successful`.

Type : chaîne

Valeurs valides : `DELETING | FAILED | SUCCESSFUL`

Obligatoire : non

DeletionStatusMessage

Cela décrit le statut de suppression de la tâche de restauration.

Type : chaîne

Obligatoire : non

ExpectedCompletionTimeMinutes

Durée en minutes prévue d'une tâche de restauration d'un point de récupération.

Type : long

Obligatoire : non

IamRoleArn

Spécifie l'ARN du rôle IAM utilisé pour créer le point de récupération cible ; par exemple, `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

PercentDone

Contient une estimation du pourcentage d'achèvement d'une tâche au moment où le statut de la tâche a été demandé.

Type : chaîne

Obligatoire : non

RecoveryPointArn

Un ARN qui identifie de façon unique un point de récupération ; par exemple, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Type : chaîne

Obligatoire : non

RecoveryPointCreationDate

Date à laquelle un point de récupération a été créé.

Type : Timestamp

Obligatoire : non

ResourceType

Le type de ressource des tâches de restauration répertoriées ; par exemple, un volume Amazon Elastic Block Store (Amazon EBS) ou une base de données Amazon Relational Database Service (Amazon RDS). Pour les sauvegardes Windows Volume Shadow Copy Service (VSS), le seul type de ressource pris en charge est Amazon EC2.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

RestoreJobId

Identifie de manière unique la tâche qui restaure un point de récupération.

Type : chaîne

Obligatoire : non

Status

Code d'état spécifiant l'état de la tâche initiée par AWS Backup pour restaurer un point de restauration.

Type : chaîne

Valeurs valides : `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

Obligatoire : non

StatusMessage

Message détaillé expliquant le statut de la tâche de restauration d'un point de récupération.

Type : chaîne

Obligatoire : non

ValidationStatus

État de la validation exécutée sur la tâche de restauration indiquée.

Type : chaîne

Valeurs valides : `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Obligatoire : non

ValidationStatusMessage

Cela décrit le statut de la validation exécutée sur la tâche de restauration indiquée.

Type : chaîne

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreJobSummary

Service : AWS Backup

Il s’agit d’un résumé des tâches de restauration créées ou en cours d’exécution au cours des 30 derniers jours.

Le résumé renvoyé peut contenir les éléments suivants : région, compte, État ResourceType, MessageCategory, StartTime, EndTime, et nombre de tâches incluses.

Table des matières

AccountId

L’ID de compte qui possède les tâches figurant dans le résumé.

Type : chaîne

Modèle : `^[0-9]{12}$`

Obligatoire : non

Count

La valeur du nombre de tâches dans un résumé des tâches.

Type : entier

Obligatoire : non

EndTime

La valeur de l’heure au format numérique de l’heure de fin d’une tâche.

Cette valeur est l’heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

Region

Les AWS régions figurant dans le résumé du poste.

Type : chaîne

Obligatoire : non

ResourceType

Cette valeur est le nombre de tâches pour le type de ressource spécifié. La demande `GetSupportedResourceTypes` renvoie des chaînes pour les types de ressources pris en charge.

Type : chaîne

Modèle : `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatoire : non

StartTime

La valeur de l'heure au format numérique de l'heure de début d'une tâche.

Cette valeur est l'heure au format Unix, en temps universel coordonné (UTC) et précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

State

Cette valeur est le nombre de tâches pour les tâches ayant l'état spécifié.

Type : chaîne

Valeurs valides : `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingPlanForCreate

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

RecoveryPointSelection

`RecoveryPointSelection`possède cinq paramètres (trois obligatoires et deux facultatifs). Les valeurs que vous spécifiez déterminent le point de récupération inclus dans le test de restauration. Vous devez indiquer `Algorithm` si vous voulez le dernier point de récupération dans votre répertoire `SelectionWindowDays` ou si vous voulez un point de récupération aléatoire, et vous devez indiquer dans `IncludeVaults` quels coffres-forts les points de récupération peuvent être choisis.

`Algorithm`(obligatoire) Valeurs valides : « `LATEST_WITHIN_WINDOW` » ou « `RANDOM_WITHIN_WINDOW` ».

`Recovery point types`(obligatoire) Valeurs valides : « `SNAPSHOT` » et/ou « `CONTINUOUS` ». Incluez `SNAPSHOT` pour restaurer uniquement les points de restauration des instantanés ; incluez `CONTINUOUS` pour restaurer les points de restauration continus (restauration ponctuelle/PITR) ; utilisez les deux pour restaurer un instantané ou un point de restauration continue. Le point de récupération sera déterminé par la valeur de`Algorithm`.

`IncludeVaults`(obligatoire). Vous devez inclure un ou plusieurs coffres-forts de sauvegarde. Utilisez le caractère générique ["*"] ou des ARN spécifiques.

`SelectionWindowDays`(facultatif) La valeur doit être un entier (en jours) compris entre 1 et 365. Si elle n'est pas incluse, la valeur par défaut est. `30`

`ExcludeVaults`(facultatif). Vous pouvez choisir de saisir un ou plusieurs ARN de sauvegarde spécifiques pour exclure le contenu de ces coffres-forts de l'éligibilité à la restauration. Vous pouvez également inclure une liste de sélecteurs. Si ce paramètre et sa valeur ne sont pas inclus, la valeur par défaut est une liste vide.

Type : objet RestoreTestingRecoveryPointSelection

Obligatoire : oui

RestoreTestingPlanName

RestoreTestingPlanName Il s'agit d'une chaîne unique qui est le nom du plan de test de restauration. Elle ne peut pas être modifiée après sa création et elle doit être composée uniquement de caractères alphanumériques et de traits de soulignement.

Type : chaîne

Obligatoire : oui

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté.

Type : chaîne

Obligatoire : oui

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d'un test de la restauration avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingPlanForGet

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

CreationTime

Date et heure de création d'un plan de test de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

RecoveryPointSelection

Les critères spécifiés d'attribution d'un ensemble de ressources, tels que les types de point de récupération ou les coffres-forts de sauvegarde.

Type : objet RestoreTestingRecoveryPointSelection

Obligatoire : oui

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un plan de test de la restauration.

Type : chaîne

Obligatoire : oui

RestoreTestingPlanName

Nom du plan de test de restauration.

Type : chaîne

Obligatoire : oui

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté.

Type : chaîne

Obligatoire : oui

CreatorRequestId

Cela identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Si la demande inclut un `CreatorRequestId` qui correspond à un plan de sauvegarde existant, ce plan est renvoyé. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

LastExecutionTime

La dernière fois qu'un test de la restauration a été exécuté avec le plan de test de la restauration spécifié. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de `LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastUpdateTime

Date et heure de mise à jour du plan de test de la restauration. Cette mise à jour est au format Unix et UTC (temps universel coordonné). La valeur de `LastUpdateTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d'un test de la restauration avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingPlanForList

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

CreationTime

Date et heure de création d'un plan de test de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

RestoreTestingPlanArn

Un Amazon Resource Name (ARN) qui identifie de façon unique un plan de test de la restauration.

Type : chaîne

Obligatoire : oui

RestoreTestingPlanName

Nom du plan de test de restauration.

Type : chaîne

Obligatoire : oui

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté.

Type : chaîne

Obligatoire : oui

LastExecutionTime

La dernière fois qu'un test de la restauration a été exécuté avec le plan de test de la restauration spécifié. Date et heure au format Unix et UTC (temps universel coordonné). La valeur de

`LastExecutionDate` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

LastUpdateTime

Date et heure de mise à jour du plan de test de la restauration. Cette mise à jour est au format Unix et UTC (temps universel coordonné). La valeur de `LastUpdateTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : non

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d’un test de la restauration avant qu’une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingPlanForUpdate

Service : AWS Backup

Il contient des métadonnées relatives à un plan de test de la restauration.

Table des matières

RecoveryPointSelection

Obligatoire : `Algorithm` ; `RecoveryPointTypes` ; `IncludeVaults` (un ou plusieurs).

Facultatif : SelectionWindowDays(« 30 » s'il n'est pas spécifié) ; `ExcludeVaults` (la valeur par défaut est une liste vide si elle n'est pas répertoriée).

Type : objet RestoreTestingRecoveryPointSelection

Obligatoire : non

ScheduleExpression

Expression CRON dans le fuseau horaire spécifié lorsqu'un plan de test de la restauration est exécuté.

Type : chaîne

Obligatoire : non

ScheduleExpressionTimezone

Facultatif. Le fuseau horaire dans lequel l'expression de planification est définie. Par défaut, ScheduleExpressions ils sont en UTC. Vous pouvez le modifier pour un fuseau horaire spécifique.

Type : chaîne

Obligatoire : non

StartWindowHours

La valeur par défaut est de 24 heures.

Valeur en heures après la planification d'un test de la restauration avant qu'une tâche soit annulée si elle ne démarre pas correctement. Cette valeur est facultative. Si cette valeur est incluse, la valeur maximale de ce paramètre est de 168 heures (une semaine).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingRecoveryPointSelection

Service : AWS Backup

`RecoveryPointSelection`possède cinq paramètres (trois obligatoires et deux facultatifs). Les valeurs que vous spécifiez déterminent le point de récupération inclus dans le test de restauration. Vous devez indiquer `Algorithm` si vous voulez le dernier point de récupération dans votre répertoire `SelectionWindowDays` ou si vous voulez un point de récupération aléatoire, et vous devez indiquer dans `IncludeVaults` quels coffres-forts les points de récupération peuvent être choisis.

`Algorithm`(obligatoire) Valeurs valides : « `LATEST_WITHIN_WINDOW` » ou « `RANDOM_WITHIN_WINDOW` ».

`Recovery point types`(obligatoire) Valeurs valides : « `SNAPSHOT` » et/ou « `CONTINUOUS` ». Incluez `SNAPSHOT` pour restaurer uniquement les points de restauration des instantanés ; incluez `CONTINUOUS` pour restaurer les points de restauration continus (restauration ponctuelle/PITR) ; utilisez les deux pour restaurer un instantané ou un point de restauration continue. Le point de récupération sera déterminé par la valeur de`Algorithm`.

`IncludeVaults`(obligatoire). Vous devez inclure un ou plusieurs coffres-forts de sauvegarde. Utilisez le caractère générique ["*"] ou des ARN spécifiques.

`SelectionWindowDays`(facultatif) La valeur doit être un entier (en jours) compris entre 1 et 365. Si elle n'est pas incluse, la valeur par défaut est. `30`

`ExcludeVaults`(facultatif). Vous pouvez choisir de saisir un ou plusieurs ARN de coffre-fort de sauvegarde spécifiques pour exclure le contenu de ces coffres-forts de l'éligibilité à la restauration. Vous pouvez également inclure une liste de sélecteurs. Si ce paramètre et sa valeur ne sont pas inclus, la valeur par défaut est une liste vide.

Table des matières

Algorithm

> Les valeurs acceptables incluent « LATEST_WITHIN_WINDOW » ou « RANDOM_WITHIN_WINDOW »
>
> Type : chaîne
>
> Valeurs valides : `LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW`
>
> Obligatoire : non

ExcludeVaults

Les valeurs acceptées incluent des ARN spécifiques ou une liste de sélecteurs. La valeur par défaut est une liste vide si elle n'est pas répertoriée.

Type : tableau de chaînes

Obligatoire : non

IncludeVaults

Les valeurs acceptées incluent un caractère générique ["*"] ou des ARN spécifiques ou un remplacement par un ARN générique ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...]

Type : tableau de chaînes

Obligatoire : non

RecoveryPointTypes

Il s'agit des types de points de récupération.

Incluez `SNAPSHOT` pour restaurer uniquement les points de restauration des instantanés ; incluez `CONTINUOUS` pour restaurer les points de restauration continus (restauration ponctuelle/PITR) ; utilisez les deux pour restaurer un instantané ou un point de restauration continue. Le point de récupération sera déterminé par la valeur de`Algorithm`.

Type : tableau de chaînes

Valeurs valides : `CONTINUOUS | SNAPSHOT`

Obligatoire : non

SelectionWindowDays

Les valeurs acceptées sont des entiers compris entre 1 et 365.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingSelectionForCreate

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration spécifique.

ProtectedResourceType est requis, comme Amazon EBS ou Amazon EC2.

Cela comprend `RestoreTestingSelectionName`, `ProtectedResourceType` et l'un des éléments suivants :

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Chaque type de ressource protégée peut avoir une seule valeur.

Une sélection de tests de la restauration peut inclure une valeur générique (« * ») pour `ProtectedResourceArns` avec `ProtectedResourceConditions`. Vous pouvez également inclure jusqu'à 30 ARN de ressources protégées spécifiques dans `ProtectedResourceArns`.

Des exemples `ProtectedResourceConditions` incluent `StringEquals` et `StringNotEquals`.

Table des matières

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : oui

ProtectedResourceType

Type de AWS ressource inclus dans une sélection de test de restauration ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Les types de ressources pris en charge incluent :

- `Aurora` pour Amazon Aurora
- `DocumentDB` pour Amazon DocumentDB (compatible avec MongoDB)

- `DynamoDB` pour Amazon DynamoDB
- `EBS` pour Amazon Elastic Block Store
- `EC2` pour Amazon Elastic Compute Cloud
- `EFS` pour Amazon Elastic File System
- `FSx` pour Amazon FSx
- `Neptune` pour Amazon Neptune
- `RDS` pour Amazon Relational Database Service
- `S3` pour Simple Storage Service (Amazon S3)

Type : chaîne

Obligatoire : oui

RestoreTestingSelectionName

Nom unique de la sélection de tests de restauration appartenant au plan de test de restauration associé.

Type : chaîne

Obligatoire : oui

ProtectedResourceArns

Chaque ressource protégée peut être filtrée en fonction de ses ARN spécifiques, tels que `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` ou par un caractère générique : `ProtectedResourceArns: ["*"]`, mais pas les deux.

Type : tableau de chaînes

Obligatoire : non

ProtectedResourceConditions

Si vous avez inclus le caractère générique ProtectedResourceArns, vous pouvez inclure des conditions de ressource, telles que`ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]`.

Type : objet ProtectedResourceConditions

Obligatoire : non

RestoreMetadataOverrides

Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Les valeurs de clé ne sont pas sensibles à la casse.

Consultez la liste complète des métadonnées déduites des tests de la restauration.

Type : mappage chaîne/chaîne

Obligatoire : non

ValidationWindowHours

Il s'agit du nombre d'heures (1 à 168) disponibles pour exécuter un script de validation sur les données. Les données seront supprimées à la fin du script de validation ou à la fin de la période de rétention spécifiée, selon la première éventualité.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingSelectionForGet

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration.

Table des matières

CreationTime

Date et heure de création d'une sélection de tests de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : oui

ProtectedResourceType

Type de AWS ressource inclus dans une sélection de ressources destinée à tester ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Type : chaîne

Obligatoire : oui

RestoreTestingPlanName

RestoreTestingPlanName Il s'agit d'une chaîne unique qui est le nom du plan de test de restauration.

Type : chaîne

Obligatoire : oui

RestoreTestingSelectionName

Nom unique de la sélection de tests de restauration appartenant au plan de test de restauration associé.

Type : chaîne

Obligatoire : oui

CreatorRequestId

Cela identifie la demande et permet de réessayer les demandes ayant échoué sans risque d'exécuter l'opération deux fois. Si la demande inclut un `CreatorRequestId` qui correspond à un plan de sauvegarde existant, ce plan est renvoyé. Ce paramètre est facultatif.

S'il est utilisé, ce paramètre doit contenir de 1 à 50 caractères alphanumériques ou « -_. » caractères.

Type : chaîne

Obligatoire : non

ProtectedResourceArns

Vous pouvez inclure des ARN spécifiques, tels que `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` ou vous pouvez inclure un caractère générique : `ProtectedResourceArns: ["*"]`, mais pas les deux.

Type : tableau de chaînes

Obligatoire : non

ProtectedResourceConditions

Dans une sélection de tests de ressources, ce paramètre filtre en fonction de conditions spécifiques telles que `StringEquals` ou `StringNotEquals`.

Type : objet ProtectedResourceConditions

Obligatoire : non

RestoreMetadataOverrides

Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Les valeurs de clé ne sont pas sensibles à la casse.

Consultez la liste complète des métadonnées déduites des tests de la restauration.

Type : mappage chaîne/chaîne

Obligatoire : non

ValidationWindowHours

Il s'agit du nombre d'heures (1 à 168) disponibles pour exécuter un script de validation sur les données. Les données seront supprimées à la fin du script de validation ou à la fin de la période de rétention spécifiée, selon la première éventualité.

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingSelectionForList

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration.

Table des matières

CreationTime

Date et heure de création d'une sélection de tests de la restauration, au format Unix et au format UTC (temps universel coordonné). La valeur de `CreationTime` est précise en millisecondes. Par exemple, la valeur 1516925490,087 représente le vendredi 26 janvier 2018 à 00 h 11 m 30,087 s.

Type : Timestamp

Obligatoire : oui

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : oui

ProtectedResourceType

Type de AWS ressource inclus dans une sélection de test de restauration ; par exemple, un volume Amazon EBS ou une base de données Amazon RDS.

Type : chaîne

Obligatoire : oui

RestoreTestingPlanName

Chaîne unique qui est le nom du plan de test de la restauration.

Le nom ne peut pas être modifié après la création. Le nom doit contenir uniquement des caractères alphanumériques et des traits de soulignement. La longueur maximale est de 50.

Type : chaîne

Obligatoire : oui

RestoreTestingSelectionName

Nom unique d’une sélection de tests de la restauration.

Type : chaîne

Obligatoire : oui

ValidationWindowHours

Cette valeur représente la durée, en heures, pendant laquelle les données sont conservées après un test de la restauration afin que la validation facultative puisse être effectuée.

La valeur acceptée est un entier compris entre 0 et 168 (l’équivalent horaire de sept jours).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

RestoreTestingSelectionForUpdate

Service : AWS Backup

Cela contient des métadonnées relatives à une sélection de tests de la restauration.

Table des matières

IamRoleArn

L'Amazon Resource Name (ARN) du rôle IAM utilisé par AWS Backup pour créer la ressource cible ; par exemple : `arn:aws:iam::123456789012:role/S3Access`.

Type : chaîne

Obligatoire : non

ProtectedResourceArns

Vous pouvez inclure une liste d'ARN spécifiques, tels que `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` ou vous pouvez inclure un caractère générique : `ProtectedResourceArns: ["*"]`, mais pas les deux.

Type : tableau de chaînes

Obligatoire : non

ProtectedResourceConditions

Les conditions que vous définissez pour les ressources dans votre plan de test de restauration à l'aide de balises.

Par exemple, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Les opérateurs de condition sont sensibles à la casse.

Type : objet ProtectedResourceConditions

Obligatoire : non

RestoreMetadataOverrides

Vous pouvez remplacer certaines clés de métadonnées de restauration en incluant le paramètre `RestoreMetadataOverrides` dans le corps de `RestoreTestingSelection`. Les valeurs de clé ne sont pas sensibles à la casse.

Consultez la liste complète des métadonnées déduites des tests de la restauration.

Type : mappage chaîne/chaîne

Obligatoire : non

ValidationWindowHours

Cette valeur représente la durée, en heures, pendant laquelle les données sont conservées après un test de la restauration afin que la validation facultative puisse être effectuée.

La valeur acceptée est un entier compris entre 0 et 168 (l'équivalent horaire de sept jours).

Type : entier

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

AWS Backup gateway

Les types de données suivants sont pris en charge par AWS Backup gateway :

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine

- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

Service : AWS Backup gateway

Décrit un intervalle limite de débit de bande passante pour une passerelle. Une planification de limite de débit de la bande passante comprend un ou plusieurs intervalles de limite de débit de bande passante. Un intervalle de limite de bande passante définit une période pendant un ou plusieurs jours de la semaine, pendant laquelle des limites de débit de bande passante sont spécifiées pour le chargement, le téléchargement ou les deux.

Table des matières

DaysOfWeek

Composante des jours de la semaine de l'intervalle limite de débit de bande passante, représentée par des nombres ordinaux compris entre 0 et 6, où 0 représente le dimanche et 6 le samedi.

Type : tableau d'entiers

Membres du tableau : Nombre minimum de 1 élément. Nombre maximal de 7 éléments.

Plage valide : Valeur minimum de 0. Valeur maximale de 6.

Obligatoire : oui

EndHourOfDay

Heure de la journée pendant laquelle l'intervalle de limite de débit de bande passante est terminé.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

EndMinuteOfHour

Minute de l'heure à laquelle l'intervalle de limite de débit de bande passante est terminé.

> **Important**
>
> L'intervalle de limite de taux de bande passante prend fin à la fin de la minute. Pour terminer un intervalle à la fin d'une heure, utilisez la valeur 59.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

StartHourOfDay

Heure de la journée pendant laquelle l'intervalle de limite de débit de bande passante commence.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

StartMinuteOfHour

Minute de l'heure à laquelle l'intervalle de limite de débit de bande passante commence. L'intervalle commence au début de cette minute. Pour commencer un intervalle exactement au début de l'heure, utilisez la valeur `0`.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

AverageUploadRateLimitInBitsPerSec

La composante limite du débit de téléchargement moyen de l'intervalle limite de débit de bande passante, en bits par seconde. Ce champ n'apparaît pas dans la réponse si la limite de débit de téléchargement n'est pas définie.

Type : long

Plage valide : valeur minimum de 51 200. Valeur maximale de 8 000 000 000 000.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Gateway

Service : AWS Backup gateway

Une passerelle est une appliance de AWS Backup passerelle qui s'exécute sur le réseau du client pour fournir une connectivité fluide au stockage des sauvegardes dans le AWS cloud.

Table des matières

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez cette `ListGateways` opération pour renvoyer une liste de passerelles pour votre compte et Région AWS.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : non

GatewayDisplayName

Le nom d'affichage de la passerelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

GatewayType

Le type de passerelle.

Type : chaîne

Valeurs valides : `BACKUP_VM`

Obligatoire : non

HypervisorId

L'ID d'hyperviseur de la passerelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Obligatoire : non

LastSeenTime

La dernière fois que la AWS Backup passerelle a communiqué avec la passerelle, au format Unix et à l'heure UTC.

Type : Timestamp

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

GatewayDetails

Service : AWS Backup gateway

Les détails de la passerelle.

Table des matières

GatewayArn

Amazon Resource Name (ARN) de la passerelle. Utilisez l'opération `ListGateways` pour renvoyer une liste des passerelles pour votre compte et la Région AWS.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 180.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : non

GatewayDisplayName

Le nom d'affichage de la passerelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

GatewayType

Type de passerelle.

Type : chaîne

Valeurs valides : `BACKUP_VM`

Obligatoire : non

HypervisorId

L'ID d'hyperviseur de la passerelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Obligatoire : non

LastSeenTime

Détails indiquant la dernière fois que la AWS Backup passerelle a communiqué avec le cloud, au format Unix et à l'heure UTC.

Type : Timestamp

Obligatoire : non

MaintenanceStartTime

Renvoie l'heure de début de la maintenance hebdomadaire de votre passerelle, en particulier le jour et l'heure de la semaine. Notez que les valeurs sont exprimées en termes de fuseau horaire de la passerelle. Cela peut être hebdomadaire ou mensuel.

Type : objet MaintenanceStartTime

Obligatoire : non

NextUpdateAvailabilityTime

Détails indiquant l'heure de disponibilité de la prochaine mise à jour de la passerelle.

Type : Timestamp

Obligatoire : non

VpcEndpoint

Nom de DNS du point de terminaison du cloud privé virtuel (VPC) utilisé par la passerelle de sauvegarde pour se connecter au cloud.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Hypervisor

Service : AWS Backup gateway

Représente les autorisations de l'hyperviseur auxquelles la passerelle se connectera.

Un hyperviseur est un matériel, un logiciel ou un microprogramme qui crée et gère des machines virtuelles et leur alloue des ressources.

Table des matières

Host

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : chaîne

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : `^.+$`

Obligatoire : non

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : non

KmsKeyArn

Le nom de ressource Amazon (ARN) AWS Key Management Service utilisé pour chiffrer l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obligatoire : non

Name

Le nom de l'hyperviseur.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

State

L'état de l'hyperviseur.

Type : chaîne

Valeurs valides : `PENDING | ONLINE | OFFLINE | ERROR`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

HypervisorDetails

Service : AWS Backup gateway

Il s'agit des détails de l'hyperviseur spécifié. Un hyperviseur est un matériel, un logiciel ou un microprogramme qui crée et gère des machines virtuelles et leur alloue des ressources.

Table des matières

Host

L'hôte du serveur de l'hyperviseur. Il peut s'agir d'une adresse IP ou d'un nom de domaine complet (FQDN).

Type : chaîne

Contraintes de longueur : Longueur minimum de 3. Longueur maximale de 128.

Modèle : `^.+$`

Obligatoire : non

HypervisorArn

Amazon Resource Name (ARN) de l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : non

KmsKeyArn

Amazon Resource Name (ARN) de la AWS KMS utilisée pour chiffrer l'hyperviseur.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obligatoire : non

LastSuccessfulMetadataSyncTime

Il s'agit de l'heure à laquelle la dernière synchronisation réussie des métadonnées a eu lieu.

Type : Timestamp

Obligatoire : non

LatestMetadataSyncStatus

Il s'agit du statut le plus récent pour la synchronisation des métadonnées indiquée.

Type : chaîne

Valeurs valides : `CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED`

Obligatoire : non

LatestMetadataSyncStatusMessage

Il s'agit du statut le plus récent pour la synchronisation des métadonnées indiquée.

Type : chaîne

Obligatoire : non

LogGroupArn

Amazon Resource Name (ARN) du groupe de passerelles dans le journal demandé.

Type : chaîne

Contraintes de longueur : longueur minimale de 0. Longueur maximale de 2048.

Modèle : `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Obligatoire : non

Name

Il s'agit du nom de l'hyperviseur spécifié.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

State

Il s'agit de l'état actuel de l'hyperviseur spécifié.

Les états possibles sont `PENDING`, `ONLINE`, `OFFLINE` ou `ERROR`.

Type : chaîne

Valeurs valides : `PENDING | ONLINE | OFFLINE | ERROR`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

MaintenanceStartTime

Service : AWS Backup gateway

Il s'agit de l'heure de début de la maintenance hebdomadaire de votre passerelle, en particulier le jour et l'heure de la semaine. Notez que les valeurs sont exprimées en termes de fuseau horaire de la passerelle. Cela peut être hebdomadaire ou mensuel.

Table des matières

HourOfDay

La composante horaire de l'heure de début de la maintenance est représentée par hh, où hh est l'heure (0 à 23). L'heure du jour correspond au fuseau horaire de la passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale fixée à 23.

Obligatoire : oui

MinuteOfHour

La composante des minutes de l'heure de début de la maintenance est représentée par mm, où mm est la minute (0 à 59). La minute de l'heure correspond au fuseau horaire de la passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 59.

Obligatoire : oui

DayOfMonth

Le composant jour du mois de l'heure de début de la maintenance est représenté sous la forme d'un nombre ordinal compris entre 1 et 28, où 1 représente le premier jour du mois et 28 le dernier jour du mois.

Type : entier

Plage valide : valeur minimum de 1. Valeur maximale de 31.

Obligatoire : non

DayOfWeek

Nombre ordinal compris entre 0 et 6 qui représente le jour de la semaine, où 0 représente le dimanche et 6 le samedi. Le jour de la semaine correspond au fuseau horaire de la passerelle.

Type : entier

Plage valide : Valeur minimum de 0. Valeur maximale de 6.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Tag

Service : AWS Backup gateway

Une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources. Les caractères autorisés incluent les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : /.

Table des matières

Key

Élément clé dans la paire clé-valeur d'une balise. La clé ne peut pas commencer par `aws:`.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatoire : oui

Value

Élément valeur dans la paire clé-valeur d'une balise.

Type : chaîne

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[^\x00]*$`

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

VirtualMachine

Service : AWS Backup gateway

Machine virtuelle sur un hyperviseur.

Table des matières

HostName

Le nom d'hôte de la machine virtuelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

HypervisorId

ID de l'hyperviseur de la machine virtuelle.

Type : chaîne

Obligatoire : non

LastBackupDate

Date de sauvegarde la plus récente d'une machine virtuelle, au format Unix et en heure UTC.

Type : Timestamp

Obligatoire : non

Name

Le nom de la machine virtuelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

Path

Le chemin de la machine virtuelle.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 4096.

Modèle : `^[^\x00]+$`

Obligatoire : non

ResourceArn

Amazon Resource Name (ARN) de la machine virtuelle. Par exemple, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

VirtualMachineDetails

Service : AWS Backup gateway

Vos objets `VirtualMachine`, classés par Amazon Resource Name (ARN).

Table des matières

HostName

Le nom d'hôte de la machine virtuelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

HypervisorId

ID de l'hyperviseur de la machine virtuelle.

Type : chaîne

Obligatoire : non

LastBackupDate

Date de sauvegarde la plus récente d'une machine virtuelle, au format Unix et en heure UTC.

Type : Timestamp

Obligatoire : non

Name

Le nom de la machine virtuelle.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximum de 100.

Modèle : `^[a-zA-Z0-9-]*$`

Obligatoire : non

Path

Le chemin de la machine virtuelle.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximum de 4096.

Modèle : `^[^\x00]+$`

Obligatoire : non

ResourceArn

Amazon Resource Name (ARN) de la machine virtuelle. Par exemple, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Type : chaîne

Contraintes de longueur : longueur minimale de 50. Longueur maximale de 500.

Modèle : `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatoire : non

VmwareTags

Voici les détails des balises VMware associées à la machine virtuelle spécifiée.

Type : tableau d'objets VmwareTag

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

VmwareTag

Service : AWS Backup gateway

Une balise VMware est une balise attachée à une machine virtuelle spécifique. Une balise est une paire clé-valeur que vous pouvez utiliser pour gérer, filtrer et rechercher vos ressources.

Le contenu des balises VMware peut être associé aux AWS balises.

Table des matières

VmwareCategory

C'est la catégorie de VMware.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : non

VmwareTagDescription

Description définie par l'utilisateur d'une balise VMware.

Type : chaîne

Obligatoire : non

VmwareTagName

Nom défini par l'utilisateur d'une balise VMware.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : non

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++

- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

VmwareToAwsTagMapping

Service : AWS Backup gateway

Cela affiche le mappage des balises VMware aux AWS balises correspondantes.

Table des matières

AwsTagKey

L'élément clé de la paire clé-valeur de la AWS balise.

Type : chaîne

Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 128.

Modèle : `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatoire : oui

AwsTagValue

La partie valeur de la paire clé-valeur de la AWS balise.

Type : chaîne

Contraintes de longueur : Longueur minimum de 0. Longueur maximum de 256.

Modèle : `^[^\x00]*$`

Obligatoire : oui

VmwareCategory

C'est la catégorie de VMware.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : oui

VmwareTagName

Nom défini par l'utilisateur d'une balise VMware.

Type : chaîne

Contraintes de longueur : longueur minimum de 1. Longueur maximale de 80.

Obligatoire : oui

consultez aussi

Pour plus d'informations sur l'utilisation de cette API dans l'un des AWS SDK spécifiques au langage, consultez les pages suivantes :

- AWS SDK pour C++
- AWS SDK pour Java V2
- AWS SDK pour Ruby V3

Paramètres communs

La liste suivante contient les paramètres que toutes les actions utilisent pour signer les demandes Signature Version 4 à l'aide d'une chaîne de requête. Tous les paramètres spécifiques d'une action particulière sont énumérées dans le sujet consacré à cette action. Pour plus d'informations sur Signature Version 4, consultez Signature des demandes d'API AWS dans le Guide de l'utilisateur IAM.

Action

Action à effectuer.

Type : chaîne

Obligatoire : oui

Version

Version de l'API pour laquelle la demande est écrite, au format AAAA-MM-JJ.

Type : chaîne

Obligatoire : oui

X-Amz-Algorithm

Algorithme de hachage que vous avez utilisé pour créer la signature de la demande.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Valeurs valides : `AWS4-HMAC-SHA256`

Obligatoire : Conditionnelle

X-Amz-Credential

Valeur de la portée des informations d'identification, qui est une chaîne incluant votre clé d'accès, la date, la région cible, le service demandé et une chaîne de terminaison (« aws4_request »). Spécifiez la valeur au format suivant : access_key/AAAAMMJJ/région/service/aws4_request.

Pour plus d'informations, consultez Création d'une demande d'API AWS signée dans le Guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Date

La date utilisée pour créer la signature. Le format doit être au format de base ISO 8601 (AAAAMMJJ'T'HHMMSS'Z'). Par exemple, la date/heure suivante est une valeur X-Amz-Date valide : `20120325T120000Z`.

Condition : X-Amz-Date est un en-tête facultatif pour toutes les demandes. Il peut être utilisé pour remplacer la date dans la signature des demandes. Si l'en-tête Date est spécifié au format de base ISO 8601, X-Amz-Date n'est pas obligatoire. Lorsque X-Amz-Date est utilisé, il remplace toujours la valeur de l'en-tête Date. Pour plus d'informations, consultez Éléments d'une signature de demande d'API AWS dans le Guide de l'utilisateur IAM.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Security-Token

Le jeton de sécurité temporaire obtenu lors d'un appel à AWS Security Token Service (AWS STS). Pour obtenir la liste des services prenant en charge les informations d'identification de

sécurité temporaires d'AWS STS, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Condition : si vous utilisez des informations d'identification de sécurité temporaires issues d'AWS STS, vous devez inclure le jeton de sécurité.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-Signature

Spécifie la signature codée en hexadécimal qui a été calculée à partir de la chaîne à signer et de la clé de signature dérivée.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

X-Amz-SignedHeaders

Spécifie tous les en-têtes HTTP qui ont été inclus dans la demande canonique. Pour plus d'informations sur la spécification d'en-têtes signés, consultez Création d'une demande d'API AWS signée dans le Guide de l'utilisateur IAM.

Condition : spécifiez ce paramètre lorsque vous incluez des informations d'authentification dans une chaîne de requête plutôt que dans l'en-tête d'autorisation HTTP.

Type : chaîne

Obligatoire : Conditionnelle

Erreurs courantes

Cette section répertorie les erreurs communes aux actions d'API de tous les services AWS. Pour les erreurs spécifiques à une action d'API pour ce service, consultez la rubrique pour cette action d'API.

AccessDeniedException

Vous ne disposez pas d'un accès suffisant pour effectuer cette action.

Code d'état HTTP : 400

IncompleteSignature

La signature de la requête n'est pas conforme aux normes AWS.

Code d'état HTTP : 400

InternalFailure

Le traitement de la demande a échoué en raison d'une erreur, d'une exception ou d'un échec inconnu.

Code d'état HTTP : 500

InvalidAction

L'action ou l'opération demandée n'est pas valide. Vérifiez que l'action est entrée correctement.

Code d'état HTTP : 400

InvalidClientTokenId

Le certificat X.509 ou l'ID de clé d'accès AWS fourni(e) n'existe pas dans nos archives.

Code d'état HTTP : 403

NotAuthorized

Vous ne disposez pas de l'autorisation nécessaire pour effectuer cette action.

Code d'état HTTP : 400

OptInRequired

L’ID de clé d’accès AWS a besoin d’un abonnement pour le service.

Code d'état HTTP : 403

RequestExpired

La demande a atteint le service plus de 15 minutes après la date affichée sur la demande ou plus de 15 minutes après la date d'expiration de la demande (comme pour les URL pré-signées) ou la date affichée sur la demande est postérieure de 15 minutes.

Code d'état HTTP : 400

ServiceUnavailable

La requête a échoué en raison d'une défaillance temporaire du serveur.

HTTP Status Code: 503

ThrottlingException

La demande a été refusée suite à une limitation des demandes.

Code d'état HTTP : 400

ValidationError

L'entrée ne satisfait pas les contraintes spécifiées par un service AWS.

Code d'état HTTP : 400

Historique du document pour AWS Backup

- Version de l'API : 6 décembre 2023
- Dernière mise à jour de la documentation : 3 juin 2024

Le tableau suivant répertorie tous les AWS Backup lancements depuis le lancement du service en janvier 2019 jusqu'à aujourd'hui. Pour recevoir les notifications sur les mises à jour de cette documentation, vous pouvez vous abonner au flux RSS ci-dessus.

Modification	Description	Date
AWS Backup fonctionnalité Expansion régionale	AWS Backup la prise en charge du niveau d'archivage des instantanés Amazon EBS est désormais disponible dans les régions suivantes : • Chine (Beijing) • Chine (Ningxia) • AWS GovCloud (US-Ouest) • AWS GovCloud (USA Est)	3 juin 2024
Mise à jour des stratégies gérées par AWS	AWS Backup autorisation ajoutée `backup:TagResource` pour les politiques gérées suivantes : • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup	17 mai 2024

Modification	Description	Date
	Pour plus d'informations, consultez la section Mises à jour des politiques.	
AWS Backup maintenant disponible dans la région du Canada Ouest (Calgary)	La sauvegarde et la restauration de nombreux types de ressources sont désormais disponibles dans le Région AWS Canada-Ouest (Calgary). Pour connaître les fonctionnalités de sauvegarde compatibles, consultez la section Disponibilité des fonctionnalités par Région AWS. Pour les types de ressources pris en charge, consultez la section Services pris en charge par Région AWS.	14 mars 2024

Modification	Description	Date
Autorisations ajoutées à la politique gérée	AWS Backup a mis à jour la politique AWSServiceRolePolicyForBackupRestoreTestingen ajoutant des autorisations pour prendre en charge des types de ressources supplémentaires dans le cadre de la fonctionnalité de test de restauration. Pour plus d'informations sur les autorisations spécifiques ajoutées, consultez la section Mises à jour des politiques.	14 février 2024
Support de sauvegarde et de restauration pour les volumes FSx for ONTAP FlexGroup	AWS Backup prend désormais en charge la sauvegarde et la restauration de FSx pour les FlexGroup volumes ONTAP dans la plupart des cas. Régions AWS Pour plus d'informations, consultez Restauration d'un système de fichiers FSX. .	10 janvier 2024

Modification	Description	Date
Support pour la sauvegarde et la restauration de SAP HANA HA	AWS Backup prend désormais en charge les bases de données SAP HANA High Availability sur la sauvegarde et la restauration Amazon EC2. Pour plus d'informations, consultez Sauvegarde de bases de données SAP HANA sur des instances Amazon EC2 et Restauration d'une base de données SAP HANA sur une instance Amazon EC2.	21 décembre 2023
AWS Backup Contrôle Audit Manager pour les tests de restauration	AWS Backup Audit Manager permet désormais de contrôler le temps de restauration pour que les ressources atteignent l'objectif afin de faciliter le suivi des temps de restauration. Ce contrôle vérifie si le temps de restauration d'une ressource correspond à la durée cible. Pour plus d'informations, consultez Contrôles et mesures correctives et Tests de restauration Audit.	18 décembre 2023

Modification	Description	Date
Support pour le stockage à froid Amazon EBS	AWS Backup prend désormais en charge la transition des sauvegardes EBS d'un stockage à chaud vers un stockage à froid. Pour plus d'informations, veuillez consulter la rubrique • Niveau d’archive Amazon EBS pour le stockage à froid • Cycle de vie et niveaux de stockage • Création d'un plan de sauvegarde	27 novembre 2023
Présentation des tests de la restauration	AWS Backup introduit les tests de restauration, qui permettent une évaluation automatique et périodique de la viabilité de la restauration, ainsi que la possibilité de surveiller la durée des tâches de restauration. Pour plus d’informations, consultez Tests de restauration.	27 novembre 2023

Modification	Description	Date
Mise à jour des stratégies gérées par AWS	AWS Backup a ajouté les autorisations `ec2:DescribeSnapshotTierStatus` et `ec2:ModifySnapshotTier` aux politiques gérées `AWSBackupServiceRolePolicyForBackups` et`AWSBackupServiceLinkedRolePolicyForBackup` . AWS Backup a également ajouté les autorisations `ec2:DescribeSnapshotTierStatus` et `ec2:RestoreSnapshotTier` à la politique gérée`AWSBackupServiceRolePolicyForRestores` . Ces autorisations sont nécessaires pour que les utilisateurs aient la possibilité de transférer les ressources Amazon EBS stockées vers le stockage AWS Backup d'archives et de restaurer les ressources depuis le niveau de stockage d'archives. Pour plus d'informations, consultez Mises à jour des politiques.	27 novembre 2023

Modification	Description	Date
Ajout d'une autorisation de transmission de rôle pour prendre en charge les tests de la restauration.	AWS Backup ajoutés `restore-testing.backup.amazonaws.com` à `IamPassRolePermissions` et `IamCreateServiceLinkedRolePermissions`. Cet ajout est nécessaire pour AWS Backup effectuer des tests de restauration pour le compte des clients.	27 novembre 2023

Modification	Description	Date
Ajout d'un nouveau rôle lié à un service	AWS Backup a ajouté le nouveau rôle lié au service nommé `AWSServiceRoleForBackupRestoreTesting`, qui fournit des autorisations de sauvegarde pour effectuer des tests de restauration. Ce nouveau rôle lié à un service fournit AWS Backup les autorisations nécessaires pour effectuer des tests de restauration. Les autorisations incluent les actions `list, read, and write` relatives aux services suivants à inclure dans les tests de la restauration : Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx pour Lustre, FSx for Windows File Server, FSx pour ONTAP, FSx pour OpenZFS, Amazon Neptune, Amazon RDS et Amazon S3.	27 novembre 2023

Modification	Description	Date
Nouveau tableau de bord des métriques relatives aux tâches dans la AWS Backup console	La AWS Backup console affiche désormais un tableau de bord des tâches, simplifiant la surveillance de l'état des sauvegardes à grande échelle grâce à une nouvelle interface utilisateur visuelle et à des mesures agrégées de sauvegarde, de copie et de restauration pour les services pris en charge par AWS Backup. Le tableau de bord des offres d'emploi est disponible dans toutes les régions où AWS Backup Audit Manager est disponible. Les régions non répertoriées pourront toujours accéder au CloudWatch tableau de bord. Pour plus d'informations, consultez Tableaux de bord de la console AWS Backup.	15 novembre 2023

Modification	Description	Date
Prise en charge des sauvegardes de piles imbriquées	AWS Backup a étendu sa prise en charge des sauvegardes de AWS CloudFormation ressource s. Vos piles CloudFormation d'applications contenant des piles imbriquées peuvent être incluses dans vos sauvegard es. Pour plus d'informations, consultez Sauvegardes de piles CloudFormation .	8 novembre 2023
Prise en charge d'Amazon S3 dans les régions Chine (Beijing) et Chine (Ningxia).	AWS Backup le support pour Amazon S3 est désormais disponible dans les régions de Chine (Pékin) et de Chine (Ningxia). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	26 octobre 2023
Support pour les sauvegardes continues d'Amazon Aurora et la oint-in-time restauration des adresses IP	AWS Backup prend désormais en charge les sauvegardes et point-in-time restaurations continues (PITR) pour les ressources Aurora. Pour plus d'informations, consultez les sections Sauvegardes continues et oint-in-time restauration IP.	7 septembre 2023

Modification	Description	Date
AWS CloudFormation les piles soutiennent l'exclusion des ressources	AWS Backup prend désormais en charge l'option d'exclure les ressources choisies de votre AWS CloudFormation pile. Pour plus d'informations, consultez Sauvegardes de piles AWS CloudFormation.	6 septembre 2023
Les règles du plan de sauvegarde introduisent la flexibilité du fuseau horaire	AWS Backup les règles du plan peuvent désormais avoir un fuseau horaire spécifié pour les fenêtres de sauvegarde. Pour plus d'informations, consultez Gestion des plans de sauvegarde.	28 août 2023
AWS Backup désormais disponible dans la région Israël (Tel Aviv)	De nombreuses AWS Backup fonctionnalités sont désormais disponibles dans la nouvelle région d'Israël (Tel Aviv). Pour connaître les ressource s prises en charge, consultez Disponibilité des fonctionn alités par Région AWS.	22 août 2023

Modification	Description	Date
AWS Backup Audit Manager prend désormais en charge les comptes d'administrateurs délégués	AWS Backup La génération de rapports Audit Manager est désormais accessible par les comptes d'administrateurs délégués. Pour plus d'informations, veuillez consulter la rubrique • Audit les sauvegardes et création de rapports avec AWS Backup Audit Manager • Utilisation des rapports d'audit • Administrateur délégué	16 août 2023
Aperçu du coffre-fort de sauvegarde logiquement cloisonné	AWS Backup propose désormais un aperçu d'un nouveau type de coffre-fort de sauvegarde destiné à compléter les opérations de protection des données. Pour plus d'informations, consultez Coffres-forts à isolation logique (version préliminaire).	08 août 2023

Modification	Description	Date
AWS Backup améliore les sauvegardes Amazon S3	AWS Backup dispose de capacités accrues en termes de performances, de taille et de rapidité pour les sauvegard es de compartiments S3. Pour plus d'informations, consultez Sauvegardes Amazon S3.	1er août 2023
Fonctionnalité de restaurat ion des balises désormais disponible dans les régions de Chine	Les balises qui font partie d'une sauvegarde peuvent désormais être copiées lorsque vous créez une tâche de restauration dans les régions Chine (Beijing) ou Chine (Ningxia). Pour plus d'informations, consultez Copie de balises lors d'une restauration.	17 juillet 2023
AWS Backup prend désormais en charge Amazon S3 dans d'autres régions	AWS Backup le support pour Amazon S3 est désormais disponible dans les régions Europe (Espagne), Europe (Zurich), Asie-Pacifique (Hyderabad) et Asie-Pacifique (Melbourne). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	6 juillet 2023

Modification	Description	Date
La copie entre comptes s'étend à d'autres régions	AWS Backup prend désormais en charge la copie de sauvegarde entre comptes de la plupart des ressources dans les régions suivantes : Asie-Pacifique (Jakarta), Moyen-Orient (Bahreïn), Asie-Paci fique (Hong Kong), Afrique (Le Cap), Europe (Milan), Asie-Pacifique (Osaka), Moyen-Orient (Émirats arabes unis), Europe (Espagne), Europe (Zurich), Asie-Pacifique (Hyderabad) et Asie-Pacifique (Melbourne). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	5 juillet 2023
Backup Audit Manager disponible dans GovCloud les régions	AWS Backup a étendu AWS Backup Audit Manager à AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). Pour plus d'informations, consultez Disponibilité des fonctionnalités par région.	29 juin 2023

Modification	Description	Date
La gestion entre comptes est désormais disponible dans les régions GovCloud	AWS Backup prend désormais en charge la gestion intercomptes des ressources en AWS GovCloud (USA Est) et AWS GovCloud (USA Ouest). Pour plus d'informations, consultez Gestion des ressources AWS Backup sur plusieurs comptes AWS.	29 juin 2023
Prise en charge des copies entre régions d'Amazon Aurora dans des régions supplémentaires	AWS Backup prend désormais en charge les copies de sauvegarde interrégionales pour les clusters Aurora à destination et en provenance des régions suivantes : Asie-Pacifique (Jakarta), Moyen-Orient (Bahreïn), Asie-Pacifique (Hong Kong), Afrique (Le Cap), Europe (Milan), Moyen-Orient (Émirats arabes unis), Europe (Espagne), Europe (Zurich), Asie-Pacifique (Hyderabad) et Asie-Pacifique (Melbourne).	5 juin 2023

Modification	Description	Date
Copie des balises lors de la restauration	Les balises qui font partie d'une sauvegarde peuvent désormais être copiées lorsque vous créez une tâche de restauration. Pour plus d'informations, consultez Copie de balises lors d'une restauration.	22 mai 2023
AWS Backup s'intègre aux notifications AWS utilisateur	Vous pouvez désormais choisir de recevoir des notifications relatives aux événements de sauvegarde, de copie et de restauration via la console de notifications utilisateur AWS. Pour plus d'informations, voir Commencer à utiliser les notifications AWS utilisateur.	10 mai 2023
Sauvegardes entre régions disponibles dans quatre nouvelles régions	AWS Backup prend désormais en charge la sauvegarde interrégionale dans les régions du Moyen-Orient (EAU), de l'Europe (Espagne), de l'Europe (Zurich) et de l'Asie-Pacifique (Hyderabad).	28 avril 2023

Modification	Description	Date
Support de AWS Backup copie étendu entre régions	Les sauvegardes entre régions des ressources Amazon EFS, VMware et DynamoDB peuvent désormais être effectuées dans les régions suivantes : Asie-Pacifique (Jakarta) , Moyen-Orient (Bahreïn), Asie-Pacifique (Hong Kong), Afrique (Le Cap) et Europe (Milan).	28 avril 2023
Sauvegarde et restauration Amazon S3 dans la région Amérique du Sud (São Paulo)	AWS Backup le support pour Amazon S3 (Amazon Simple Storage Service) est désormais disponible dans la région Amérique du Sud (São Paulo). Pour plus d'informations, consultez Sauvegardes Amazon S3.	20 avril 2023
AWS Backup s'étend à la région Asie-Pacifique (Melbourne)	AWS Backup est désormais disponible dans la région Asie-Pacifique (Melbourne). Pour plus d'informations, consultez la section Disponibilité des fonctionnalités par AWS région.	20 avril 2023

Modification	Description	Date
Prise en charge régionale étendue pour Amazon S3	AWS Backup le support pour Amazon S3 (Amazon Simple Storage Service) est désormais disponible dans les AWS GovCloud régions (USA Est) et AWS GovCloud (USA Ouest) Pour plus d'informations, consultez Sauvegardes Amazon S3.	19 avril 2023
Sauvegarde et restauration de bases de données SAP HANA sur des instances Amazon EC2	AWS Backup permet désormais de sauvegarder et de restaurer des bases de données SAP HANA exécutées sur des instances Amazon EC2 dans la plupart des régions. Pour plus d'informations, consultez Sauvegarde de bases de données SAP HANA sur des instances Amazon EC2.	17 avril 2023

Modification	Description	Date
AWS Backup désormais disponible dans les régions Europe (Espagne), Europe (Zurich) et Asie-Pacifique (Hyderabad)	AWS Backup le support s'est étendu à de nouvelles régions, notamment l'Europe (Espagne), l'Europe (Zurich) et l'Asie-Pacifique (Hyderabad). Les ressources prises en charge peuvent être sauvegardées et restaurées dans ces régions. Pour plus d'informations, consultez la section Disponibilité des fonctionnalités par AWS région.	13 avril 2023
Politique AWS gérée mise à jour `AWSBackupAuditAccess`	Politique AWS gérée mise à jour AWSBackupAuditAccess. AWS Backup a remplacé la sélection de ressources dans l'API `config:DescribeComplianceByConfigRule` par une ressource générique. Pour plus d'informations, consultez Mises à jour de politiques pour AWS Backup.	11 avril 2023

Modification	Description	Date
Hyperviseurs avec Amazon Logs CloudWatch	AWS Backup les utilisateurs de la passerelle peuvent désormais intégrer des hyperviseurs aux CloudWatch journaux pour gérer les journaux. Pour plus d'informations, reportez-vous aux sections Modification de la configuration d'un hyperviseur et CloudWatch Journaux.	29 mars 2023
Prise en charge régionale étendue pour Amazon S3	AWS Backup le support pour Amazon S3 est désormais disponible dans les régions Asie-Pacifique (Jakarta) et Moyen-Orient (Émirats arabes unis).	22 mars 2023
Amélioration de la sauvegarde incrémentielle des machines virtuelles	Les sauvegardes de machines virtuelles VMware présentant des problèmes de données CBT (Changed Block Tracking) contiennent désormais des informations supplémentaires permettant d'y remédier et de résoudre les problèmes. Pour plus d'informations, consultez Sauvegardes de machines virtuelles incrémentielles et Dépannage de vos machines virtuelles.	15 mars 2023

Modification	Description	Date
AWS Backup prise en charge de plusieurs adaptateurs réseau	AWS Backup la passerelle prend désormais en charge la configuration de plusieurs adaptateurs réseau Pour plus d'informations sur la configuration de vos adaptateurs réseau, consultez Configuration de votre passerelle pour plusieurs NIC dans VMware dans le Guide du développeur AWS Backup .	8 mars 2023
AWS Backup prise en charge de vSphere 8	AWS Backup prend désormais en charge la sauvegarde et la restauration des machines virtuelles qui s'exécutent sur VMware vSphere 8. Pour plus d'informations sur les options VMware prises en charge, consultez Machines virtuelles prises en charge dans le Guide du développeur AWS Backup .	8 mars 2023

Modification	Description	Date
AWS Backup Audit Manager prend en charge les sauvegardes Amazon RDS Multi-AZ	Backup Audit Manager prend désormais en charge les sauvegardes à plusieurs zones de disponibilité d'Amazon Relational Database Service. Pour plus d'informations, découvrez comment auditer les sauvegardes et créer des rapports avec AWS Backup Audit Manager.	1er février 2023
AWS Backup propose une sauvegarde incrémentielle pour les tables Amazon Timestream	AWS Backup propose désormais des fonctionnalités de sauvegarde étendues pour les sauvegardes Timestrea m. Les plans de sauvegarde peuvent désormais prendre en charge des sauvegard es incrémentielles afin de réduire le temps nécessaire à la sauvegarde des ressource s Timestream et les coûts de stockage. Pour plus d'informations, consultez Sauvegardes Amazon Timestream.	23 janvier 2023

Modification	Description	Date
AWS Backup désormais disponible à Dubaï	AWS Backup s'est étendu à la région du Moyen-Orient (EAU). Les ressources prises en charge peuvent être sauvegardées et restaurées dans cette région.	17 janvier 2023
Copie entre régions disponible dans d'autres régions	AWS Backup propose désormais des sauvegardes interrégionales dans la région Asie-Pacifique (Jakarta), le Moyen-Orient (Bahreïn), la région Asie-Pacifique (Hong Kong), la région Afrique (Le Cap) et la région Europe (Milan) pour la plupart des ressources. Pour plus d'informations, consultez Création de copies de sauvegardes entre Régions AWS.	21 décembre 2022

Modification	Description	Date
Limites et limitation de la bande passante de Backup Gateway	AWS Backup Gateway permet désormais de limiter le débit de téléchargement depuis les passerelles AWS Backup afin de contrôler la quantité de bande passante réseau utilisée par la passerelle. Pour prendre en charge cette fonctionnalité, AWS Backup a créé et mis à jour des politiques gérées, notamment `AWSBackupFullAccess` et`AWSBackupOperatorAccess` . Pour plus d'informations, consultez Limitation de la bande passante de Backup Gateway.	15 décembre 2022

Modification	Description	Date
Prise en charge des balises VMware par Backup Gateway	AWS Backup Gateway prend désormais en charge les balises VMware. Les utilisateurs ont la possibilité supplémentaire de créer des AWS balises correspondant aux balises utilisées pour les machines virtuelles. Pour prendre en charge cette fonctionnalité, AWS Backup a créé et mis à jour des politiques gérées`AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` , notamment`AWSBackupFullAccess` , et`AWSBackupOperatorAccess` . Pour plus d'informations, consultez Balises VMware.	15 décembre 2022
AWS Backup support pour Amazon Timestream	AWS Backup prend désormais en charge la sauvegarde et la restauration des tables Amazon Timestream. Pour plus d'informations, consultez Sauvegardes Amazon Timestream.	13 décembre 2022

Modification	Description	Date
AWS Backup offres Legal Hold	AWS Backup introduit un nouvel outil destiné à protéger les points de récupération grâce à une mise en détention légale. Pour plus d'informations, consultez Conservation légale.	27 novembre 2022
AWS Backup Audit Manager : rapports interrégionaux et multicomptes	AWS Backup Audit Manager apporte des fonctionnalités supplémentaires à la conformité et aux rapports de travail. Les utilisateurs peuvent générer des rapports incorporant plusieurs régions et comptes. Pour plus d'informations, consultez Utilisation des rapports d'audit.	27 novembre 2022
AWS Backup prend en charge Amazon Redshift	AWS Backup offre désormais un support pour la sauvegarde des clusters Amazon Redshift et pour la restauration des clusters et des tables Amazon Redshift. Pour plus d'informations, consultez la page Amazon Redshift backups (Sauvegardes Amazon Redshift).	27 novembre 2022

Modification	Description	Date
AWS Backup prend en charge les piles d' AWS CloudFormation applications de sauvegarde	AWS Backup permet de sauvegarder CloudFormation et de restaurer des applicati ons contenant plusieurs ressources en sauvegardant une pile et en restaurant les ressources qu'elle contient. Pour plus d'informations, consultez Sauvegardes de pile d'applications.	27 novembre 2022
AWS Backup propose des comptes d'administrateur délégués et une délégation des politiques de sauvegarde	AWS Backup les comptes inscrits AWS Organizations peuvent désigner les comptes des membres comme des comptes d'administrateur délégué. Pour plus d'informations, consultez la section Gestion de plusieurs comptes avec AWS Organizations.	27 novembre 2022

Modification	Description	Date
Version préliminaire publique des sauvegardes et restaurations de SAP HANA sur des instances Amazon EC2	AWS Backup et AWS Backint proposent un aperçu public intégré des fonctionnalités de sauvegarde et de restauration des bases de données SAP HANA sur des instances EC2. Pour plus d'informations, consultez notre Version préliminaire publique de SAP HANA sur les instances Amazon EC2. Pour soutenir cette version préliminaire, AWS Backup a fourni des mises à jour des politiques et de nouvelles politiques AWS gérées pour ces fonctionnalités.	20 novembre 2022

Modification	Description	Date
Restauration de VMware sur des instances Amazon EC2	AWS Backup offre désormais la possibilité de restaurer des machines virtuelles sur des instances Amazon EC2, en plus de la possibilité de restaurer des machines sur EBS, VMware, VMware Cloud on AWS et VMware Cloud on. AWS Outposts Pour plus d'informations, consultez la documentation sur l'utilisation de la AWS Backup console pour restaurer les points de restauration des machines virtuelles.	9 novembre 2022
Fonctionnalité étendue de AWS Backup Vault Lock	AWS Backup Vault Lock peut désormais être créé en mode gouvernance pour des protections IAM supplémen taires ou en mode conformité pour garantir l'immuabilité. En savoir plus sur AWS Backup Vault Lock.	4 octobre 2022

Modification	Description	Date
AWS Backup Audit Manager est désormais disponible dans les régions Afrique (Le Cap) et Europe (Milan)	AWS Backup Audit Manager s'est étendu à la région Afrique (Le Cap) et à la région Europe (Milan). Pour plus d'informations sur Backup Audit Manager, consultez Audit les sauvegardes et création de rapports avec AWS Backup Audit Manager.	14 septembre 2022
AWS Backup intègre CloudWatch les métriques Amazon au tableau de bord de la console Backup	AWS Backup améliore le tableau de bord de sa console Backup afin d'afficher CloudWatch les métriques Amazon intégrées pour les tâches de sauvegarde et de restauration afin de renforcer les capacités de surveillance et de flexibilité.	8 septembre 2022
Prise en charge d'une flexibilité de chiffrement Amazon EBS supplémentaire lors de la restauration	AWS Backup propose désormais des options de chiffrement supplémentaires lors de la restauration des instantanés Amazon EBS.	1er septembre 2022
AWS Backup prend en charge la copie de sauvegarde entre comptes Amazon S3 et entre régions	AWS Backup propose désormais la copie de sauvegarde entre régions et entre comptes pour les sauvegardes Amazon S3. Pour plus d'informations, consultez Sauvegardes Amazon S3.	28 juillet 2022

Modification	Description	Date
AWS Backup Audit Manager offre un support de contrôle supplémentaire pour FSx for ONTAP	AWS Backup Audit Manager propose désormais des contrôles supplémentaires pour prendre en charge la surveillance et l'audit de FSx pour les volumes ONTAP, notamment les ressources de sauvegarde protégées par un plan de sauvegarde et le dernier point de restauration créé. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager.	22 juillet 2022
AWS Backup ajoute la prise en charge de la sauvegarde et de la restauration des clusters multi-AZ Amazon RDS pour les clusters PostgreSQL et MySQL	AWS Backup a ajouté une option de sauvegarde et de restauration de clusters de zones de disponibilité multiples avec une instance de base de données principale et deux instances de base de données de secours lisibles. Pour en savoir plus, consultez Sauvegardes Amazon RDS Multi-AZ.	20 juillet 2022

Modification	Description	Date
AWS Backup Audit Manager ajoute un nouveau contrôle pour la création de points de restauration	AWS Backup Audit Manager propose un nouveau contrôle d'audit pour une meilleure prise en charge de la conformité. `Last recovery point created` est un contrôle supplémentaire facultatif permettant de garantir que les points de récupération sont créés dans les délais spécifiés . Pour en savoir plus, consultez Contrôle créé par le dernier point de récupération.	29 juin 2022
Exemple de point de terminaison AWS Backup Gateway ajouté	AWS Backup Gateway a fourni un exemple de point de terminaison pour aider les utilisateurs à se connecter aux VPN (réseaux privés virtuels) . Pour plus d'informations, consultez Création d'un point de AWS Backup terminaison VPC.	14 juin 2022

Modification	Description	Date
AWS Backup propose désormais des points de terminaison Amazon VPC pour VMware	AWS Backup prend désormais en charge les points de terminaison Amazon VPC pour VMware, ce qui vous permet d'utiliser un réseau privé virtuel entre vos environnements VMware et d'utiliser. AWS AWS PrivateLink Pour plus d'informations, consultez Création d'une passerelle et AWS Backup et AWS PrivateLink.	1 juin 2022
AWS Backup Audit Manager offre un support de contrôle supplémentaire pour Amazon S3	Backup Audit Manager prend désormais en charge le contrôle de conformité Ressources de sauvegarde protégées par des plans de sauvegarde pour les types de ressources S3. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager.	25 mai 2022

Modification	Description	Date
AWS Backup Audit Manager offre un support de contrôle supplémentaire pour Storage Gateway	Backup Audit Manager prend désormais en charge le contrôle de conformité Ressources de sauvegarde protégées par des plans de sauvegarde pour les types de ressources Storage Gateway. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager.	25 mai 2022
Prise en charge d'Amazon FSx pour OpenZFS	AWS Backup offre désormais une gestion supplémentaire de la protection des données pour la sauvegarde et la restauration vers FSx pour les systèmes de fichiers OpenZFS.	18 mai 2022
AWS Backup Support d'Audit Manager pour VMware	AWS Backup fournit désormais un support pour les machines virtuelles dans les contrôles et les mesures correctives de Backup Audit Manager. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager.	11 mai 2022

Modification	Description	Date
Amazon FSx est désormais disponible dans la région Asie-Pacifique (Osaka)	AWS Backup propose désormais la sauvegarde d'Amazon FSx dans la région Asie-Pacifique (Osaka) ainsi que des copies interrégionales à destination et en provenance de celle-ci.	26 avril 2022
Prise en charge d'Amazon FSx pour Lustre Persistent_2	AWS Backup offre désormais un support général pour Amazon FSx for Lustre, qui prend en charge des niveaux de débit par unité de stockage supérieurs à ceux des systèmes de fichiers Persistent_1.	5 avril 2022
Améliorations VMware	AWS Backup propose désormais la restauration sur Amazon EBS Volume, la restauration au niveau du disque et le support de VMware on AWS Outposts. Pour plus d'informations, consultez Restauration d'une machine virtuelle.	31 mars 2022
AWS Backup Disponibilité pour l'Asie-Pacifique (Jakarta)	AWS Backup est désormais disponible pour les clients de la région Asie-Pacifique (Jakarta).	17 mars 2022

Modification	Description	Date
Nouveaux contrôles pour AWS Backup Audit Manager	AWS Backup Audit Manager introduit trois nouveaux contrôles d'audit : la copie entre régions, la copie entre comptes et Backup Vault Lock. Pour plus d'informations, consultez Contrôles et corrections d'AWS Backup Audit Manager.	17 mars 2022
Support pour AWS PrivateLink	Avec AWS PrivateLink for AWS Backup, vous pouvez vous connecter directement à AWS Backup l'aide d'un point de terminaison d'interface dans votre VPC au lieu de vous connecter via l'Internet public. Les points de terminaison de l'interface sont directement accessibles depuis des applications qui se trouvent sur site ou dans une autre AWS région. Pour plus d'informations, consultez AWS Backup et AWS PrivateLink.	28 février 2022

Modification	Description	Date
Prise en charge d'Amazon Simple Storage Service (Amazon S3)	La disponibilité générale de AWS Backup pour Amazon S3 Régions AWS est disponible dans tous les domaines, sauf pour les régions Chine (Pékin), Chine (Ningxia), AWS GovCloud (États-Unis ouest) et AWS GovCloud (États-Unis est). Pour plus d'informations, consultez Utilisation avec des données Amazon S3.	14 février 2022
Support pour la sauvegarde DynamoDB avancée dans les régions chinoises AWS	La sauvegarde DynamoDB avancée est désormais disponible dans les régions Chine (Beijing) et Chine (Ningxia). Pour plus d'informations, consultez Sauvegarde DynamoDB avancée.	18 janvier 2022
Version préliminaire publique de la prise en charge d'Amazon S3	AWS Backup propose un aperçu public des sauvegardes Amazon S3. Pour plus d’informations, consultez Utilisation avec les données Amazon S3.	30 novembre 2021
Prise en charge des machines virtuelles (VM) VMware	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder automatiquement les machines virtuelles VMware. Pour plus d’informations, consultez Sauvegardes de machines virtuelles.	30 novembre 2021

Modification	Description	Date
Prise en charge de la sauvegarde DynamoDB avancée	Vous pouvez désormais utiliser AWS Backup les fonctionnalités suivantes pour toutes les nouvelles sauvegardes de tables DynamoDB que vous créez : hiérarchisation du stockage à froid, balisage de répartiti on des coûts, copie entre régions, copie entre comptes, chiffrement indépendant et copie de balises depuis les tables DynamoDB sources. Pour plus d'informations, consultez Sauvegarde DynamoDB avancée le guide du développeur Amazon DynamoDB et son utilisati on avec AWS Backup DynamoDB.	23 novembre 2021
Support à l'amélioration de l'affectation des AWS Backup ressources dans les régions AWS chinoises	AWS Backup l'amélioration de l'affectation des ressources est désormais disponible dans les régions de Chine (Pékin) et de Chine (Ningxia). Pour plus d'informations, consultez Affectation de ressources à un plan de sauvegarde.	16 novembre 2021

Modification	Description	Date
Lancement de l'amélioration de l'affectation des AWS Backup ressources	L'amélioration de l'attribution des ressources de sauvegarde vous offre des contrôles supplémentaires et précis ainsi que de nouveaux processus rationalisés pour déployer des plans de sauvegarde qui protègent des centaines de milliers de AWS ressources. Utilisez cette fonctionnalité pour plus de vitesse, de flexibilité et de précision lors de la protection des données avec AWS Backup. Pour plus d'informations, consultez Affectation de ressources à un plan de sauvegarde.	10 novembre 2021
Prise en charge d'Amazon Neptune	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder des clusters Amazon Neptune. Pour en savoir plus, consultez Qu'est-ce qu' AWS Backup ?	5 novembre 2021
Prise en charge d'Amazon DocumentDB	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder des clusters Amazon DocumentDB. Pour en savoir plus, consultez Qu'est-ce qu' AWS Backup ?	5 novembre 2021

Modification	Description	Date
Support pour AWS Backup Vault Lock dans les régions AWS chinoises	AWS Backup Vault Lock est désormais disponible dans les régions Chine (Pékin) et Chine (Ningxia). Pour plus d'informations, consultez AWS Backup Vault Lock.	03 novembre 2021
Lancement de AWS Backup Vault Lock	Avec AWS Backup Vault Lock, vous pouvez empêcher la suppression des sauvegardes stockées dans un coffre-fort AWS Backup de sauvegarde. Pour plus d'informations, consultez AWS Backup Vault Lock.	7 octobre 2021
Lancement des rapports de conformité AWS Backup d'Audit Manager	Grâce aux rapports de conformité, vous pouvez générer des rapports quotidiens sur la conformité de votre activité de sauvegarde et de vos ressources par rapport aux contrôles que vous avez définis dans vos frameworks AWS Backup Audit Manager. Pour plus d'informations, consultez Modèles de rapport de conformité.	5 octobre 2021

Modification	Description	Date
AWS CloudFormation support pour AWS Backup Audit Manager	Avec AWS CloudFormation, vous pouvez désormais déployer les frameworks, les contrôles et les plans de rapports d' AWS Backup Audit Manager de manière sûre et reproductible à grande échelle. Pour plus d'informations, consultez la section Audit et rapports de sauvegarde avec AWS Backup Audit Manager.	4 octobre 2021
Lancement d' AWS Backup Audit Manager	Avec AWS Backup Audit Manager, vous pouvez désormais définir des contrôles pour votre activité et vos ressources de sauvegarde, et identifier les activités et les ressources qui ne sont pas conformes à vos contrôles. Vous pouvez également utiliser AWS Backup Audit Manager pour générer des rapports quotidiens et à la demande qui prouvent la conformité avec les contrôles que vous avez définis au fil du temps. Pour plus d'informations, consultez la section Audit et rapports de sauvegarde avec AWS Backup Audit Manager.	24 août 2021

Modification	Description	Date
Prise en charge de nouvelles opérations de point de récupération asynchrones	AWS Backup assume désormais un rôle lié au service pour gérer les règles du cycle de vie de vos sauvegardes au cas où vous modifieriez ou supprimeriez votre rôle IAM d'origine. Pour plus d'informations, consultez Suppression des sauvegardes.	23 août 2021
Prise en charge de sauvegardes multi-volumes en cas de panne sur Amazon EBS	Désormais, lorsque vous protégez AWS Backup vos instances Amazon EC2, vous effectuez des sauvegardes multivolumes AWS Backup cohérentes en cas de crash de tous les volumes Amazon EBS attachés à chaque instance Amazon EC2 par défaut. Pour plus d'informations, consultez Création d'une sauvegarde Amazon EBS multi-volume en cas de panne.	14 juin 2021

Modification	Description	Date
Support supplémentaire pour Amazon FSx Régions AWS	Vous pouvez désormais les utiliser AWS Backup pour protéger vos systèmes de fichiers Amazon FSx dans les régions suivantes : AWS GovCloud (US) région Europe (Milan), région Afrique (Le Cap) et région Moyen-Orient (Bahreïn). Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	15 avril 2021
Prise en charge de sauvegardes Amazon FSx entre régions et entre comptes	Vous pouvez désormais les utiliser AWS Backup pour copier des sauvegardes Amazon FSx sur des comptes Régions AWS et des comptes. Pour plus d'informations, consultez Création d'une copie de sauvegarde. Si vous utilisez des politiques gérées par le client, vous devez ajouter la nouvelle autorisation `fsx:CopyBackup` pour éviter l'échec des tâches de sauvegarde existantes. Pour obtenir cette autorisation, consultez la dernière déclaration de la politique de sauvegarde Amazon FSx dans les politiques gérées par le client.	12 avril 2021

Modification	Description	Date
Prise en charge des balises de répartition des coûts pour les sauvegardes Amazon EFS	Vous pouvez désormais utiliser des balises de répartition des coûts pour suivre les coûts de vos sauvegardes Amazon EFS de manière détaillée, ainsi que pour afficher et filtrer ces balises à l'aide de ces balises AWS Cost Explorer. Pour plus d'informations, consultez Utilisation des balises de répartition des coûts.	7 avril 2021
Autorisation de FedRAMP High	AWS Backup est désormais autorisé à prendre en charge les charges de travail élevées de FedRAMP. Pour plus d'informations, consultez les Services AWS concernés par le programme de conformité.	25 mars 2021
Nouveau Région AWS	AWS Backup est désormais disponible dans la région Asie-Pacifique (Osaka). Dans cette région, AWS Backup ne prend pas en charge Storage Gateway, Amazon FSx et la sauvegarde entre comptes. Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	25 mars 2021

Modification	Description	Date
Prise en charge des opérations par lots du point de récupération	Vous pouvez désormais utiliser la AWS Backup console pour automatiser les opérations par lots afin de nettoyer les points de restauration dans vos coffres-forts de sauvegarde. Pour plus d'informations, consultez Suppression des sauvegardes.	23 mars 2021
Prise en charge des restaurations vers la classe de stockage Amazon EFS One Zone	Vous pouvez désormais restaurer vos sauvegardes Amazon EFS dans la classe de stockage Amazon EFS One Zone. Pour plus d'informations, consultez Restauration d'un système de fichiers Amazon EFS.	12 mars 2021
Support pour la restauration et la sauvegarde continue d'Amazon Relational Database point-in-time Service	Vous pouvez désormais l'utiliser AWS Backup pour automatiser les sauvegardes continues d'Amazon RDS et effectuer des point-in-time restaurations (PITR), en plus d'orchestrer vos sauvegardes de snapshots. Pour plus d'informations, voir Restauration à une heure spécifiée à l'aide de point-in-time la restauration.	10 mars 2021

Modification	Description	Date
Support pour Amazon CloudWatch	Vous pouvez désormais l'utiliser CloudWatch pour surveiller AWS Backup les métriques. Pour plus d'informations, consultez la section Surveillance des événements et des mesures avec Amazon CloudWatch et Amazon EventBridge.	3 février 2021
Support pour Amazon EventBridge	Vous pouvez désormais l'utiliser EventBridge pour surveiller les AWS Backup événements. Pour plus d'informations, consultez la section Surveillance des événements et des mesures avec Amazon CloudWatch et Amazon EventBridge.	3 février 2021
Prise en charge des sauvegardes entre comptes	Vous pouvez désormais l' AWS Backup utiliser pour sauvegarder vos ressources sur plusieurs Comptes AWS. Pour plus d'informations, consultez la section Création de copies de sauvegarde entre AWS comptes.	18 novembre 2020

Modification	Description	Date
Prise en charge de la sauvegarde et de la restauration des systèmes de fichiers Amazon FSx	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder les systèmes de fichiers Amazon FSx. Pour plus d'informations, consultez Utilisation avec des systèmes de fichiers Amazon FSx.	9 novembre 2020
Nouveau Régions AWS	AWS Backup est désormais disponible en Afrique (Le Cap) et en Europe (Milan) Régions AWS. Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	21 octobre 2020
Prise en charge de la sauvegarde Windows compatible avec VSS	Vous pouvez désormais sauvegarder et restaurer des applications Windows compatibles avec VSS (Volume Shadow Copy Service) exécutées sur des instances Amazon EC2. Pour plus d'informations, consultez Création de sauvegardes Windows VSS.	22 septembre 2020

Modification	Description	Date
Prise en charge de la sauvegarde automatique d'Amazon EFS	Vous pouvez désormais l'utiliser AWS Backup pour sauvegarder automatiquement les systèmes de fichiers Amazon EFS. Pour plus d'informations, consultez Mise en route 4 : création de sauvegardes automatiques Amazon EFS.	16 juillet 2020
Nouveau Région AWS	AWS Backup est désormais disponible dans le AWS GovCloud (US) Region. Pour plus d'informations, veuillez consulter la rubrique Points de terminaison et quotas AWS Backup dans la Référence générale AWS .	24 juin 2020
Support pour la gestion des sauvegardes sur plusieurs Comptes AWS	Vous pouvez désormais gérer les sauvegardes sur plusieurs Comptes AWS en utilisant AWS Organizations. Pour de plus amples informations, veuillez consulter Fonctionnement de la gestion inter-comptes.	24 juin 2020

Modification	Description	Date
Support pour Amazon Aurora ajouté à AWS Backup	Vous pouvez désormais configurer AWS Backup pour sauvegarder les ressource s d'Amazon Aurora. Pour plus d'informations, consultez Présentation de la sauvegard e et de la restauration d'un cluster de bases de données Aurora dans le Guide de l'utilisateur Amazon Aurora.	10 juin 2020
Support pour la configuration des services à utiliser AWS Backup	Vous pouvez désormais configurer AWS Backup pour sauvegarder les ressources de AWS services spécifiques. Pour plus d'informations, voir Activer la gestion des services avec AWS Backup.	20 mai 2020
Prise en charge de la sauvegarde d'instances Amazon EC2 et ajout de la prise en charge des sauvegardes entre régions	Vous pouvez désormais sauvegarder des instances Amazon EC2 entières et copier des ressources entre Régions AWS. Pour plus d'informations, consultez Création de copies de sauvegardes entre Régions AWS.	13 janvier 2020
Nouveau guide	AWS AWS Backup les lancements et le guide du AWS Backup développeur.	15 janvier 2019

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.