Guía para desarrolladores

AWS Backup

AWS Backup: Guía para desarrolladores

Table of Contents

¿Qué es AWS Backup?

AWS Backup es un servicio totalmente gestionado que facilita la centralización y la automatización de la protección de datos en todos los AWS servicios, en la nube y en las instalaciones. Con este servicio, puede configurar las políticas de respaldo y monitorear la actividad de sus AWS recursos en un solo lugar. Le permite automatizar y consolidar las tareas de respaldo que se service-by-service realizaban anteriormente y elimina la necesidad de crear scripts personalizados y procesos manuales. Con unos pocos clics en la consola de AWS Backup , puede automatizar sus políticas y programas de protección de datos.

AWS Backup no regula las copias de seguridad que realice en su AWS entorno externo AWS Backup. Por lo tanto, si desea una end-to-end solución centralizada para cumplir con los requisitos empresariales y normativos, empiece a utilizarla AWS Backup hoy mismo.

Descripción general de las características

AWS Backup ofrece muchas funciones y capacidades, entre las que se incluyen las siguientes.

Administración centralizada de copias de seguridad

AWS Backup proporciona una consola de respaldo centralizada, un conjunto de API de respaldo y la opción AWS Command Line Interface (AWS CLI) para administrar los respaldos de los AWS servicios que utilizan sus aplicaciones. Con ella AWS Backup, puede administrar de forma centralizada las políticas de respaldo que cumplan con sus requisitos de respaldo. A continuación, puede aplicarlas a sus AWS recursos en todos los AWS servicios, lo que le permitirá realizar copias de seguridad de los datos de sus aplicaciones de forma coherente y conforme a las normas. La consola de backup AWS Backup centralizada ofrece una vista consolidada de las copias de seguridad y los registros de actividad de las copias de seguridad, lo que facilita la auditoría de las copias de seguridad y garantiza el cumplimiento.

Copias de seguridad basadas en políticas

Con AWS Backup ella, puede crear políticas de respaldo conocidas como planes de respaldo. Utilice estos planes de respaldo para definir sus requisitos de respaldo y, a continuación, aplíquelos a los AWS recursos que desee proteger en todos los AWS servicios que utilice. Puede crear distintos planes de copias de seguridad de forma que cada uno de ellos cumpla requisitos específicos empresariales y de conformidad normativa. Esto ayuda a garantizar que se realice una copia de

seguridad de cada AWS recurso de acuerdo con sus requisitos. Los planes de copias de seguridad facilitan el cumplimiento de la estrategia de copias de seguridad en la organización y en las aplicaciones de manera escalable.

Para ver todas las opciones de configuración de los planes de copia de seguridad, consulte Opciones y configuración del plan de copia de seguridad.

Políticas de copia de seguridad basadas en etiquetas

Puede utilizarlos AWS Backup para aplicar planes de respaldo a sus AWS recursos de diversas formas, incluso etiquetándolos. El etiquetado facilita la implementación de su estrategia de respaldo en todas sus aplicaciones y garantiza que todos sus AWS recursos estén respaldados y protegidos. AWS las etiquetas son una forma excelente de organizar y clasificar AWS los recursos. La integración con AWS etiquetas le permite aplicar rápidamente un plan de copia de seguridad a un grupo de AWS recursos, de forma que se realice una copia de seguridad coherente y conforme a las normas.

Para ver todas las formas en que puede asignar sus recursos a los planes de copia de seguridad, consulte Asignación de recursos a un plan de copia de seguridad.

Políticas de administración del ciclo de vida

AWS Backup le permite cumplir con los requisitos de conformidad y, al mismo tiempo, minimizar los costos de almacenamiento de las copias de seguridad al almacenar las copias de seguridad en un nivel de almacenamiento en frío de bajo costo. Puede configurar políticas de ciclo de vida que trasladarán automáticamente copias de seguridad de un almacenamiento en caliente a otro en frío en función del programa que defina.

Para obtener una lista de los recursos que pueden realizar la transición a almacenamiento en frío, consulte Disponibilidad de características por recurso. Para ver los pasos a seguir para activar el almacenamiento en frío en su plan de copias de seguridad, consulte los niveles de ciclo de vida y almacenamiento.

Copias de seguridad entre regiones

Con él AWS Backup, puede copiar copias de seguridad a varios tipos de copias Regiones de AWS de seguridad bajo demanda o automáticamente como parte de un plan de copias de seguridad programado. Las copias de seguridad entre regiones resultan especialmente útiles si los requisitos de continuidad del negocio o de conformidad exigen que se almacenen copias de seguridad a una

distancia mínima de los datos de producción. Para obtener más información, consulte Creación de copias de las copias de seguridad entre Regiones de AWS.

Administración entre cuentas y copias de seguridad entre cuentas

Puede usarlo AWS Backup para administrar sus copias de seguridad en todo el Cuentas de AWS interior de su AWS Organizationsestructura. Con la administración entre cuentas, puede utilizar automáticamente políticas de copia de seguridad para aplicar planes de copia de seguridad en las Cuentas de AWS de su organización. Esto hace que el cumplimiento de normas y la protección de datos sean eficientes de forma escalable y reduce el gasto operativo. También ayuda a eliminar la duplicación manual de planes de copias de seguridad en cuentas individuales. Para obtener más información, consulte Administración de recursos de AWS Backup en varias Cuentas de AWS.

También puede copiar las copias de seguridad en varios sitios diferentes Cuentas de AWS dentro de su estructura AWS Organizations de gestión. De esta forma, puede “agrupar” las copias de seguridad en una sola cuenta de repositorio y, a continuación, “distribuir” las copias de seguridad para aumentar la resiliencia. Creación de copias de las copias de seguridad entre Cuentas de AWS.

Para poder utilizar las características de administración entre cuentas y copia de seguridad entre cuentas, debe tener configurada una estructura de organización existente en AWS Organizations. Una unidad organizativa (OU) es un grupo de cuentas que se pueden administrar como una sola entidad. AWS Organizations es una lista de cuentas que se pueden agrupar en unidades organizativas y administrar como una sola entidad.

Auditoría e informes con AWS Backup Audit Manager

AWS Backup Audit Manager le ayuda a simplificar la gobernanza de los datos y la gestión del cumplimiento de todas sus copias de seguridad AWS. AWS Backup Audit Manager proporciona controles integrados y personalizables que puede alinear con los requisitos de su organización. También puede usar estos controles para realizar un seguimiento automático de sus actividades y recursos de copia de seguridad.

AWS Backup Audit Manager puede ayudarle a localizar actividades y recursos específicos que aún no cumplen con los controles que ha definido. También genera informes diarios que puede utilizar para mostrar la conformidad de sus controles a lo largo del tiempo.

Para incluir su conformidad en materia de backup junto con su postura general de conformidad, puede importar automáticamente las conclusiones de AWS Backup Audit Manager a AWS Audit Manager.

Copias de seguridad incrementales

AWS Backup almacena de forma eficiente sus copias de seguridad periódicas de forma incremental. La primera copia de seguridad de un recurso de AWS hace una copia de seguridad completa de sus datos. Para cada copia de seguridad incremental sucesiva, solo se respaldan los cambios en sus AWS recursos. Las copias de seguridad incrementales le permiten beneficiarse de la protección de datos que ofrecen las copias de seguridad frecuentes y, al mismo tiempo, minimizar los costos de almacenamiento.

Para obtener una lista de los recursos que admiten copias de seguridad incrementales, consulte Disponibilidad de características por recurso.

AWS Backup Administración completa

Algunos tipos de recursos admiten una AWS Backup administración completa. Los beneficios de la AWS Backup administración completa incluyen:

- Cifrado independiente. AWS Backup cifra automáticamente las copias de seguridad con la clave KMS de su AWS Backup almacén, en lugar de utilizar la misma clave de cifrado que el recurso fuente. Esto aumenta sus niveles de defensa. Para obtener más información, consulte Cifrado de copias de seguridad en AWS Backup.
- Nombre de recurso de Amazon (ARN) de **`awsbackup`** Los ARN de copia de seguridad comienzan con `arn:aws:backup` en lugar de `arn:aws:`*`source-resource`*. Esto le permite crear políticas de acceso que se apliquen específicamente a las copias de seguridad y no a los recursos de origen. Para obtener más información, consulte Control de acceso.
- Facturación de copias de seguridad centralizada y etiquetas de asignación de costos de Cost Explorer. Los cargos AWS Backup (incluidos el almacenamiento, las transferencias de datos, las restauraciones y la eliminación anticipada) aparecen en la sección «Backup» de tu Amazon Web Services factura, en lugar de aparecer en cada recurso admitido. También puede usar las etiquetas de asignación de costos de Cost Explorer para hacer un seguimiento y optimizar sus costos de copia de seguridad. Para obtener más información, consulte Medición, costos y facturación.

Para ver qué tipos de recursos son aptos para una AWS Backup administración completa, consulteDisponibilidad de características por recurso.

Monitorización de la actividad de copia de seguridad

AWS Backup proporciona un panel que facilita la auditoría de la actividad de copia de seguridad y restauración en todos AWS los servicios. Con solo unos pocos clics en la AWS Backup consola, puede ver el estado de los trabajos de copia de seguridad recientes. También puede restaurar los trabajos en todos AWS los servicios para garantizar que sus AWS recursos estén debidamente protegidos.

AWS Backup se integra con Amazon CloudWatch y Amazon EventBridge. CloudWatch permite realizar un seguimiento de las métricas y crear alarmas. EventBridge le permite ver y monitorear AWS Backup los eventos. Para obtener más información, consulte Supervisión de AWS Backup eventos mediante EventBridge y Supervisión de AWS Backup métricas con CloudWatch.

AWS Backup se integra con AWS CloudTrail. CloudTrail le ofrece una vista consolidada de los registros de actividad de respaldo que permite auditar rápida y fácilmente la forma en que se respaldan sus recursos. AWS Backup también se integra con Amazon Simple Notification Service (Amazon SNS) y le proporciona notificaciones sobre la actividad de las copias de seguridad, como cuando una copia de seguridad se realiza correctamente o se ha iniciado una restauración. Para obtener más información, consulte Registrar llamadas a la AWS Backup API con Amazon SNS CloudTrail y usar Amazon SNS para realizar un seguimiento AWS Backup de los eventos.

Seguridad de los datos en los almacenes de copias de seguridad

El contenido de cada AWS Backup copia de seguridad es inmutable, lo que significa que nadie puede modificarlo. AWS Backup protege aún más sus copias de seguridad en almacenes de copias de seguridad, lo que las separa de forma segura de sus instancias de origen. Por ejemplo, su almacén retendrá las copias de seguridad de Amazon EC2 y Amazon EBS de acuerdo con la política de ciclo de vida que elija, incluso si elimina la instancia de Amazon EC2 de origen y los volúmenes de Amazon EBS.

Los almacenes de copias de seguridad ofrecen cifrado y políticas de acceso basadas en recursos que le permiten definir quién tiene acceso a las copias de seguridad. Puede definir políticas de acceso para un almacén de copias de seguridad que define quién tiene acceso a las copias de seguridad dentro de ese almacén y qué acciones se les permite realizar. Esto proporciona una forma sencilla y segura de controlar el acceso a sus copias de seguridad en todos los servicios. AWS Para revisar AWS las políticas administradas por el cliente AWS Backup, consulte Políticas administradas para AWS Backup.

Puedes usar AWS Backup Vault Lock para evitar que cualquier persona (incluido tú) elimine las copias de seguridad o altere su período de retención. AWS Backup Vault Lock te ayuda a reforzar un modelo write-once-read-many(WORM) y a añadir otro nivel de defensa a tu defensa en profundidad. Para empezar, consulte Bloqueo de almacenes de AWS Backup.

Ayuda con las obligaciones de conformidad

AWS Backup le ayuda a cumplir sus obligaciones de conformidad globales. AWS Backup está dentro del ámbito de los siguientes programas AWS de cumplimiento:

- FedRAMP High
- RGPD
- SOC 1, 2 y 3
- PCI
- HIPAA
- y muchos más

Introducción

Para obtener más información AWS Backup, le recomendamos que comience conEmpezar con AWS Backup.

AWS Recursos y aplicaciones compatibles

Los siguientes son AWS recursos y aplicaciones de terceros de los que puede hacer copias de seguridad y restaurar AWS Backup. Para obtener más información, consulte the section called “Disponibilidad de características”.

Servicio	Tipos de recursos admitidos
Amazon Elastic Compute Cloud (Amazon EC2)	Instancias de Amazon EC2 (excluidas las AMI con copia de seguridad en el almacén de instancias)
Amazon Simple Storage Service (Amazon S3)	Datos de Amazon S3

Servicio	Tipos de recursos admitidos
Amazon Elastic Block Store (Amazon EBS)	Volúmenes de Amazon EBS
Amazon DynamoDB	Tablas de Amazon DynamoDB.
Amazon Relational Database Service (Amazon RDS)	Instancias de bases de datos de Amazon RDS (incluidos todos los motores de bases de datos); clústeres de varias zonas de disponibilidad
Amazon Aurora	Clústeres de Aurora
Amazon Elastic File System (Amazon EFS)	Sistemas de archivos de Amazon EFS
FSx para Lustre	Sistemas de archivos de FSx para Lustre
FSx para Windows File Server	Sistemas de archivos de FSx para Windows File Server
Amazon FSx para ONTAP NetApp	Sistemas de archivos de FSx para ONTAP
Amazon FSx para OpenZFS	Sistemas de archivos de FSx para OpenZFS
AWS Storage Gateway (Volume Gateway)	AWS Storage Gateway volúmenes
Amazon DocumentDB	Clústeres basados en instancias de Amazon DocumentDB
Amazon Neptune	Clústeres de Amazon Neptune
Amazon Redshift	Clústeres de Amazon Redshift
Amazon Timestream	Tablas de Amazon Timestream
VMware Cloud™ en AWS	Máquinas virtuales VMware Cloud™ activadas AWS

Servicio	Tipos de recursos admitidos
VMware Cloud™ activado AWS Outposts	Máquinas virtuales VMware Cloud™ activadas AWS Outposts
AWS CloudFormation	AWS CloudFormation pilas
Bases de datos de SAP HANA	Bases de datos de SAP HANA en instancias de Amazon EC2

Precios

Con AWS Backup, usted paga por el almacenamiento de copias de seguridad, la restauración de datos, las pruebas de restauración, la transferencia de datos entre regiones y AWS Backup Audit Manager. Para obtener más información, consulte AWS Backup Precios.

AWS Backup disponibilidad de funciones

AWS Backup las funciones se ofrecen según el recurso y Región de AWS. Las siguientes secciones y tablas pueden ayudarle a determinar la disponibilidad de las características.

Contenido

Características disponibles para todos los recursos compatibles

AWS Backup ofrece las siguientes funciones para sus AWS servicios compatibles, así como para las aplicaciones de terceros compatibles. No se debe dar por hecho que una característica o servicio es compatible, a menos que se mencione explícitamente.

- Programación de copias de seguridad automatizada y administración de la retención
- Monitorización centralizada de las copias de seguridad

- Respaldos cifrados
- Respaldos incrementales
- Gestión multicuenta con AWS Organizations
- Auditorías e informes de respaldo automatizados con AWS Backup Audit Manager
- Escribe una vez y lee muchas veces (WORM) con Vault Lock AWS Backup

Disponibilidad de características por recurso

Para usarlo AWS Backup con un AWS servicio compatible en una región en particular, el servicio debe estar disponible en la región. Para determinar la disponibilidad del servicio en una región, consulte los puntos finales del Referencia general de AWSservicio en.

AWS Backup admite	Copias de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copias de seguridad incrementales	Respaldo y point-in-time restauración continuos	Administración completa	Del ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento [1]	Restaurar las pruebas
Amazon	✓	✓	✓	✓					✓
Amazon	✓	✓	✓	✓	✓	✓		✓	✓
Amazon EBS	✓	✓	✓	✓			✓		✓
Instancia única de Amazon RDS	✓ [3]	✓ [3]	✓ [4]	✓	✓				✓
Clúster de Amazon	✓ [3]	✓ [3]	✓ [4]	✓					✓

AWS Backup admite	Copias de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copias de seguridad incrementales	Respaldo y point-in-time restauración continuos	Administración completa	Del ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento [1]	Restaurar las pruebas
Amazon Aurora	✓ [3]	✓ [3]	✓	✓ [6]	✓				✓
Amazon	✓	✓	✓	✓		✓	✓	✓	✓
FSx para Lustre	✓	✓	✓	✓					✓
FSx para Windows File Server	✓	✓	✓	✓					✓
FSx para ONTAP			✓ [2]	✓					✓
FSx para OpenZFS	✓	✓	✓	✓					✓
AWS Storage Gateway	✓	✓	✓	✓					
Amazon Documen B	✓ [3]	✓ [3]	✓						✓

AWS Backup admite	Copias de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copias de seguridad incrementales	Respaldo y point-in-time restauración continuos	Administración completa	Del ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento [1]	Restaurar las pruebas
Amazon Neptune	✓ [3]	✓ [3]	✓						✓
Amazon Redshift								✓	
Timestream	✓	✓	✓	✓		✓	✓	✓	
Windows VSS	✓	✓	✓	✓					
Máquinas virtuales	✓	✓	✓	✓		✓	✓	✓	
AWS CloudFormation plantillas	✓	✓		✓ [5]		✓	✓ [5]		
Amazon DynamoDB			✓						✓

AWS Backup admite	Copias de seguridad entre regiones	Copia de seguridad entre cuentas	AWS Backup Audit Manager	Copias de seguridad incrementales	Respaldo y point-in-time restauración continuos	Administración completa	Del ciclo de vida al almacenamiento en frío	Restauración a nivel de elemento [1]	Restaurar las pruebas
Dynamol con características avanzadas de AWS Backup	✓	✓	✓			✓	✓		✓
Bases de datos de SAP HANA en instancias de Amazon EC2				✓	✓	✓	✓		

Algunos tipos de recursos tienen capacidades de copia de seguridad continua y copia entre regiones y entre cuentas. Cuando se realiza una copia entre regiones o entre cuentas de una copia de seguridad continua, el punto de recuperación copiado (copia de seguridad) se convierte en una copia de seguridad de instantánea (periódica). Amazon RDS y Amazon S3 admiten copias instantáneas incrementales; Amazon Aurora solo admite copias instantáneas completas. La PITR (restauración en un momento dado) no está disponible para estas copias.

[1] El «elemento» de una restauración a nivel de elemento varía en función del recurso compatible. Por ejemplo, un elemento del sistema de archivos es un archivo o directorio, mientras que un elemento de S3 es un objeto de S3. Un elemento de VMware es un disco. Para obtener más información, consulte la sección Restauración de una copia de seguridad del recurso compatible.

[2] AWS Backup Audit Manager admite este recurso en todos los controles, excepto en la copia multicuenta y en la copia interregional.

[3] RDS, Aurora, DocumentDB y Neptune no admiten una sola acción de copia que realice copias de seguridad entre regiones y entre cuentas. Debe elegir una u otra. También puede usar un AWS Lambda script para escuchar cómo se ha completado la primera copia, ejecutar la segunda copia y, a continuación, eliminar la primera copia. Las instancias de base de datos de varias zonas de disponibilidad (Multi-AZ) de RDS se pueden copiar, pero los clústeres de Multi-AZ no admiten la copia entre regiones o entre cuentas en estos momentos. Consulte Consideraciones sobre la copia entre regiones con recursos específicos para obtener más información.

[4] Consulte las copias de seguridad de zonas de disponibilidad múltiple de RDS para ver las regiones en las que está disponible el soporte de Backup Audit Manager.

[5] En las copias de seguridad CloudFormation apiladas, los recursos anidados conservan las características de sus recursos de origen. Sin embargo, los recursos de la pila no conservan la funcionalidad de restauración puntual (PITR) (como Amazon S3 y Amazon RDS). Las propiedades de la matriz anterior se aplican solo a las CloudFormation plantillas y no a los recursos de la pila.

[6] En el caso de Aurora, las instantáneas están completas y se ofrece una copia de seguridad incremental mediante PITR.

Disponibilidad de las funciones por Región de AWS

AWS Backup está disponible en todo lo siguiente Regiones de AWS. AWS Backup las funciones están disponibles en todas estas regiones, a menos que se indique lo contrario en la siguiente tabla.

AWS Backup apoya	Copias de seguridad entre regiones	Administración entre cuentas	Copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Restaurar las pruebas
Este de EE. UU. (Norte de Virginia)	✓	✓	✓	✓	✓
Este de EE. UU. (Ohio)	✓	✓	✓	✓	✓
Oeste de EE. UU. (Norte de California)	✓	✓	✓	✓	✓
Oeste de EE. UU. (Oregón)	✓	✓	✓	✓	✓
África (Ciudad del Cabo)	✓		✓	✓	✓
Asia-Pacífico (Hong Kong)	✓		✓	✓	✓
Asia-Pacífico (Hyderabad)	✓		✓		✓
Asia-Pacífico (Yakarta)	✓		✓		✓

AWS Backup apoya	Copias de seguridad entre regiones	Administración entre cuentas	Copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Restaurar las pruebas
Asia-Pacífico (Melbourne)	✓		✓		✓
Asia-Pacífico (Bombay)	✓	✓	✓	✓	✓
Asia-Pacífico (Osaka)	✓	✓	✓		✓
Asia-Pacífico (Seúl)	✓	✓	✓	✓	✓
Asia-Pacífico (Singapur)	✓	✓	✓	✓	✓
Asia-Pacífico (Sídney)	✓	✓	✓	✓	✓
Asia-Pacífico (Tokio)	✓	✓	✓	✓	✓
Canadá (centro)	✓	✓	✓	✓	✓
Oeste de Canadá (Calgary	✓ (excepto Amazon S3)		✓		
China (Pekín)	✓				
China (Ningxia)	✓				

AWS Backup apoya	Copias de seguridad entre regiones	Administración entre cuentas	Copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Restaurar las pruebas
Europa (Fráncfort)	✓	✓	✓	✓	✓
Europa (Irlanda)	✓	✓	✓	✓	✓
Europa (Londres)	✓	✓	✓	✓	✓
Europa (Milán)	✓		✓	✓	✓
Europa (París)	✓	✓	✓	✓	✓
Europa (España)	✓		✓		✓
Europa (Estocolmo)	✓	✓	✓	✓	✓
Europa (Zúrich)	✓		✓		✓
Israel (Tel Aviv)	✓		✓		
Medio Oriente (Baréin)	✓		✓	✓	✓

AWS Backup apoya	Copias de seguridad entre regiones	Administración entre cuentas	Copia de seguridad entre cuentas	AWS Backup Panel de control de Audit Manager y trabajos	Restaurar las pruebas
Medio Oriente (EAU)	✓		✓		✓
América del Sur (São Paulo)	✓	✓	✓	✓	✓
AWS GovCloud (Este de EE. UU.)	✓	✓	✓	✓	
AWS GovCloud (Estados Unidos-Oeste)	✓	✓	✓	✓	

China (Pekín) y China (Ningxia) admiten copias entre regiones de una de estas dos regiones a la otra. No se admiten copias entre regiones desde estas regiones a otras regiones o a estas regiones. No se admite la copia entre cuentas para estas regiones.

El panel de empleos no está disponible en AWS GovCloud (EE. UU. Este) ni (EE. UU. AWS GovCloud Oeste). La agregación del panel de empleos solo está disponible en las regiones que admiten la administración multicuenta y AWS Backup Audit Manager.

Amazon FSx for Windows File Server y Amazon Neptune no admiten copias de seguridad entre regiones en las regiones en las que se haya optado por participar.

Servicios compatibles con Región de AWS

AWS Backup admite lo siguiente en todas las regiones compatibles:

- Aurora
- DynamoDB
- DynamoDB con funciones avanzadas AWS Backup
- Amazon EBS
- Amazon EC2
- Amazon EFS
- Amazon Redshift
- Amazon RDS

En la siguiente tabla se indica la AWS Backup compatibilidad con otros sistemas Servicios de AWS por región.

Usuarios y regiones	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware y Backup Gateway
Este de EE. UU. (Norte de Virginia)	✓	✓	✓	✓	✓	✓
Este de EE. UU. (Ohio)	✓	✓	✓	✓	✓	✓
Oeste de EE. UU. (Norte de California)	Windows; Lustre; ONTAP	✓	✓	✓		✓

Usuarios y regiones	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware y Backup Gateway
Oeste de EE. UU. (Oregón)	Windows; Lustre; ONTAP	✓	✓	✓	✓	✓
África (Ciudad del Cabo)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Asia-Pacífico (Hong Kong)	✓	✓	✓ [1]	✓		✓
Asia-Pacífico (Hyderabad)	Windows; Lustre; ONTAP		✓ [1]	✓		
Asia-Pacífico (Yakarta)	Windows; Lustre; ONTAP		✓	✓		
Asia-Pacífico (Melbourne)	Windows; Lustre; ONTAP		✓ [1]	✓		
Asia-Pacífico (Bombay)	✓	✓	✓	✓		✓
Asia-Pacífico (Osaka)	Windows; Lustre	✓	✓ [1]	✓		✓

Usuarios y regiones	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware y Backup Gateway
Asia-Pacífico (Seúl)	✓	✓	✓	✓		✓
Asia-Pacífico (Singapur)	✓	✓	✓	✓		✓
Asia-Pacífico (Sídney)	✓	✓	✓	✓	✓	✓
Asia-Pacífico (Tokio)	✓	✓	✓	✓	✓	✓
Canadá (centro)	✓	✓	✓	✓		✓
Oeste de Canadá (Calgary						
China (Pekín)	Windows; Lustre		✓ [1]	✓	✓	
China (Ningxia)	Windows; Lustre		✓ [1]	✓	✓	
Europa (Fráncfort)	✓	✓	✓	✓	✓	✓
Europa (Irlanda)	✓	✓	✓	✓	✓	✓

Usuarios y regiones	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware y Backup Gateway
Europa (Londres)	✓	✓	✓	✓		✓
Europa (Milán)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Europa (París)	Windows; Lustre; ONTAP	✓	✓	✓		✓
Europa (España)	Windows; Lustre; ONTAP		✓ [1]	✓		
Europa (Estocolmo)	✓	✓	✓	✓		✓
Europa (Zúrich)	Windows; Lustre; ONTAP		✓ [1]	✓		
Israel (Tel Aviv)	Windows; Lustre; ONTAP		✓ [1]	✓		
Medio Oriente (Baréin)	Windows; Lustre; ONTAP	✓	✓ [1]	✓		✓
Medio Oriente (EAU)			✓ [1]	✓		

Usuarios y regiones	Amazon FSx	SAP HANA en instancias EC2	Amazon S3	Storage Gateway	Amazon Timestream	VMware y Backup Gateway
América del Sur (São Paulo)		✓	✓	✓		✓
AWS GovCloud (EE. UU.-Oeste)	Windows; Lustre; ONTAP		✓ [1]	✓		✓
AWS GovCloud (EEUU-Este)	Windows; Lustre; ONTAP		✓ [1]	✓		✓

Una comprobación en Amazon FSx indica que FSx for Windows File Server, fSx for Lustre, fSx for ONTAP y FSx for OpenZFS son compatibles en esa región; de lo contrario, aparecerán en la lista las configuraciones compatibles. AWS Backup

1 No se admiten copias entre regiones y cuentas.

AWS Backup: Cómo funciona

AWS Backup es un servicio de copias de seguridad totalmente gestionado que facilita la centralización y automatización de las copias de seguridad de los datos en todos los AWS servicios. Con él AWS Backup, puede crear políticas de respaldo denominadas planes de respaldo. Puede utilizar estos planes para definir los requisitos de copia de seguridad, como la frecuencia con la que se va a realizar la copia de seguridad de los datos y el tiempo durante el que se van a conservar esas copias de seguridad.

AWS Backup le permite aplicar planes de respaldo a sus AWS recursos simplemente etiquetándolos. AWS Backup a continuación, realiza automáticamente una copia de seguridad de sus AWS recursos de acuerdo con el plan de copia de seguridad que haya definido.

En las siguientes secciones se describe cómo AWS Backup funciona, los detalles de su implementación y las consideraciones de seguridad.

Temas

¿Cómo AWS Backup funciona con AWS los servicios compatibles

Algunos AWS servicios AWS Backup compatibles ofrecen sus propias funciones de copia de seguridad independientes. Esas características están disponibles independientemente de si utiliza AWS Backup. Sin embargo, las copias de seguridad que crean otros AWS servicios no están disponibles para el gobierno central. AWS Backup

AWS Backup Para configurar la gestión centralizada de la protección de datos de todos los servicios compatibles, debe optar por gestionar ese servicio AWS Backup, crear una copia de seguridad a pedido o programar copias de seguridad mediante un plan de copias de seguridad y almacenar las copias de seguridad en bóvedas de copias de seguridad.

Temas

- Uso de máquinas virtuales de VMware
- Uso de Amazon DynamoDB
- Uso de sistemas de archivos de Amazon FSx
- Uso de Amazon EC2
- Uso de Amazon EFS
- Uso de Amazon EBS
- Uso de Amazon RDS Y Aurora
- ¿Trabajando con AWS BackInt
- Trabajando con AWS Storage Gateway
- Uso de Amazon DocumentDB
- Uso de Amazon Neptune
- Uso de Amazon Timestream
- Trabajando con AWS Organizations
- Trabajando con AWS CloudFormation
- Trabajando con AWS BackInt, AWS Systems Manager para SAP y SAP HANA
- ¿Cómo respaldan AWS los servicios sus propios recursos

Opte por gestionar los servicios con AWS Backup

Cuando haya nuevos AWS servicios disponibles, debe AWS Backup habilitar el uso de esos servicios. Si intenta crear una copia de seguridad bajo demanda o con un plan de copia de seguridad utilizando recursos de un servicio que no está habilitado, aparecerá un mensaje de error y el proceso no se completará.

La AWS Backup consola tiene dos formas de incluir los tipos de recursos en un plan de respaldo: asignar explícitamente el tipo de recurso en un plan de respaldo o incluir todos los recursos. Consulte los puntos siguientes para entender cómo funcionan estas selecciones con las suscripciones a servicios.

- Si las asignaciones de recursos se basan únicamente en etiquetas, se aplica la configuración de suscripción al servicio.
- Si un tipo de recurso se asigna explícitamente a un plan de respaldo, se incluirá en el respaldo incluso si la opción no está habilitada para ese servicio en particular. Esto no se aplica a Aurora, Neptune ni Amazon DocumentDB. Para incluir estos servicios, la suscripción debe estar habilitada.

- Si se especifican tanto el tipo de recurso como las etiquetas en una asignación de recursos, los tipos de recursos especificados se filtran primero y, a continuación, las etiquetas filtran aún más esos recursos.

  La configuración de suscripción del servicio se ignora en la mayoría de los tipos de recursos. Sin embargo, Aurora, Neptune y Amazon DocumentDB requieren la suscripción del servicio.
- En el caso de Amazon FSx para NetApp ONTAP, cuando utilice la selección de recursos basada en etiquetas, aplique etiquetas a volúmenes individuales en lugar de a todo el sistema de archivos.

La configuración de suscripción del servicio es específica de cada región. Cuando una cuenta utiliza AWS Backup (crea una bóveda de respaldo o un plan de respaldo) en una región, la cuenta se incluye automáticamente en todos los tipos de recursos admitidos por la región AWS Backup en ese momento. Los servicios compatibles que se agreguen a esa región en una fecha posterior no se incluirán automáticamente en un plan de respaldo. Puede optar por utilizar esos tipos de recursos una vez que se admitan.

Para configurar los servicios utilizados con AWS Backup

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, seleccione Configuración.
3. En la página Activación del servicio, elija Configurar recursos.
4. Utilice los conmutadores para activar o desactivar los servicios utilizados con AWS Backup.

   > **Important**
   >
   > RDS, Aurora, Neptune y DocumentDB comparten el mismo nombre de recurso de Amazon (ARN). Al optar por administrar uno de estos tipos de recursos, se AWS Backup habilitan todos ellos al asignarlo a un plan de respaldo. En cualquier caso, le recomendamos que se suscriba a todos ellos para representar con precisión su estado de suscripción.
5. Elija Confirmar.

Uso de datos de Amazon S3

AWS Backup ofrece copias de seguridad y restauración totalmente gestionadas para las copias de seguridad de Amazon S3. Para obtener más información, consulte Copias de seguridad de Amazon S3.

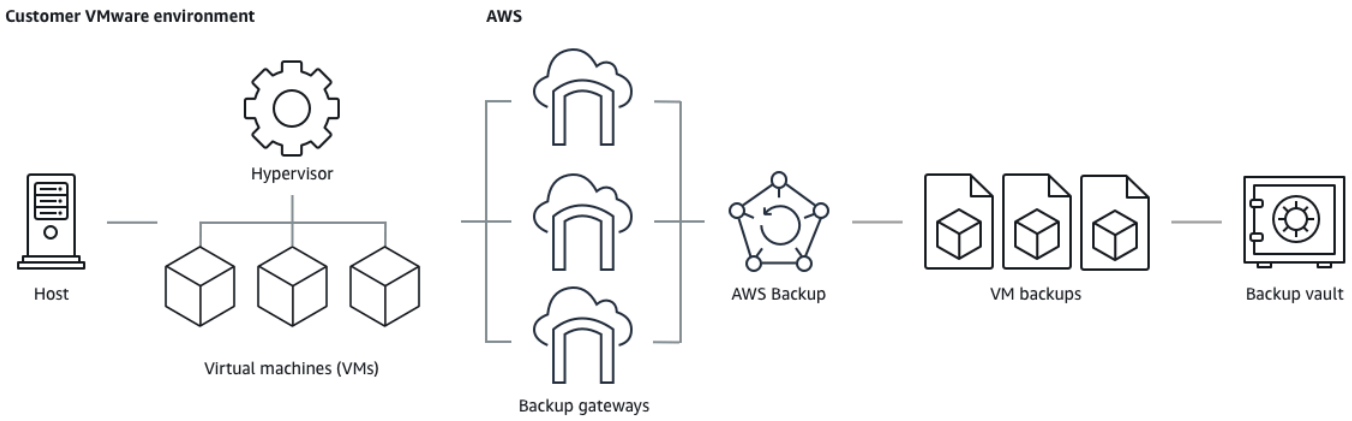
- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los datos de Amazon S3 mediante AWS Backup: Restauración de datos de S3

Para obtener información detallada acerca de S3, consulte la Documentación de Amazon S3.

Uso de máquinas virtuales de VMware

AWS Backup admite la protección de datos centralizada y automatizada para las máquinas virtuales (VM) VMware locales y las máquinas virtuales en VMware Cloud™ (VMC) on. AWS Puede realizar copias de seguridad desde sus máquinas virtuales locales y de VMC hasta. AWS Backup A continuación, puede realizar la restauración desde AWS Backup una ubicación local o desde VMC.

Backup Gateway es un AWS Backup software descargable que se implementa en las máquinas virtuales de VMware para conectarlas a AWS Backup ellas. La puerta de enlace se conecta a su servidor de administración de máquinas virtuales para detectar las máquinas virtuales, cifrar datos y transferirlos eficazmente a AWS Backup. El siguiente diagrama ilustra cómo se conecta la puerta de enlace de copia de seguridad a las máquinas virtuales:



- Cómo hacer copias de seguridad de los recursos: Copias de seguridad de máquinas virtuales
- Cómo restaurar los recursos de la máquina virtual: Restauración de una máquina virtual mediante AWS Backup

Uso de Amazon DynamoDB

AWS Backup admite la creación de copias de seguridad y la restauración de tablas de Amazon DynamoDB. DynamoDB es un servicio de bases de datos NoSQL completamente administrado que proporciona un rendimiento rápido y predecible, así como una perfecta escalabilidad.

Desde su lanzamiento, siempre AWS Backup ha sido compatible con DynamoDB. A partir de noviembre de 2021, AWS Backup también se introdujeron funciones avanzadas para las copias de seguridad de DynamoDB. Estas funciones avanzadas incluyen copiar las copias de seguridad entre cuentas Regiones de AWS y cuentas, organizar las copias de seguridad en niveles para almacenarlas en frío y utilizar etiquetas para gestionar los permisos y los costes.

AWS Backup Los nuevos clientes que se incorporen después de noviembre de 2021 tendrán las funciones avanzadas de copia de seguridad de DynamoDB habilitadas de forma predeterminada.

Recomendamos a todos los AWS Backup clientes actuales que habiliten las funciones avanzadas de DynamoDB. No hay diferencia en los precios del almacenamiento de copias de seguridad en caliente después de habilitar las características avanzadas, y puede ahorrar dinero al organizar las copias de seguridad en niveles en el almacenamiento en frío y optimizar sus costos mediante el uso de etiquetas de asignación de costos.

Para obtener una lista completa de las características avanzadas y cómo habilitarlas, consulte Copia de seguridad avanzada de DynamoDB.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los recursos de DynamoDB: Restauración de una tabla de Amazon DynamoDB

Para obtener información detallada acerca de DynamoDB, consulte ¿Qué es Amazon DynamoDB? en la Guía para desarrolladores de Amazon DynamoDB.

Uso de sistemas de archivos de Amazon FSx

AWS Backup admite la creación de copias de seguridad y la restauración de los sistemas de archivos Amazon FSx. Amazon FSx proporciona sistemas de archivos de terceros totalmente gestionados con la compatibilidad nativa y los conjuntos de características para las cargas de trabajo. AWS Backup utiliza la funcionalidad de copia de seguridad integrada de Amazon FSx. Por lo tanto, las copias de seguridad realizadas desde la consola de AWS Backup tienen el mismo nivel de coherencia y rendimiento del sistema de archivos y las mismas opciones de restauración que las copias de seguridad que se realizan a través de la consola de Amazon FSx.

Si las utiliza AWS Backup para gestionar estas copias de seguridad, obtiene funciones adicionales, como opciones de retención ilimitadas y la posibilidad de crear copias de seguridad programadas con una frecuencia de hasta una hora. Además, AWS Backup conserva las copias de seguridad incluso después de eliminar el sistema de archivos de origen. Esto protege contra la eliminación accidental o malintencionada.

Úselo AWS Backup para proteger los sistemas de archivos Amazon FSx si desea configurar políticas de respaldo y supervisar las tareas de respaldo desde una consola de respaldo central que también amplíe el soporte para otros AWS servicios.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los recursos de Amazon FSx: Restauración de un sistema de archivos de FSx

Para obtener información detallada acerca de los sistemas de archivos de Amazon FSx, consulte Documentación de Amazon FSx.

Uso de Amazon EC2

AWS Backup admite instancias de Amazon EC2.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los recursos de Amazon EC2: Restauración de una instancia de Amazon EC2

Puede programar o realizar trabajos de backup bajo demanda que incluyan instancias EC2 completas, incluidos sus volúmenes de Amazon EBS. Por lo tanto, puede restaurar una instancia Amazon EC2 completa desde un único punto de recuperación, incluidos el volumen raíz, los volúmenes de datos y algunos ajustes de configuración de la instancia, como el tipo de instancia y el key pair.

También puede hacer copias de seguridad y restaurar las aplicaciones de Microsoft Windows habilitadas para VSS. Puede programar copias de seguridad coherentes con las aplicación, definir políticas de ciclo de vida y realizar restauraciones coherentes como parte de una copia de seguridad bajo demanda o de un plan de copia de seguridad programada. Para obtener más información, consulte Creación de copias de seguridad de Windows VSS.

AWS Backup no reinicia las instancias EC2 en ningún momento.

Imágenes e instantáneas

Al realizar una copia de seguridad de una instancia de Amazon EC2, AWS Backup toma una instantánea del volumen de almacenamiento raíz de Amazon EBS, las configuraciones de lanzamiento y todos los volúmenes de EBS asociados. AWS Backup almacena determinados parámetros de configuración de la instancia EC2, incluidos el tipo de instancia, los grupos de seguridad, Amazon VPC, la configuración de supervisión y las etiquetas. Los datos de copia de seguridad se almacenan como una Imagen de máquina de Amazon (AMI) respaldada por un volumen de Amazon EBS.

Si elimina una imagen de máquina de Amazon (AMI) o una instantánea de Amazon EBS gestionada AWS Backup mediante AWS Backup y tiene configurada la papelera de reciclaje de Amazon EC2, la imagen o la instantánea podrían incurrir en cargos según la política de papelera de reciclaje de Amazon EC2. Las instantáneas e imágenes de la papelera de reciclaje de Amazon EC2 ya no se gestionan ni se gestionarán AWS Backup AWS Backup mediante políticas si las restaura desde la papelera de reciclaje.

AWS Backup Las instantáneas gestionadas de Amazon EBS y las instantáneas asociadas a una AMI de AWS Backup Amazon EC2 gestionada que tengan aplicado el bloqueo de instantáneas de Amazon EBS no se pueden eliminar como parte del ciclo de vida del punto de recuperación si la duración del bloqueo de instantáneas supera el ciclo de vida de la copia de seguridad. Por el contrario, estos puntos de recuperación tendrán el estado de `EXPIRED`. Estos puntos de recuperación se pueden eliminar manualmente si decide eliminar primero el bloqueo de instantáneas de Amazon EBS.

AWS Backup puede cifrar las instantáneas de EBS asociadas a una copia de seguridad de Amazon EC2. Es similar a la forma en que cifra las instantáneas de EBS. AWS Backup utiliza el mismo cifrado aplicado a los volúmenes de EBS subyacentes al crear una instantánea de la AMI de Amazon EC2, y los parámetros de configuración de la instancia original se conservan en los metadatos de restauración.

El cifrado de una instantánea proviene del volumen y se aplica el mismo cifrado a las instantáneas correspondientes. Las instantáneas de EBS de una AMI copiada siempre están cifradas. Si especifica una clave KMS durante la copia, se aplica la clave especificada. Si no especificas una clave de KMS, se aplicará una clave de KMS predeterminada.

Para obtener más información, consulte las instancias de Amazon EC2 en la Guía del usuario de Amazon EC2 y el cifrado de Amazon EBS en la Guía del usuario de Amazon EBS.

Uso de Amazon EFS

AWS Backup es compatible con Amazon Elastic File System (Amazon EFS).

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los recursos de Amazon EFS: Restauración de un sistema de archivos de Amazon EFS

Para obtener información detallada acerca de los sistemas de archivos de Amazon EFS, consulte What is Amazon Elastic File System? en la Guía del usuario de Amazon Elastic File System.

Uso de Amazon EBS

AWS Backup admite volúmenes de Amazon Elastic Block Store (Amazon EBS).

AWS Backup Las instantáneas gestionadas de Amazon EBS y las instantáneas asociadas a una AMI de AWS Backup Amazon EC2 gestionada que tengan aplicado el bloqueo de instantáneas de Amazon EBS no se pueden eliminar como parte del ciclo de vida del punto de recuperación si la duración del bloqueo de instantáneas supera el ciclo de vida de la copia de seguridad. Por el contrario, estos puntos de recuperación tendrán el estado de `EXPIRED`. Estos puntos de recuperación se pueden eliminar manualmente si decide eliminar primero el bloqueo de instantáneas de Amazon EBS.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los volúmenes de Amazon EBS: Restauración de un volumen de Amazon EBS

Para obtener más información, consulte los volúmenes de Amazon EBS en la Guía del usuario de Amazon EBS.

Uso de Amazon RDS Y Aurora

AWS Backup admite los motores de bases de datos de Amazon RDS y los clústeres Aurora.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los recursos de Amazon RDS: Restauración de una base de datos de RDS
- Cómo restaurar los clústeres de Aurora: Restauración de un clúster de Amazon Aurora

Para obtener más información acerca de Amazon RDS, consulte ¿Qué es Amazon Relational Database Service? en la Guía del usuario de Amazon RDS.

Para obtener información detallada acerca de Aurora, consulte ¿Qué es Amazon Aurora? en la Guía del usuario de Amazon Aurora.

> **Note**
>
> Si inicia un trabajo de copia de seguridad desde la consola de Amazon RDS, esto puede entrar en conflicto con un trabajo de copia de seguridad de un clúster de Aurora y provocar el error El trabajo de copia de seguridad venció antes de completarse. Si ocurre esto, configure un intervalo de copia de seguridad más largo en AWS Backup.

> **Note**
>
> Actualmente, RDS Custom para SQL Server y RDS Custom para Oracle no son compatibles con AWS Backup.

> **Note**
>
> AWS no cobra por las instantáneas de Aurora almacenadas en un almacén de copias de seguridad siempre que Aurora tenga habilitadas las copias de seguridad automatizadas y el período de retención de las copias de seguridad automatizadas de Aurora sea superior al período de retención de las instantáneas de Aurora. Si se elimina la base de datos de las instantáneas, se cobrarán todas las instantáneas que se encuentren en el almacén de copias de seguridad (las eliminaciones pueden producirse accidentalmente o durante una implementación azul/verde).
> Las instantáneas de gran tamaño y las copias de seguridad frecuentes de una base de datos eliminada podrían conllevar gastos de almacenamiento significativos. Visite la calculadora de AWS Backup para estimar los posibles cargos de AWS Backup .

¿Trabajando con AWS BackInt

AWS Backup funciona con AWS Backint para respaldar y restaurar bases de datos de SAP HANA en instancias de Amazon EC2.

- Instrucciones para hacer copias de seguridad y restaurar los recursos de SAP HANA: copia de seguridad y restauración de instancias Amazon EC2 de SAP HANA
- Configurar AWS Backint Agent AWS : Backint Agent para SAP HANA

Trabajando con AWS Storage Gateway

AWS Backup es compatible con Storage Gateway Volume Gateway. También puede restaurar las instantáneas de Amazon EBS como volúmenes de Storage Gateway.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los recursos de Storage Gateway: Restauración de un volumen de Storage Gateway.

Uso de Amazon DocumentDB

AWS Backup admite clústeres de Amazon DocumentDB.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los recursos de Amazon DocumentDB:. Restauración de un clúster de DocumentDB

Uso de Amazon Neptune

AWS Backup es compatible con los clústeres de Amazon Neptune.

- Cómo hacer copias de seguridad de los recursos: Empezar con AWS Backup
- Cómo restaurar los clústeres de Amazon Neptune: Restauración de un clúster de Neptune.

Uso de Amazon Timestream

AWS Backup es compatible con las tablas Amazon Timestream.

- Cómo hacer copias de seguridad de las tablas de Timestream.
- Cómo restaurar las tablas de Timestream.

Trabajando con AWS Organizations

AWS Backup funciona AWS Organizations para simplificar el monitoreo y la administración entre cuentas

- Cree una cuenta de administración en Organizations.
- Active la administración entre cuentas.
- Designe cuentas de administrador delegado y delegue políticas.

Trabajando con AWS CloudFormation

AWS Backup AWS CloudFormation plantillas de soporte y pilas de aplicaciones

- AWS CloudFormation apile copias de seguridad

Trabajando con AWS BackInt, AWS Systems Manager para SAP y SAP HANA

AWS Backup trabaja con AWS BackInt y con SSM para SAP para dar soporte a las funciones de backup y restauración de SAP HANA.

- Copia de seguridad de bases de datos de SAP HANA en instancias de Amazon EC2
- Comience con AWS Systems Manager SAP
- AWS Backint Agent para SAP HANA

¿Cómo respaldan AWS los servicios sus propios recursos

Puede consultar la documentación técnica del proceso de copia de seguridad y restauración de un AWS servicio específico, especialmente si, durante una restauración, necesita configurar una nueva instancia de ese AWS servicio. A continuación se muestra una lista de la documentación:

- Servicios relacionados de Amazon EC2
- Uso AWS Backup con Amazon EFS
- Copia de seguridad y restauración bajo demanda para DynamoDB
- Instantáneas de Amazon EBS

- Copia de seguridad y restauración de instancias de base de datos de Amazon RDS
  - Información general de copias de seguridad y restauración de un clúster de base de datos de Aurora
- Uso AWS Backup con FSx para Windows File Server
- Uso AWS Backup con FSx for Lustre
- Realice copias de seguridad de sus volúmenes en AWS Storage Gateway
- Backing Up and Restoring in Amazon DocumentDB
- Backing Up and Restoring an Amazon Neptune Cluster

Medición, costos y facturación

AWS Backup precios

AWS Backup Los precios actuales están disponibles en AWS Backup los precios.

> **Important**
>
> Para evitar cargos adicionales, configure su política de retención con una duración de almacenamiento en caliente de al menos una semana.
> Por ejemplo, supongamos que realiza copias de seguridad diarias y las retiene durante un día. Además, suponga que sus recursos protegidos son tan grandes que se tarda todo el día en completar la copia de seguridad. AWS Backup implementa el período de retención de un día y retira la copia de seguridad del almacenamiento en caliente cuando finaliza la tarea de copia de seguridad. Al día siguiente, AWS Backup no puede crear una copia de seguridad incremental porque no tiene ninguna copia de seguridad en almacenamiento caliente. Dado que este periodo de retención no siguió las prácticas recomendadas, corre el riesgo y los gastos de crear una copia de seguridad completa todos los días.
> Póngase en contacto con nosotros AWS Support para obtener más ayuda.

AWS Backup facturación

Cuando un tipo de recurso admite la AWS Backup administración completa, los cargos por AWS Backup actividad (incluidos el almacenamiento, las transferencias de datos, las restauraciones y la eliminación anticipada) aparecen en la sección «Backup» de la Amazon Web Services factura. Para ver una lista de los servicios que permiten una AWS Backup administración completa, consulta la

sección AWS Backup Administración completa de la Disponibilidad de características por recurso tabla.

Cuando un tipo de recurso no admite la AWS Backup administración completa, algunas de sus AWS Backup actividades, como los costos de almacenamiento de las copias de seguridad, hacen que la facturación se refleje en el AWS servicio correspondiente.

Errores en los trabajos de copia

Solo se le cobrará una vez que se haya creado un punto de recuperación en el almacén de destino. No se aplica ningún cargo cuando se produce un error en un trabajo de copia y no se crea ningún punto de recuperación.

Etiquetas de asignación de costos

Puede utilizar las etiquetas de asignación de costes para realizar un seguimiento y optimizar AWS Backup los costes de forma detallada, así como ver y filtrar esas etiquetas mediante ellas AWS Cost Explorer.

Para usar etiquetas de asignación de costos, consulte Automatizar las copias de seguridad y optimizar los costos de las copias de seguridad para Amazon EFS mediante AWS Backup y Uso de etiquetas de asignación de costos.

AWS Backup Precios de Audit Manager

AWS Backup Audit Manager cobra por el uso en función del número de evaluaciones de control. Una evaluación de control es la evaluación de un recurso con respecto a un control. Los cargos por la evaluación del control aparecen en su AWS Backup factura. Para ver los precios actuales de las evaluaciones de control, consulte Precios de AWS Backup.

Para utilizar los controles de AWS Backup Audit Manager, debe habilitar la AWS Config grabación para realizar un seguimiento de la actividad de backup. AWS Config cargos por cada elemento de configuración registrado y estos cargos aparecen en su AWS Config factura. Para ver los precios actuales de los elementos de configuración registrados, consulte Precios de AWS Config.

Precios de Amazon Aurora

Durante el periodo de retención configurado para las copias de seguridad continuas de Aurora (hasta 35 días), las instantáneas no incurren en cargos de almacenamiento. Las instantáneas que se retienen una vez transcurrido este intervalo se cobran como copias de seguridad completas.

AWS Backup blogs, vídeos, tutoriales y otros recursos

Para obtener más información al respecto AWS Backup, consulte lo siguiente:

- Backup y restaure máquinas virtuales VMware locales mediante AWS Backup. Por Olumuyiwa Koya y Ezekiel Oyerinde (junio de 2022).
- Se utiliza AWS Backup para proteger las bases de datos de Amazon Aurora. Por Chris Hendon, Brandon Rubadou y Thomas Liddle (mayo de 2022).
- Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups. Por Evan Peck y Sabith Venkitachalapathy (mayo de 2022).
- Automatice y mejore su postura de seguridad mediante AWS Backup y AWS PrivateLink. Por Bilal Alam (abril de 2022).
- Obtenga informes agregados diarios entre cuentas y regiones. AWS Backup Por Wali Akbari y Sabith Venkitachalapathy (febrero de 2022).
- Automatice la visibilidad de los resultados de las copias de seguridad mediante AWS Backup y. AWS Security Hub Por Kanishk Mahajan (enero de 2022).
- Las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS. Por Ibukun Oyewumi (enero de 2022).
- Optimización de SAS Grid AWS con FSx for Lustre (y optimización de la recuperación ante desastres AWS Backup mediante). Por Matt Saeger y Shea Lutton (enero de 2022).
- Centralización de la protección de datos y el cumplimiento en Amazon Neptune AWS Backup con. Por Brian O'Keefe (noviembre de 2021).
- Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup. Por Karthik Vijayraghavan (noviembre de 2021).
- Simplifique la auditoría de sus políticas de protección de datos con AWS Backup Audit Manager. Por Jordan Bjorkman y Harshitha Putta (noviembre de 2021).
- Mejore la seguridad de sus copias de seguridad con AWS Backup Vault Lock. Por Rolland Miller (octubre de 2021).
- Cómo conservar las etiquetas de recursos en los trabajos de AWS Backup restauración. Por Ibukun Oyewumi, Amee Shah y Sabith Venkitachalapathy (septiembre de 2021).
- Gestione el acceso a las copias de seguridad mediante políticas de control de servicios con AWS Backup. Por Sabith Venkitachalapathy y Ibukun Oyewumi (agosto de 2021).
- Automatice el respaldo centralizado a escala en todos AWS los servicios utilizando AWS Backup. Por Ibukun Oyewumi y Sabith Venkitachalapathy (julio de 2021).

- Blog: Cómo simplificar las copias de seguridad de Microsoft SQL Server mediante AWS Backup VSS. Por Siavash Irani y Sepehr Samiei (julio de 2021).
- Automatice la validación de la recuperación de datos con AWS Backup. Por Mahanth Jayadeva (junio de 2021).
- Configurar las notificaciones para supervisar los AWS Backup trabajos. Por Virgil Ennes (junio de 2021).
- Automating backups and optimizing backup costs for Amazon EFS using AWS Backup. Por Prachi Gupta y Rohit Verma (junio de 2021).
- Administre los costos de respaldo de Amazon EFS: AWS Backup soporte para etiquetas de asignación de costos. Por Aditya Maruvada (mayo de 2021).
- Cree y comparta copias de seguridad cifradas entre cuentas y regiones utilizando AWS Backup. Por Prachi Gupta (mayo de 2021).
- AWS Backup ahora cuenta con la aprobación de FedRAMP High para sus necesidades de cumplimiento y protección de datos. Por Andy Grimes (mayo de 2021).
- ZS Associates mejora la eficiencia del respaldo con. AWS Backup Por Mitesh Naik, Hiranand Mulchandani y Sushant Jadhav (mayo de 2021).
- Tutorial: Uso AWS Backup de Amazon EBS Backup and Restore. Por Fathima Kamal (abril de 2021).
- Tutorial de vídeo: Managing Cross-Region Copies of Backups. Con David DeLuca (abril de 2021).
- Elimine varios puntos AWS Backup de recuperación con AWS Herramientas para PowerShell. Por Sherif Talaat (abril de 2021).
- Se utilizan copias de seguridad entre regiones y cuentas para Amazon FSx. AWS Backup Por Adam Hunter y Fathima Kamal (abril de 2021).
- Amazon CloudWatch Events and Metrics para AWS Backup. Por Rolland Miller (marzo de 2021).
- Tutorial: Backup y restauración de Amazon Relational Database Service (RDS) mediante. AWS Backup Por Fathima Kamal (marzo de 2021).
- oint-in-time Recuperación de P y copia de seguridad continua para Amazon RDS con AWS Backup. Por Kelly Griffin (marzo de 2021).
- Automatice AWS Backup con AWS Service Catalog con John Husemoller (enero de 2021).
- Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup. Por Cher Simon (enero de 2021).
- AWS Resumen de re:Invent: Protección de datos y cumplimiento. AWS Backup Por Nancy Wang (diciembre de 2020).

- AWS Backup proporciona una protección de datos centralizada en todos sus recursos. AWS Por Nancy Wang (noviembre de 2020).
- Tech Talk: Data protection at scale with AWS Backup. Por Kareem Behairy (septiembre de 2020).
- Administración centralizada de varias cuentas con el uso de copias entre regiones. AWS Backup Por Cher Simon (septiembre de 2020).
- Tutorial en vídeo: Gestiona copias de seguridad a gran escala mientras lo usas. AWS OrganizationsAWS Backup Por Ildar Sharafeev (julio de 2020).
- Gestione las copias de seguridad a escala según su AWS Organizations uso AWS Backup. Por Nancy Wang, Avi Drabkin, Ganesh Sundaresan y Vikas Shah (junio de 2020).
- Recupere archivos y carpetas de Amazon EFS con AWS Backup. Por Abrar Hussain y Gurudath Pai (mayo de 2020).
- Scheduling automated backups using Amazon EFS and AWS Backup. Por Rob Barnes (diciembre de 2019).
- re:Invent Recording: AWS re:Invent 2019: Profundiza en ft. AWS Backup Rackspace. Por Nancy Wang y Jason Pavao (diciembre de 2019).
- Proteja sus datos con AWS Backup. Por Anthony Fiore (julio de 2019).
- Vídeo de marketing: Introducing AWS Backup. Enero de 2019.
- Vídeo: Introduction to AWS Backup. Con AWS formación y certificación.

Configuración AWS por primera vez

Antes de usarlo AWS Backup por primera vez, complete las siguientes tareas:

1. Inscríbase en AWS
2. Creación un usuario de IAM
3. Creación de un rol de IAM

Inscríbase en AWS

Cuando te registras en Amazon Web Services (AWS), Cuenta de AWS se suscribe automáticamente a todos los servicios de AWS, incluidos AWS Backup. Solo se le cobrará por los servicios que utilice.

Para obtener más información sobre las tarifas de AWS Backup uso, consulta la página AWS Backup de precios.

Si Cuenta de AWS ya tienes una, pasa a la siguiente tarea. Si no dispone de una cuenta de AWS , utilice el siguiente procedimiento para crear una.

Para crear un Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Anota tu Cuenta de AWS número, ya que lo necesitarás para la siguiente tarea.

Creación un usuario de IAM

Los servicios de AWS, por ejemplo AWS Backup, requieren que proporciones credenciales al acceder a ellos, de modo que el servicio pueda determinar si tienes permisos para acceder a sus recursos. AWS recomienda no utilizar el usuario Cuenta de AWS raíz para realizar solicitudes. En su lugar, cree un usuario de IAM y concédale derechos de acceso completos. Estos usuarios se denominan usuarios administradores. Puede usar las credenciales del usuario administrador, en lugar de las credenciales del usuario Cuenta de AWS raíz, para interactuar AWS y realizar tareas, como crear un bucket, crear usuarios y concederles permisos. Para obtener más información, consulte Credenciales de usuario raíz de Cuenta de AWS y credenciales de usuario de IAM en la Referencia general de AWS y las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Si te has registrado AWS pero no has creado un usuario de IAM para ti, puedes crear uno mediante la consola de IAM.

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	Usar credenciales a corto plazo para acceder a AWS. Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas,	Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center .	Configure el acceso mediante programación configurando el AWS CLI que se utilizará AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
	consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.		
En IAM (no recomendado)	Usar credenciales a largo plazo para acceder a AWS.	Siga las instrucciones en Creación del primer grupo de usuarios y usuario de administrador de IAM en la Guía del usuario de IAM.	Configurar el acceso programático mediante Administración de las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Para iniciar sesión como este nuevo usuario de IAM, cierre sesión en. AWS Management Console A continuación, utilice la siguiente URL, donde your_aws_account_id es su Cuenta de AWS número sin guiones (por ejemplo, si su número es, su ID es): Cuenta de AWS `1234-5678-9012` Cuenta de AWS `123456789012`

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

Escriba el nombre y la contraseña del usuario de IAM que acaba de crear. Cuando haya iniciado sesión, en la barra de navegación se mostrará su_nombre_de_usuario@su_id_de_cuenta_de_aws.

Si no quieres que la URL de tu página de inicio de sesión contenga tu ID, puedes crear un alias de cuenta. Cuenta de AWS En el panel de IAM, haga clic en Crear alias de cuenta y especifique un alias, como el nombre de su empresa. Para iniciar sesión después de crear un alias de cuenta, use la siguiente dirección URL:

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

Para verificar el enlace de inicio de sesión de los usuarios de IAM de su cuenta, abra la consola de IAM y verifique el campo Alias de Cuenta de AWS en el panel.

Creación de un rol de IAM

Puedes usar la consola de IAM para crear un rol de IAM que otorgue AWS Backup permisos para acceder a los recursos compatibles. Después de crear el rol de IAM, podrá crear y asociar políticas al rol.

Para crear un rol de IAM con la consola

1. Inicie sesión en la consola de AWS administración y abra la consola de IAM.
2. En la consola de IAM, elija Roles en el panel de navegación y elija Crear rol.
3. Elija Rol de servicio de AWS y, a continuación, elija Seleccionar para AWS Backup. Elija Siguiente: permisos.
4. En la página Asociar políticas de permisos, active tanto `AWSBackupServiceRolePolicyForBackup` como `AWSBackupServiceRolePolicyForRestores`. Estas políticas AWS administradas otorgan AWS Backup permiso para realizar copias de seguridad y restaurar todos los AWS recursos compatibles. Para obtener más información sobre las políticas administradas y ver ejemplos, consulte Políticas administradas.

   A continuación, elija Next: Tags (Siguiente: Etiquetas).
5. Elija Siguiente: Revisar.
6. Para Role Name (Nombre de rol), escriba un nombre que describa el objetivo de este rol. Los nombres de los roles deben ser únicos en su nombre Cuenta de AWS. Dado que varias entidades pueden hacer referencia al rol, no puede editar el nombre del rol después de crearlo.

   Seleccione Crear rol.
7. En la página Roles, elija el rol que ha creado para abrir su página de detalles.

Empezar con AWS Backup

En este tutorial, se muestran los pasos genéricos para utilizar las funciones y AWS Backup características. Al igual que con cualquier parte de esta documentación técnica, debe seguir las instrucciones de la consola AWS de administración que aparece en la otra ventana.

También puede aprender a usarlo AWS Backup con un servicio específico leyendo estos tutoriales:

- Backup y restauración de Amazon Relational Database Service (Amazon RDS) mediante AWS Backup
- Tutorial: Backup y restauración de Amazon EBS mediante AWS Backup

Temas

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Un Cuenta de AWS. Para obtener más información, consulte Configuración AWS por primera vez.
- Al menos un recurso respaldado por AWS Backup.
- Debe estar familiarizado con los AWS servicios y recursos de los que va a hacer copias de seguridad. Consulte la lista de Recursos de AWS y aplicaciones de terceros compatibles.

  Cuando haya nuevos AWS servicios disponibles, habilite AWS Backup el uso de esos servicios.

Para configurar los AWS servicios que se van a utilizar con AWS Backup

1. Inicie sesión en AWS Management Console y abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, seleccione Configuración.
3. En la página Activación del servicio, elija Configurar recursos.
4. En la página Configurar recursos, utilice los conmutadores para activar o desactivar los servicios con AWS Backup los que se utilizan. Cuando los servicios estén configurados, elija Confirmar. Asegúrese de que el AWS servicio por el que está optando esté disponible en su. Región de AWS

Consulte Asignación de recursos a un plan de copia de seguridad para obtener información adicional. La AWS Backup consola permite al usuario asignar un tipo de recurso a un plan de respaldo; esto se incluirá incluso si la opción no está habilitada para ese servicio en particular.

- Asegúrese de que los recursos de los que va a hacer copias de seguridad estén todos en la misma Región de AWS.

Para completar este tutorial, puede usar su usuario Cuenta de AWS root para iniciar sesión en. AWS Management Console Sin embargo, AWS Identity and Access Management (IAM) recomienda no utilizar el usuario Cuenta de AWS root. En su lugar, cree un administrador en su cuenta y utilice esas credenciales para administrar los recursos de su cuenta. Para obtener más información, consulte Configuración AWS por primera vez.

La AWS Backup consola ofrece diferentes opciones para hacer copias de seguridad de los recursos. Puede crear una copia de seguridad bajo demanda, programar y configurar la forma en que desea que se realice la copia de seguridad del recurso o configurar los recursos para que se realicen copias de seguridad automáticamente cuando se cree el recurso.

Primeros pasos 1: suscripción al servicio

La AWS Backup consola tiene dos formas de incluir los tipos de recursos en un plan de respaldo: asignar explícitamente el tipo de recurso en un plan de respaldo o incluir todos los recursos. Consulte los puntos siguientes para entender cómo funcionan estas selecciones con las suscripciones a servicios.

- Si las asignaciones de recursos se basan únicamente en etiquetas, se aplica la configuración de suscripción al servicio.
- Si un tipo de recurso se asigna explícitamente a un plan de respaldo, se incluirá en el respaldo incluso si la opción no está habilitada para ese servicio en particular. Esto no se aplica a Aurora, Neptune ni Amazon DocumentDB. Para incluir estos servicios, la suscripción debe estar habilitada.
- Si se especifican tanto el tipo de recurso como las etiquetas en una asignación de recursos, los tipos de recursos especificados se filtran primero y, a continuación, las etiquetas filtran aún más esos recursos.

  La configuración de suscripción del servicio se ignora en la mayoría de los tipos de recursos. Sin embargo, Aurora, Neptune y Amazon DocumentDB requieren la suscripción del servicio.
- En el caso de Amazon FSx para NetApp ONTAP, cuando utilice la selección de recursos basada en etiquetas, aplique etiquetas a volúmenes individuales en lugar de a todo el sistema de archivos.

Las opciones de suscripción se aplican a la cuenta específica y. Región de AWS Cuando una cuenta utiliza AWS Backup (crea una bóveda de respaldo o un plan de respaldo) en una región, la cuenta se incluye automáticamente en todos los tipos de recursos admitidos por la región AWS Backup en ese momento. Los servicios compatibles que se agreguen a esa región en una fecha posterior no se incluirán automáticamente en un plan de respaldo. Puede optar por utilizar esos tipos de recursos una vez que se admitan.

Dado que cada vez AWS Backup es compatible con más AWS servicios y aplicaciones de terceros, es posible que tengas que revisar este paso para optar por esos recursos recientemente compatibles.

AWS Backup no regula ni administra las copias de seguridad realizadas en AWS entornos distintos de. AWS Backup

Optar por utilizarlos AWS Backup para proteger todos los tipos de recursos compatibles

1. Inicie sesión y abra la AWS Backup consola en https://console.aws.amazon.com/backup. AWS Management Console
2. En el panel de navegación izquierdo, elija Configuración.
3. En Activación del servicio, elija Configurar recursos.
4. Para acceder a todos los recursos AWS Backup compatibles, mueve todos los botones hacia la derecha.
5. Elija Confirmar.

Siguientes pasos

Para crear una copia de seguridad bajo demanda utilizando AWS Backup, proceda a. Primeros pasos 2: creación de una copia de seguridad bajo demanda

Primeros pasos 2: creación de una copia de seguridad bajo demanda

En la AWS Backup consola, la página de recursos protegidos muestra los recursos de los que se ha hecho una copia de seguridad al AWS Backup menos una vez. Si lo utiliza AWS Backup por primera vez, en esta página no aparece ningún recurso, como volúmenes de Amazon EBS o bases de datos de Amazon RDS. Esto es así incluso si dicho recurso se asignó a un plan de copias de seguridad y dicho plan no ha ejecutado ningún trabajo de copias de seguridad programadas al menos una vez.

En este paso, va a crear una copia de seguridad bajo demanda de uno de los recursos. A continuación, consulte este recurso que se indica en la página Protected resources (Recursos protegidos).

Para crear una copia de seguridad bajo demanda

1. Inicie sesión en y abra la AWS Management ConsoleAWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y Crear copia de seguridad bajo demanda.
3. En la página Crear copia de seguridad bajo demanda, elija el tipo de recurso del que desea realizar una copia de seguridad; por ejemplo, elija DynamoDB para tablas de Amazon DynamoDB.
4. Elija el nombre o ID del recurso que desea proteger. Asegúrese de que el recurso que elija es el que desea.

   > **Note**
   >
   > Para Amazon FSx para Lustre, se admiten los tipos de implementación Persistent y Persistent_2.

5. Asegúrese de que la opción Create backup now (Crear copia de seguridad ahora) esté seleccionada. De esta manera, se inicia una copia de seguridad de inmediato y le permite ver antes los recursos guardados en la página Protected resources (Recursos protegidos).

6. Especifique una transición a un valor de almacenamiento en frío (si procede) y un valor de caducidad.

> **Note**
>
> - Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla Disponibilidad de características por recurso. Todos los demás tipos de recursos se guardan en almacenamiento en caliente y hacen caso omiso de la expresión de transferencia al almacenamiento en frío. El valor Vencimiento es válido para todos los tipos de recursos.
> - Cuando las copias de seguridad caduquen y estén marcadas para su eliminación como parte de su política de ciclo de vida, las AWS Backup eliminará en un momento elegido al azar durante las 8 horas siguientes. Este intervalo ayuda a garantizar un rendimiento uniforme.

7. Elija un almacén de copias de seguridad existente. Al elegir Create new backup vault (Crear nuevo almacén de copias de seguridad) se abre una nueva página para crear un almacén y a continuación, vuelve a la página Create on-demand backup (Crear copia de seguridad bajo demanda) cuando termine.
8. En IAM role (Rol de IAM), elija Default role (Rol predeterminado).

> **Note**
>
> Si el rol AWS Backup predeterminado no está presente en tu cuenta, se crea un rol para ti con los permisos correctos.

9. Si desea asignar una o varias etiquetas a su copia de seguridad bajo demanda, introduzca una key (clave) y un value (valor) opcional y elija Add tag (Añadir etiqueta).

> **Note**
>
> - En el caso de los recursos de Amazon EC2, copia AWS Backup automáticamente las etiquetas de recursos individuales y grupales existentes, además de las etiquetas que añada a esta copia de seguridad. Para obtener más información, consulte Copia de etiquetas en copias de seguridad.

- Al crear un plan de respaldo basado en etiquetas, si elige un rol que no sea el predeterminado, asegúrese de que tenga los permisos necesarios para realizar copias de seguridad de todos los recursos etiquetados. AWS Backup intenta procesar todos los recursos con las etiquetas seleccionadas. Si se encuentra un recurso para el que no tiene permiso de acceso, se producirá un error en el plan de copia de seguridad.

10. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). Esto le lleva a la página Jobs (Trabajos), donde verá una lista de trabajos.
11. Si el tipo de recurso es EC2, aparecerá la sección Configuración avanzada de copia de seguridad. Elija Windows VSS si la instancia EC2 ejecuta Microsoft Windows. Esto le permite realizar copias de seguridad de Windows VSS coherentes con la aplicación.

> **Note**
>
> AWS Backup actualmente solo admite copias de seguridad coherentes con las aplicaciones de los recursos que se ejecutan en Amazon EC2. No todos los tipos de instancia o aplicaciones son compatibles con las copias de seguridad de Windows VSS. Para obtener más información, consulte Creación de copias de seguridad de Windows VSS.

12. Elija el ID de trabajo de copia de seguridad que corresponda al recurso del que desea realizar la copia de seguridad para ver los detalles de ese trabajo.

Siguientes pasos

Para automatizar la actividad de copia de seguridad, vaya a Primeros pasos 3: creación de una copia de seguridad programada.

Primeros pasos 3: creación de una copia de seguridad programada

En este paso del AWS Backup tutorial, creará un plan de respaldo, le asignará recursos y, a continuación, creará un almacén de respaldo.

Antes de comenzar, asegúrese de que se cumplen los requisitos previos necesarios. Para obtener más información, consulte Empezar con AWS Backup.

Temas

Paso 1: cree un plan de copia de seguridad basado en uno existente

Un plan de copia de seguridad es una expresión de la política que define cuándo y cómo desea realizar la copia de seguridad de sus recursos de AWS , como tablas de Amazon DynamoDB o sistemas de archivos de Amazon Elastic File System (Amazon EFS). Los recursos se asignan a los planes de copia de seguridad y, a AWS Backup continuación, se realizan copias de seguridad y se conservan automáticamente las copias de seguridad de esos recursos de acuerdo con el plan de copia de seguridad. Para obtener más información, consulte Administración de copias de seguridad mediante planes de copia de seguridad.

Hay dos formas de crear un nuevo plan de copia de seguridad: puede crearlo desde cero o crear uno basado en un plan de copia de seguridad existente. En este ejemplo, se usa la AWS Backup consola para crear un plan de respaldo mediante la modificación de un plan de respaldo existente.

Para crear un plan de copia de seguridad a partir de uno existente

1. Inicie sesión en AWS Management Console y abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de control, elija Administrar planes de Backup. O, en el panel de navegación, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. Elija Empezar con plantilla, elija un plan de la lista (por ejemplo, `Daily-Monthly-1yr-Retention`) y escriba un nombre en el cuadro Nombre del plan de copia de seguridad.

   > **Note**
   >
   > Si intenta crear un plan de copia de seguridad idéntico a uno existente, aparecerá un error `AlreadyExistsException`.

4. En la página de resumen del plan, elija la regla de copia de seguridad que desee y, a continuación, elija Editar.
5. Revise y seleccione los valores que desee para la regla (consulte las opciones de reglas en Opciones y configuración del plan de copia de seguridad).

6. Para el almacén de copias de seguridad, elija Predeterminado o elija Crear nuevo almacén de copia de seguridad para crear un nuevo almacén.
7. (Opcional): selecciona una opción Región de AWS de la lista de la región de destino para copiar la copia de seguridad en otra región. Para agregar más regiones, elija Agregar copia.
8. Cuando haya terminado de editar la regla, elija Guardar regla de copia de seguridad.

En la página Resumen, elija Asignar recursos para prepararse para la siguiente sección.

Paso 2: asigne recursos a un plan de copia de seguridad

Después de crear un plan de respaldo, debe asignar sus AWS recursos a ese plan de respaldo. Para obtener más información acerca de la asignación de recursos, consulte Asignación de recursos a un plan de copia de seguridad.

Si aún no tiene AWS recursos existentes que desee asignar a un plan de respaldo, cree algunos recursos nuevos para usarlos en este ejercicio. Cree uno o dos recursos con Recursos de AWS y aplicaciones de terceros compatibles.

Para asignar recursos a un plan de copias de seguridad

1. Los pasos anteriores deberían haberle llevado a la página Asignar recursos.
2. Escriba un Nombre de asignación de recursos.
3. Para el rol de IAM, elija Rol predeterminado. Si elige otro rol, este debe tener permisos para hacer copias de seguridad de todos los recursos que asigne.
4. En la sección Asignar recursos, elija Incluir todos los tipos de recursos. Un tipo de recurso es un AWS servicio AWS Backup compatible o una aplicación de terceros. Este plan de respaldo ahora protegerá todos los tipos de recursos que haya elegido proteger mediante AWS Backup
5. Elija Asignar recursos.

Volverá a la página Resumen del plan de copia de seguridad. Elija Crear plan de copia de seguridad para implementar su primer plan de copia de seguridad.

Paso 3: cree un almacén de copias de seguridad

En lugar de utilizar el almacén de copias de seguridad predeterminado que se crea automáticamente en la consola de AWS Backup , puede crear almacenes de copia de seguridad específicos para guardar y organizar grupos de copias de seguridad en el mismo almacén.

Para obtener más información acerca de los almacenes de copia de seguridad, consulte Almacenes de copias de seguridad.

Para crear un almacén de copias de seguridad

1. En la AWS Backup consola, en el panel de navegación, seleccione Backup Vaults.

   > **Note**
   >
   > Si el panel de navegación no está visible en el lado izquierdo, puede abrirlo seleccionando el icono de menú situado en la esquina superior izquierda de la consola. AWS Backup

2. Seleccione Create backup vault (Crear almacén de copias de seguridad).
3. Escriba un nombre para su almacén de copias de seguridad. Puede asignar un nombre a su almacén para reflejar lo que almacenará en él o para facilitar la búsqueda de las copias de seguridad que necesite. Por ejemplo, podría denominarlo **`FinancialBackups`**.
4. Seleccione una tecla AWS Key Management Service (AWS KMS). Puede usar una clave que ya haya creado o seleccionar la clave AWS Backup KMS predeterminada.

   > **Note**
   >
   > La AWS KMS clave que se especifica aquí solo se aplica a las copias de seguridad de los servicios que admiten el cifrado AWS Backup independiente. Para ver la lista de tipos de recursos que admiten el cifrado AWS Backup independiente, consulte la sección « AWS Backup Administración total» de la Disponibilidad de características por recurso tabla.

5. Opcionalmente, añada etiquetas que le ayudarán a buscar e identificar el almacén de copias de seguridad. Por ejemplo, podría añadir una etiqueta **`BackupType:Financial`**.
6. Seleccione Create Backup vault (Crear almacén de copias de seguridad).
7. En el panel de navegación, elija Backup vaults (Almacenes de copias de seguridad) y verifique que se ha añadido el almacén de copias de seguridad.

> **Note**
>
> Ahora puede editar una regla de uno de los planes para que las copias de seguridad creadas por esa regla se guarden en el almacén que acaba de crear.

Siguientes pasos

Para realizar copias de seguridad de los sistemas de archivos de Amazon EFS específicamente, vaya a Primeros pasos 4: creación de copias de seguridad automáticas de Amazon EFS.

Primeros pasos 4: creación de copias de seguridad automáticas de Amazon EFS

Al crear un sistema de archivos de Amazon Elastic File System (Amazon EFS) mediante la consola de Amazon EFS, las copias de seguridad automáticas se activan de forma predeterminada. Si desea realizar automáticamente una copia de seguridad de un sistema de archivos de Amazon EFS existente, puede hacerlo mediante la consola, la API o la CLI de Amazon EFS.

Para realizar automáticamente una copia de seguridad de un sistema de archivos de Amazon EFS existente mediante la consola

1. Abra la consola de Amazon EFS en https://console.aws.amazon.com/efs.
2. En la página Sistemas de archivos, elija un sistema de archivos para activar las copias de seguridad automáticas.
3. Elija Editar en el panel de configuración General.
4. Para activar las copias de seguridad automáticas, elija Permitir copias de seguridad automáticas.

La configuración predeterminada del plan de copia de seguridad es `daily backups, 35-day retention`. El intervalo de copia de seguridad predeterminado (el plazo de tiempo en el que se ejecutará la copia de seguridad) está establecido para que comience a las 5 h UTC (horario universal coordinado) y dure 8 horas.

> **Note**
>
> El almacén de copias de seguridad automáticas de Amazon EFS `aws/efs/automatic-backup-vault` está reservado únicamente para esas copias de seguridad automáticas.

> Esta bóveda no debe utilizarse para crear copias entre cuentas ni como destino de copias de seguridad creadas mediante otros planes de copias de seguridad no automatizadas. Si lo usa como destino para otros planes de copia de seguridad, recibirá un mensaje de error indicando que no tiene suficientes privilegios.

AWS Backup crea un rol vinculado al servicio en tu cuenta en tu nombre. Este rol cuenta con los permisos necesarios para realizar copias de seguridad de Amazon EFS. Para obtener más información sobre los roles vinculados a servicios, consulte Uso de roles vinculados a servicios de AWS Backup.

Para step-by-step obtener instrucciones sobre cómo activar o desactivar las copias de seguridad automáticas mediante la consola, la API o la CLI de Amazon EFS, consulte las copias de seguridad automáticas en la Guía del usuario de Amazon Elastic File System.

Siguientes pasos

Para ver las copias de seguridad que ha creado, vaya a Primeros pasos 5: visualización de los trabajos de copia de seguridad y los puntos de recuperación.

Primeros pasos 5: visualización de los trabajos de copia de seguridad y los puntos de recuperación

Con AWS Backup ella, puede ver el estado y otros detalles de la actividad de copia de seguridad y restauración en todos los AWS servicios que utiliza.

En el AWS Backup panel de control, puede gestionar los planes de copia de seguridad, crear copias de seguridad a pedido, restaurarlas y ver el estado de las tareas de copia de seguridad y restauración.

Temas

Visualización del estado de los trabajos de copia de seguridad

Utilice el AWS Backup panel de control para ver rápidamente el estado de su actividad de copia de seguridad y restauración.

Para ver el estado del trabajo de copia de seguridad

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Panel.
3. Para ver el estado de los trabajos de copia de seguridad, seleccione Backup jobs details (Detalles de trabajos de copia de seguridad). Esto le llevará a la página Trabajos de copia de seguridad, donde encontrará tablas con trabajos de copia de seguridad y trabajos de restauración.
4. Puede filtrar los trabajos que aparecen por periodo de tiempo. Por ejemplo, puede filtrar los trabajos creados en las últimas 24 horas, la última semana o los últimos 30 días. También puede definir el número de trabajos que mostrar por página seleccionando el icono de engranaje.

Visualización de todas las copias de seguridad en un almacén

Siga estos pasos para ver las copias de seguridad que se han creado en un almacén especificado en AWS Backup.

Para ver todas las copias de seguridad de un almacén

1. En la AWS Backup consola, en el panel de navegación, seleccione Backup Vaults.
2. Elija el almacén que utilizó al crear una copia de seguridad bajo demanda o programada y vea todas las copias de seguridad que se crearon en este almacén.

> **Note**
>
> Cada copia de seguridad tiene un Estado, que normalmente es Completado. Si por alguna razón no AWS Backup se puede eliminar una copia de seguridad según su configuración de ciclo de vida, la marca como caducada. Se le facturará por el almacenamiento que consuman las copias de seguridad Vencidas y deberá eliminarlas.

Visualización de detalles de recursos protegidos

En la página Protected resources (Recursos protegidos), puede explorar detalles de los recursos de los que se hace una copia de seguridad en AWS Backup.

Para ver los recursos protegidos

1. En la AWS Backup consola, en el panel de navegación, selecciona Recursos protegidos.
2. Vea los AWS recursos de los que se está haciendo una copia de seguridad. Elija un recurso en la lista para explorar las copias de seguridad de dicho recurso.

Siguientes pasos

Para restaurar un punto de recuperación que ha visto, vaya a Primeros pasos 6: restauración de una copia de seguridad.

Primeros pasos 6: restauración de una copia de seguridad

Una vez que se ha hecho una copia de seguridad de un recurso al menos una vez, se considera protegido y se puede restaurar mediante él AWS Backup. Siga estos pasos para restaurar un recurso utilizando la consola de AWS Backup .

Para obtener información sobre los parámetros de restauración de servicios específicos o sobre la restauración de una copia de seguridad mediante la API AWS CLI o la AWS Backup API, consulte Restauración de una copia de seguridad.

Para restaurar un recurso

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso que desee restaurar.
3. Aparecerá una lista con los puntos de recuperación, incluido el tipo de recurso, por ID de recurso. Elija un recurso para abrir la página Detalles del recurso.
4. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
5. Especifique los parámetros de restauración. Los parámetros de restauración que aparecen son específicos del tipo de recurso seleccionado.

> **Note**
>
> Si solo mantiene una copia de seguridad, únicamente podrá restaurar el estado del sistema de archivos al momento en que realizó la copia de seguridad. No podrá restaurar copias de seguridad incrementales anteriores.

Para obtener instrucciones sobre cómo restaurar recursos específicos, consulte Restauración de una copia de seguridad.

6. En Rol de restauración, elija Rol predeterminado.

> **Note**
>
> Si el rol AWS Backup predeterminado no está presente en su cuenta, se creará un rol para usted con los permisos correctos.

7. Seleccione Restaurar copia de seguridad.

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

> **Note**
>
> Cuando restaure elementos específicos incluidos en una instancia de Amazon EFS, puede restaurar esos elementos en un sistema de archivos nuevo o en uno existente. Si restaura los elementos en un sistema de archivos existente, AWS Backup crea un nuevo directorio Amazon EFS a partir del directorio raíz para contener los elementos. La jerarquía completa de los elementos especificados se conserva en el directorio de recuperación. Por ejemplo, si el directorio A contiene los subdirectorios B, C y D, AWS Backup conserva la estructura jerárquica cuando se recuperan A, B, C y D.
> Independientemente de si realiza una restauración parcial de Amazon EFS en un sistema de archivos existente o en otro nuevo, con cada intento de restauración se creará un nuevo directorio de recuperación fuera del directorio raíz para incluir los archivos restaurados.
> Si intenta realizar varias restauraciones de la misma ruta, es posible que existan varios directorios que contengan los elementos restaurados.

Para restaurar una instancia de Amazon EFS

Si va a restaurar una instancia de Amazon EFS, puede realizar una Restauración completa, lo que restaura todo el sistema de archivos. O bien, puede restaurar archivos y directorios específicos mediante la Restauración a nivel de elemento (las restauraciones a nivel de elemento tienen límites). Consulte Restoring an EFS file system para obtener más información). Para obtener información sobre la restauración de otros tipos de recursos, consulte Restauración de una copia de seguridad.

> **Note**
>
> Para restaurar una instancia de Amazon EFS, debe “Permitir” `backup:startrestorejob`.

Para obtener información detallada sobre la restauración de una copia de seguridad, consulte Restauración de una copia de seguridad.

Siguientes pasos

Con AWS Backup Audit Manager, puede auditar su actividad y sus recursos de backup. También puede crear informes que puede utilizar como prueba de sus trabajos de copia de seguridad, restauración y copia. Para crear un informe, consulte Primeros pasos 7: creación de un informe de auditoría.

Primeros pasos 7: creación de un informe de auditoría

EnPrimeros pasos 5: visualización de los trabajos de copia de seguridad y los puntos de recuperación, observó su actividad de respaldo en las vistas AWS Backup Dashboard, Backup Vault y Protected Resources. Sin embargo, estas vistas son dinámicas y se actualizarán en función de cuándo las visite. Estas opiniones no son necesariamente la mejor prueba de la conformidad continua con los requisitos y controles de protección de datos de su organización a lo largo del tiempo.

En este paso, creará un informe de trabajo de respaldo bajo demanda mediante AWS Backup Audit Manager.

AWS Backup Audit Manager entrega una variedad de informes de auditoría en CSV, JSON o ambos formatos a diario y bajo demanda a su bucket de Amazon S3. Puede auditar la conformidad de su actividad y recursos de copia de seguridad con respecto a una serie de controles personalizables.

Puede recibir informes sobre sus trabajos de copia de seguridad, copia y restauración. El informe del trabajo de copia de seguridad es una prueba de que sus trabajos de copia de seguridad se llevaron a cabo.

A continuación se muestra un ejemplo de un plan de copia de seguridad.


```
{
  "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"
    }
  ]
}
```


Para crear un informe de copia de seguridad (incluido un informe de copia de seguridad bajo demanda), primero debe crear un plan de informes para automatizar los informes y enviarlos a un bucket de Amazon S3.

Un plan de informes requiere tener un bucket de Amazon S3 que reciba los informes. Para obtener instrucciones sobre cómo configurar un nuevo bucket de S3, consulte el Paso 1: Crear su primer bucket de S3 en la Guía del usuario de Amazon Simple Storage Service.

Para crear un plan de informes

1. Inicie sesión y abra la AWS Backup consola en https://console.aws.amazon.com/backup. AWS Management Console
2. En el panel de navegación izquierdo, elija Informes.
3. Elija Crear plan de informe.
4. Seleccione Informe de trabajo de copia de seguridad en la lista desplegable.
5. En Nombre del plan de informe, escriba **`TestBackupJobReport`**.
6. En Formato del archivo, elija CSV y JSON.
7. En el Nombre del bucket de S3, seleccione el destino de sus informes en la lista desplegable.
8. Elija Crear plan de informe.

A continuación, debe permitir que su bucket de S3 reciba informes AWS Backup. AWS Backup Audit Manager genera automáticamente una política de acceso a S3 para usted.

Para ver y aplicar esta política de acceso

1. En el panel de navegación izquierdo, elija Informes.
2. En Nombre del plan de informe, elija el nombre de su plan de informes (`TestBackupJobReport`).
3. Elija Editar.
4. Elija Ver política de acceso para el bucket de S3.
5. Elija Copiar permisos.
6. Elija Editar política del bucket para editar la política del bucket de S3 de destino para que reciba sus informes de trabajos de copias de seguridad.
7. Copie o agregue los permisos a la política del bucket de S3 de destino.

A continuación, cree su primer informe de trabajos de copias de seguridad.

Para crear informes de copias de seguridad bajo demanda

1. En el panel de navegación izquierdo, elija Informes.
2. En Nombre del plan de informe, elija el nombre de su plan de informes (`TestBackupJobReport`).

3. Elija Crear informe en diferido.

Por último, consulte el informe.

Para ver los informes

1. En el panel de navegación izquierdo, elija Informes.
2. En Nombre del plan de informe, elija el nombre de su plan de informes (`TestBackupJobReport`).
3. En la sección Trabajos de informe, elija el enlace de S3. De este modo, llegará al bucket de S3 de destino.
4. Elija Descargar.
5. Abra el informe con el programa que utiliza para trabajar con archivos CSV o JSON.

Siguientes pasos

Para depurar los recursos utilizados en los primeros pasos y evitar cargos no deseados, vaya a Primeros pasos 8: depuración de recursos.

Primeros pasos 8: depuración de recursos

Después de llevar a cabo todas las tareas en Empezar con AWS Backup, es posible que desee limpiar lo que ha creado con el fin de evitar incurrir en cargos innecesarios.

Temas

- Paso 1: Eliminar los recursos restaurados AWS
- Paso 2: elimine el plan de copia de seguridad
- Paso 3: elimine los puntos de recuperación
- Paso 4: elimine el almacén de copias de seguridad
- Paso 5: elimine el plan de informes
- Paso 6: elimine los informes

Paso 1: Eliminar los recursos restaurados AWS

Para eliminar AWS los recursos que haya restaurado de un punto de recuperación, como los volúmenes de Amazon Elastic Block Store (Amazon EBS) o las tablas de Amazon DynamoDB, utilice la consola de ese servicio. Por ejemplo, para eliminar un sistema de archivos de Amazon Elastic File System (Amazon EFS), utilice la consola de Amazon EFS.

> **Note**
>
> Esta información se aplica a los recursos restaurados, no a los puntos de recuperación guardados en un almacén de copias de seguridad.

Paso 2: elimine el plan de copia de seguridad

Si no desea crear copias de seguridad programadas, debe eliminar los planes de copias de seguridad. Para poder eliminar un plan de copia de seguridad, debe eliminar todas las asignaciones de recursos a ese plan de copia de seguridad.

Siga estos pasos para eliminar un plan de copias de seguridad:

Para eliminar un plan de copia de seguridad

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, seleccione Backup plans (Planes de copias de seguridad).
3. En la página Backup plans (Planes de copias de seguridad), elija el plan de copias de seguridad que desea eliminar. Esto le lleva a la página de detalles de dicha copia de seguridad.
4. Para eliminar las asignaciones de recursos para el plan, elija el botón de radio situado junto al nombre de la asignación y, a continuación, elija Delete (Eliminar).
5. Para eliminar el plan de copias de seguridad, elija Delete (Eliminar) en la esquina superior derecha de la página.
6. En la página de confirmación, introduzca el nombre del plan y elija Delete plan (Eliminar plan).

Paso 3: elimine los puntos de recuperación

A continuación, puede eliminar los puntos de recuperación que se encuentran en el almacén de copia de seguridad.

Para eliminar los puntos de recuperación

1. En la AWS Backup consola, en el panel de navegación, seleccione Backup Vaults.
2. En la página Backup vaults (Almacenes de copias de seguridad), elija el almacén de copias de seguridad donde almacenó las copias de seguridad.
3. Compruebe el punto de recuperación y elija Eliminar.
4. Si va a eliminar más de un punto de recuperación, siga estos pasos:

    a. Si la lista contiene una copia de seguridad continua, elija si desea conservar o eliminar los datos de la copia de seguridad continua.

    b. Para eliminar todos los puntos de recuperación de la lista, escriba **`delete`** y, a continuación, elija Eliminar punto de recuperación.

    Mantenga la pestaña del navegador abierta hasta que vea el banner verde de confirmación en la parte superior de la página. Si cierra esta pestaña antes de tiempo, se dará por finalizado el proceso de eliminación y es posible que se pierdan algunos de los puntos de recuperación que quería eliminar. Para obtener más información, consulte Eliminación de copias de seguridad.

Paso 4: elimine el almacén de copias de seguridad

Por lo general, el almacén de copias de seguridad predeterminado no se puede eliminar. Sin embargo, si hay uno o más almacenes en una región, el almacén de copias de seguridad predeterminado de esa región se puede eliminar mediante la AWS CLI.

Puede eliminar otros almacenes no predeterminados una vez que se hayan eliminado todas las copias de seguridad (puntos de recuperación) que contengan. Para ello, seleccione Eliminar en el almacén vacío.

Paso 5: elimine el plan de informes

Su plan de informes envía automáticamente un nuevo informe todos los días. Para evitarlo, elimine el plan de informes.

Para eliminar el plan de informes

1. En la AWS Backup consola, en el panel de navegación, selecciona Informes.
2. En Nombre del plan de informe, elija el nombre del plan de informes.

3. Elija Eliminar.
4. Introduzca el nombre del plan de informes y elija Eliminar el plan de informe.

Paso 6: elimine los informes

Puede eliminar los informes según las instrucciones de Eliminación de un solo objeto de cada uno de los informes. Si ya no necesita su bucket de S3 de destino, tras eliminar todos los objetos del bucket, puede eliminarlo según las instrucciones en Eliminar un bucket.

Administración de copias de seguridad mediante planes de copia de seguridad

En AWS Backup, un plan de respaldo es una expresión de política que define cuándo y cómo desea realizar copias de seguridad de sus AWS recursos, como las tablas de Amazon DynamoDB o los sistemas de archivos Amazon Elastic File System (Amazon EFS). Puede asignar recursos a los planes de respaldo y realizar copias de seguridad y conservar AWS Backup automáticamente las copias de seguridad de esos recursos de acuerdo con el plan de respaldo. Puede crear varios planes de copia de seguridad si tiene cargas de trabajo con requisitos de copia de seguridad diferentes. De forma predeterminada, AWS Backup optimiza los intervalos de copia de seguridad. Puede personalizar el intervalo de copia de seguridad en la consola o mediante programación.

AWS Backup almacena de forma eficiente las copias de seguridad periódicas de forma incremental. La primera copia de seguridad de un recurso de AWS hace una copia de seguridad completa de sus datos. Para cada copia de seguridad incremental sucesiva, solo se respaldan los cambios en sus AWS recursos. Las copias de seguridad incrementales le permiten beneficiarse de la protección de datos que ofrecen las copias de seguridad frecuentes y, al mismo tiempo, minimizar los costos de almacenamiento.

AWS Backup también administra sin problemas el ciclo de vida de su plan de respaldo en función de su configuración de retención, lo que le permite realizar restauraciones cuando sea necesario.

En las siguientes secciones se proporcionan los aspectos básicos de la gestión de su estrategia de copia de seguridad AWS Backup.

Temas

Creación de un plan de copia de seguridad

Puede crear un plan de respaldo mediante la AWS Backup consola, la API, la CLI, el SDK o una AWS CloudFormation plantilla.

Temas

- Creación de planes de copia de seguridad mediante la consola de AWS Backup
- Creación de planes de respaldo mediante el AWS CLI
- Opciones y configuración del plan de copia de seguridad
- AWS CloudFormation plantillas para planes de respaldo

Creación de planes de copia de seguridad mediante la consola de AWS Backup

Abra la AWS Backup consola en https://console.aws.amazon.com/backup. En el panel de control, elija Administrar planes de Backup. O, en el panel de navegación, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.

Opciones de inicio

Tienes tres opciones para el nuevo plan de copia de seguridad:

- Paso 1: cree un plan de copia de seguridad basado en uno existente
- Crear un plan nuevo
- Creación de planes de respaldo mediante el AWS CLI

En este tutorial elegiremos Crear un plan nuevo. Cada parte de la configuración tiene un enlace a una sección ampliada situada más adelante en la página, a la que puede desplazarse para obtener más detalles.

1. Introduzca un nombre de plan en Nombre del plan de copia de seguridad. No puede cambiar el nombre de un plan una vez creado.

   Si intentas crear un plan alternativo que sea idéntico a un plan existente, recibirás un `AlreadyExistsException` error.
2. Si lo desea, puede agregar etiquetas a su plan de copia de seguridad.
3. Configuración de reglas de copia de seguridad: en la sección de configuración de reglas de copia de seguridad, establezca la programación, la ventana y el ciclo de vida de la copia de seguridad.
4. Programación:

a. Introduzca el nombre de una regla de copia de seguridad en el campo de texto.

b. En el menú desplegable del almacén de copia de seguridad, elija Predeterminado o elija Crear nuevo almacén de copia de seguridad para crear un nuevo almacén.

c. En el menú desplegable de frecuencia de copia de seguridad, elija la frecuencia con la que desea que este plan cree una copia de seguridad.

5. Intervalo de copia de seguridad:

a. La hora de inicio predeterminada son las 12:30 a. m. (00:30 en 24 horas) en la zona horaria local del sistema.

b. Comenzar en un plazo de se establece de manera predeterminada en 8 horas. Puede cambiarlo para especificar un intervalo de tiempo para que comience la copia de seguridad.

c. Completar en se establece de manera predeterminada en 7 días.

6. Copias de seguridad y point-in-time restauración continuas (PITR): Puede seleccionar Activar copias de seguridad continuas para point-in-time la recuperación (PITR). Para verificar qué recursos son compatibles con este tipo de copia de seguridad, consulte la matriz de Disponibilidad de características por recurso.

7. Ciclo de vida

a. Almacenamiento en frío: seleccione esta casilla para permitir que los tipos de recursos que cumplen los requisitos pasen al almacenamiento en frío de acuerdo con el calendario que especifique en el periodo de retención total. Para utilizar el almacenamiento en frío debe tener un periodo de retención total de 90 días o más.

b. El almacenamiento en frío para Amazon EBS es Archivo de instantáneas de Amazon EBS. Las instantáneas que pasen al nivel de almacenamiento de archivo se mostrarán en la consola como nivel frío. Si está habilitado el almacenamiento en frío y la frecuencia de copia de seguridad es mensual o menor, puede hacer que el plan de copia de seguridad cambie a instantáneas de EBS.

c. El periodo de retención total es el número de días que se almacenan los recursos en AWS Backup. Es el número total de días de almacenamiento templado más almacenamiento en frío.

8. (Opcional) Utilice Copiar en el destino para crear una copia entre regiones de los recursos que cumplen los requisitos si desea almacenar una copia de seguridad en otra Región de AWS.

9. (Opcional) Etiquetas agregadas a puntos de recuperación.

10. Cuando todas las secciones estén configuradas según sus especificaciones, elija Guardar regla de copia de seguridad.

Creación de planes de respaldo mediante el AWS CLI

También puede definir su plan de copia de seguridad en un documento JSON y proporcionarlo mediante la consola de AWS Backup o la AWS CLI. El siguiente documento JSON contiene un ejemplo de plan de copias de seguridad que crea una copia de seguridad diaria a las 13:00, hora del Pacífico (la hora local se ajusta a las condiciones de luz diurna, estándar o de verano, si corresponde). Elimina automáticamente una copia de seguridad al cabo de un año.

```
{
  "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
        }
      }
    ]
  }
}
```

Puede almacenar el documento JSON con el nombre que elija. El siguiente comando de la CLI muestra `create-backup-plan` con un JSON denominado `test-backup-plan.json`:

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

Tenga en cuenta que, si bien algunos sistemas numeran los días de la semana del 0 al 6, nosotros los numeramos del 1 al 7. Para obtener más información, consulte Expresiones cron. Para obtener más información sobre las zonas horarias, consulta la referencia de TimeZonela API de Amazon Location Service.

Opciones y configuración del plan de copia de seguridad

Al definir un plan de respaldo en la AWS Backup consola, se configuran las siguientes opciones:

Nombre del plan de copia de seguridad

Debe proporcionar un nombre único de plan de copias de seguridad.

Si elige un nombre que sea idéntico al nombre de un plan existente, recibirá un mensaje de error.

Reglas de copia de seguridad

Los planes de copias de seguridad se componen de una o más reglas de copia de seguridad. Para agregar reglas de copia de seguridad a un plan de copia de seguridad o para editar las reglas existentes en un plan de copia de seguridad:

1. En la AWS Backup consola, en el panel de navegación izquierdo, selecciona Planes de Backup.
2. En Nombre del plan de copia de seguridad, seleccione un plan de copia de seguridad.
3. En la sección Reglas de copia de seguridad:
   - Para agregar una regla de copia de seguridad, elija Agregar regla de copia de seguridad.
   - Para editar una regla de copia de seguridad existente, elija la regla y, a continuación, elija Editar.

> **Note**
>
> Si tiene un plan de respaldo con varias reglas y los plazos de ambas reglas se superponen, AWS Backup optimiza la copia de seguridad y toma una copia de seguridad para la regla con el mayor tiempo de retención. La optimización tiene en cuenta el intervalo de inicio completo, no solo el momento en que se realiza la copia de seguridad diaria.

Cada regla de copia de seguridad consta de los siguientes elementos.

Nombre de la regla de copia de seguridad

Los nombres de la regla de copia de seguridad distinguen mayúsculas de minúsculas. Deben contener de 1 a 50 caracteres alfanuméricos o guiones.

Backup frequency (Frecuencia de copia de seguridad)

La frecuencia de las copias de seguridad determina la frecuencia con la que se AWS Backup crea una copia de seguridad instantánea. En la consola, puede elegir una frecuencia de cada hora, cada 12 horas, diaria, semanal o mensual. También puede crear una expresión cron que cree copias de seguridad instantáneas con una frecuencia de una hora. Con la AWS Backup CLI, puede programar copias de seguridad de instantáneas con una frecuencia de hasta una hora.

Si selecciona semanalmente, puede especificar en qué días de la semana desea que se lleven a cabo las copias de seguridad. Si selecciona mensualmente, puede elegir un día determinado del mes.

También puede marcar la casilla Habilitar copias de seguridad continuas para los recursos compatibles para crear una regla de copia de seguridad continua habilitada para la point-in-time restauración (PITR). A diferencia de las copias de seguridad instantáneas, las copias de seguridad continuas permiten realizar restauraciones. point-in-time Para obtener más información sobre las copias de seguridad continuas, consulte Recuperación en un momento dado.

Backup target (Intervalo de copia de seguridad)

Los periodos de copia de seguridad constan de la hora de comienzo del periodo de copia de seguridad y de la duración del periodo indicada en horas. Los trabajos de copia de seguridad comienzan dentro de este periodo. La configuración predeterminada de la consola es:

- 12:30 a. m., hora local según la zona horaria del sistema (0:30 en sistemas abiertos las 24 horas)
- Inicio dentro de 8 horas
- Conclusión en 7 días

  (El parámetro Completar en no se aplica a recursos de Amazon FSx)

Puede personalizar la frecuencia de las copias de seguridad y la hora de inicio del periodo de copia de seguridad mediante una expresión cron. Para ver los seis campos de las expresiones AWS cron, consulte Cron Expressions en la Guía del usuario de Amazon CloudWatch Events. Dos ejemplos de expresiones AWS cron son `15 * ? * * *` (realizar una copia de seguridad cada hora 15 minutos después de la hora) y `0 12 * * ? *` (realizar una copia de seguridad todos los días a las 12 del mediodía UTC). Para ver una tabla de ejemplos, haga clic en el enlace anterior y desplácese hacia abajo en la página.

AWS Backup evalúa las expresiones cron entre las 00:00 y las 23:59. Si crea una regla de copia de seguridad “cada 12 horas” pero especifica una hora de inicio posterior a las 11:59, solo se ejecutará una vez al día.

Las copias de seguridad y point-in-time restauración continuas (PITR) hacen referencia a los cambios registrados durante un período de tiempo; por lo tanto, no se pueden programar con una expresión de hora o cron.

> **Note**
>
> En general, los servicios de AWS bases de datos no pueden iniciar las copias de seguridad 1 hora antes o durante su período de mantenimiento y Amazon FSx no puede iniciar las copias de seguridad 4 horas antes o durante su período de mantenimiento o período de respaldo automático (Amazon Aurora está exento de esta restricción de período de mantenimiento). Las copias de seguridad instantáneas programadas durante esos periodos producirán un error.
> Hay una excepción cuando opta por utilizar AWS Backup tanto para copias de seguridad instantáneas como continuas para un servicio compatible. AWS Backup programará los intervalos de copia de seguridad automáticamente para evitar conflictos. Consulte Point-in-Time Recovery para obtener una lista de los servicios compatibles e instrucciones sobre cómo utilizarlos AWS Backup para realizar copias de seguridad continuas.

Reglas de copia de seguridad superpuestas

En ocasiones, un plan de copia de seguridad puede contener varias reglas superpuestas. Cuando las ventanas de inicio de diferentes reglas se superpongan, AWS Backup conserva la copia de seguridad según la regla con un período de retención más largo. Por ejemplo, considere un plan de copia de seguridad con dos reglas:

1. Copia de seguridad cada hora, con un intervalo de inicio de 1 hora y retención de 1 día.
2. Copia de seguridad cada 12 horas, con un intervalo de inicio de 8 horas y retención de 1 semana.

Al cabo de 24 horas, la segunda regla crea dos copias de seguridad (ya que es la que tiene un periodo de retención más largo). La primera regla crea ocho copias de seguridad (porque el intervalo de inicio de 8 horas de la segunda regla impedía que se ejecutaran más copias de seguridad por hora). En concreto:

Durante este intervalo de inicio	Esta regla crea una copia de seguridad
De medianoche a 8 h	12 horas
De 8 a 9	Por hora
De 9 a 10	Por hora
De 10 a 11	Por hora
De 11 a mediodía	Por hora
De mediodía a 20 h	12 horas
De 8 a 9	Por hora
De 9 a 10	Por hora
De 10 a 11	Por hora
De 11 a medianoche	Por hora

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado `CREATED` hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia a`RUNNING`) o hasta que el estado del trabajo cambie a `EXPIRED` (lo que se espera que ocurra cuando termine el tiempo de la ventana de inicio).

Ciclo de vida y niveles de almacenamiento

Las copias de seguridad se almacenan durante el número de días que especifique, lo que se conoce como ciclo de vida de la copia de seguridad. Las copias de seguridad se pueden restaurar hasta el final de su ciclo de vida.

Se establece como el período de retención total en la sección del ciclo de vida de la configuración de las reglas de respaldo en la AWS Backup consola.

Si lo usa AWS CLI, se establece mediante el parámetro `DeleteAfterDays`. El periodo de retención de las instantáneas puede oscilar entre 1 día y 100 años (o indefinidamente si no se introduce nada), mientras que el periodo de retención de las copias de seguridad continuas puede oscilar entre 1 y 35 días. La fecha de creación de una copia de seguridad es la fecha en que se inició el trabajo de copia de seguridad, no la fecha en que se completó. Si el trabajo de copia de seguridad no se completa en la misma fecha en que se inició, utilice la fecha en la que comenzó para calcular los períodos de retención.

Las copias de seguridad se mantienen en un nivel de almacenamiento. Cada nivel conlleva un costo de almacenamiento y restauración diferente, tal como se indica en Precios de AWS Backup. Todas las copias de seguridad se crean y se almacenan en almacenamiento templado. Según el tiempo que decida almacenar la copia de seguridad, es posible que desee pasarla a un nivel de menor costo denominado almacenamiento en frío. Disponibilidad de características por recurso muestra qué recursos tienen esta característica opcional.

Console

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Cree o edite un plan de copia de seguridad.
3. En la sección de ciclo de vida de la configuración de reglas de copia de seguridad, marca la casilla Mover copias de seguridad de almacenamiento templado almacenamiento en frío.
4. (Opcional) Si Amazon EBS es uno de los recursos de los que hace copias de seguridad y la frecuencia de copia de seguridad es mensual o menor, puede pasarlas a nivel frío mediante el archivado de instantáneas de EBS.
5. Introduzca un valor (en días) para indicar que las copias de seguridad permanecen almacenadas en caliente. AWS Backup recomienda un mínimo de 8 días.
6. Introduzca un valor (en días) para el periodo de retención total. La diferencia entre el periodo de retención total y el tiempo de almacenamiento en caliente será el número de días que las copias de seguridad permanezcan en almacenamiento en frío.

AWS CLI

1. Utilice `create-backup-plan` or `update-backup-plan`.
2.
3. Incluya el parámetro booleano `OptInToArchiveForSupportedResources`para los recursos de EBS.

4. Incluya el parámetro `MoveToColdStorageAfterdays`.
5. Utilice el parámetro `DeleteAfterDays`. Este valor debe ser 90 (días) más el valor que introduzca para `MoveToColdStorageAfterDays`.

El almacenamiento en frío está disponible actualmente para los siguientes tipos de recursos:

Tipo de recurso	Copia de seguridad incremental o completa en almacenamiento en frío
AWS CloudFormation	Incremental
DynamoDB con características avanzadas de	Completa; no hay copias de seguridad incrementales en ningún nivel
Amazon EBS (mediante Archivo de instantán eas de EBS)	Completa; las copias de seguridad increment ales se convertirán en completas después de la transición.
Amazon EFS	Incremental
Bases de datos de SAP HANA que se ejecutan en instancias de Amazon EC2	Incremental
Amazon Timestream	Incremental
Máquinas virtuales de VMware	Incremental

Una vez que haya activado la transición al almacenamiento en frío mediante la consola o la línea de comandos, se cumplen las siguientes condiciones para copias de seguridad en almacenamiento (o archivo) en frío:

- Las copias de seguridad transferidas deben almacenarse en cámaras frigoríficas durante un mínimo de 90 días, además del tiempo en cámaras templadas. AWS Backup requiere que la retención se establezca durante 90 días más que la configuración de «transición al frío después de días». El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede modificarse una vez que una copia de seguridad se ha migrado al almacenamiento en frío.

- Algunos servicios admiten copias de seguridad incrementales. Para las copias de seguridad incrementales, debe tener al menos una copia de seguridad completa en caliente. AWS Backup recomienda configurar su ciclo de vida para no mover la copia de seguridad a una cámara frigorífica hasta transcurridos al menos 8 días. Si la copia de seguridad completa pasa a una cámara de almacenamiento en frío demasiado pronto (por ejemplo, si se pasa a una cámara de almacenamiento en frío después de un día), AWS Backup se creará otra copia de seguridad completa en caliente.
- En el caso de los tipos de recursos que admiten copias de seguridad incrementales, AWS Backup los datos pasan del almacenamiento en caliente al almacenamiento en frío si las copias de seguridad en caliente ya no hacen referencia a los datos en transición. Los datos de las copias de seguridad retenidas en almacenamiento en frío a los que solo hacen referencia otras copias de seguridad en frío se facturan según los precios de los niveles de almacenamiento en frío. Otras copias de seguridad continúan con los precios de los niveles de almacenamiento en caliente.

Almacén de copias de seguridad

Un almacén de copias de seguridad es un contenedor que sirve para organizar sus copias de seguridad. Las copias de seguridad creadas por una regla de copia de seguridad se organizan en el almacén de copia de seguridad que especifique en la regla de copia de seguridad. Puede usar las bóvedas de respaldo para establecer la clave de cifrado AWS Key Management Service (AWS KMS) que se usa para cifrar las copias de seguridad en la bóveda de respaldo y para controlar el acceso a las copias de seguridad en la bóveda de respaldo. Puede añadir también etiquetas a los almacenes de copias de seguridad para organizarlos. Si no desea utilizar el almacén predeterminado, puede crear el suyo propio. Para obtener step-by-step instrucciones sobre cómo crear un almacén de copias de seguridad, consulte. Paso 3: cree un almacén de copias de seguridad

Realizar copias entre regiones

Si lo desea, como parte del plan de copia de seguridad, puede crear una copia de una copia de seguridad en otra Región de AWS. Para obtener más información sobre las copias de las copias de seguridad, consulte Creación de copias de las copias de seguridad entre Regiones de AWS.

Cuando defina una réplica de una copia de seguridad, tendrá que establecer las siguientes opciones:

Región de destino

Región de destino de la copia de seguridad.

Almacén de copias de seguridad (configuración avanzada)

Almacén de copia de seguridad de destino de la copia.

(Configuración avanzada) Rol de IAM

La función de IAM que se AWS Backup utiliza al crear la copia. El rol también debe AWS Backup figurar como entidad de confianza, lo que AWS Backup permite asumirlo. Si eliges Predeterminado y el rol AWS Backup predeterminado no está presente en tu cuenta, se crea un rol para ti con los permisos correctos.

(Configuración avanzada) Ciclo de vida

Especifica cuándo se va a migrar la copia de seguridad al almacenamiento en frío y cuándo va a caducar (eliminarse). Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Una vez que la copia ha migrado al almacenamiento en frío, no se puede modificar este valor.

Vencimiento especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío.

Etiquetas agregadas a puntos de recuperación

Las etiquetas que enumere aquí se añaden automáticamente a las copias de seguridad cuando se crean.

Etiquetas agregadas a planes de copia de seguridad

Estas etiquetas están asociadas con el propio plan de copias de seguridad para ayudarle a organizar y realizar un seguimiento de su plan de copias de seguridad.

Configuración de copia de seguridad avanzada

Permite realizar copias de seguridad coherentes con la aplicación para las aplicaciones de terceros que se ejecutan en instancias de Amazon EC2. Actualmente, AWS Backup es compatible con las copias de seguridad de Windows VSS. AWS Backup excluye tipos específicos de instancias de Amazon EC2 de las copias de seguridad de Windows VSS. Para obtener más información, consulte Creación de copias de seguridad de Windows VSS.

AWS CloudFormation plantillas para planes de respaldo

Proporcionamos dos AWS CloudFormation plantillas de muestra para su referencia. La primera plantilla crea un plan de copia de seguridad sencillo. La segunda plantilla permite realizar copias de seguridad VSS en un plan de copia de seguridad.

> **Note**
>
> Si utiliza el rol de servicio predeterminado, reemplace el *`rol de servicio`* por `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
```

Asignación de recursos a un plan de copia de seguridad

La asignación de recursos especifica qué recursos AWS Backup protegerá con su plan de respaldo. AWS Backup le proporciona una configuración predeterminada simple y controles detallados para asignar recursos a su plan de respaldo. Cada vez que se ejecuta su plan de respaldo, Cuenta de AWS busca todos los recursos que coincidan con sus criterios de asignación de recursos. Este nivel de automatización le permite definir el plan de respaldo y la asignación de recursos exactamente una vez. AWS Backup hace abstracción de la tarea de buscar y hacer copias de seguridad de nuevos recursos que se ajusten a la asignación de recursos definida anteriormente.

Puede asignar cualquier tipo AWS Backup de recurso compatible que haya elegido administrar. AWS Backup Para obtener instrucciones sobre cómo optar por más tipos de recursos AWS Backup compatibles, consulte Primeros pasos 1: suscripción al servicio.

La AWS Backup consola tiene dos formas de incluir los tipos de recursos en un plan de respaldo: asignar explícitamente el tipo de recurso en un plan de respaldo o incluir todos los recursos. Consulte los puntos siguientes para entender cómo funcionan estas selecciones con las suscripciones a servicios.

- Si las asignaciones de recursos se basan únicamente en etiquetas, se aplica la configuración de suscripción al servicio.
- Si un tipo de recurso se asigna explícitamente a un plan de respaldo, se incluirá en el respaldo incluso si la opción no está habilitada para ese servicio en particular. Esto no se aplica a Aurora, Neptune ni Amazon DocumentDB. Para incluir estos servicios, la suscripción debe estar habilitada.
- Si se especifican tanto el tipo de recurso como las etiquetas en una asignación de recursos, los tipos de recursos especificados se filtran primero y, a continuación, las etiquetas filtran aún más esos recursos.

  La configuración de suscripción del servicio se ignora en la mayoría de los tipos de recursos. Sin embargo, Aurora, Neptune y Amazon DocumentDB requieren la suscripción del servicio.

- Cuando una cuenta utiliza AWS Backup (crea un almacén de copias de seguridad o un plan de copias de seguridad) en una región, la cuenta opta automáticamente por todos los tipos de recursos admitidos por la región AWS Backup en ese momento. Los servicios compatibles que se agreguen a esa región en una fecha posterior no se incluirán automáticamente en un plan de respaldo. Puede optar por utilizar esos tipos de recursos una vez que se admitan.
- En el caso de Amazon FSx para NetApp ONTAP, cuando utilice la selección de recursos basada en etiquetas, aplique etiquetas a volúmenes individuales en lugar de a todo el sistema de archivos.

La asignación de recursos puede incluir (o excluir) tipos de recursos y recursos.

- Un tipo de recurso incluye todas las instancias o recursos de un AWS servicio AWS Backup compatible o de una aplicación de terceros. Por ejemplo, el tipo de recurso de DynamoDB hace referencia a todas las tablas de DynamoDB.
- Un recurso es una instancia única de un tipo de recurso, como una de las tablas de DynamoDB. Puede especificar un recurso mediante su ID de recurso único.

Puede ajustar aún más la asignación de recursos mediante etiquetas y operadores condicionales.

Temas

Asignación de recursos mediante la consola

Para ir a la página Asignación de recursos:

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Elija Planes de copia de seguridad.
3. Elija Crear plan de copia de seguridad.
4. Seleccione cualquier plantilla en la lista desplegable Elegir plantilla y, a continuación, elija Crear plan.
5. Escriba el Nombre del plan de copia de seguridad.

6. Elija Crear plan.
7. Elija Asignar recursos.

Para comenzar la asignación de recursos, en la sección General:

1. Escriba un Nombre de asignación de recursos.
2. Elija el Rol predeterminado o Elegir un rol de IAM.

> **Note**
>
> Si elige un rol de IAM, verifique que tiene permiso para hacer copias de seguridad de todos los recursos que va a asignar. Si su rol encuentra un recurso para el que no tiene permiso para hacer una copia de seguridad, se producirá un error en el plan de copia de seguridad.

Para asignar sus recursos, en la sección Asignar recursos, elija una de las dos opciones que aparecen en Definir la selección de recurso:

- Incluir todos los tipos de recursos. Esta opción configura su plan de respaldo para proteger todos los recursos AWS Backup compatibles actuales y futuros asignados a su plan de respaldo. Utilice esta opción para proteger su patrimonio de datos de forma rápida y sencilla.

  Si elige esta opción, como siguiente paso, puede Ajustar la selección mediante etiquetas.
- Incluir tipos de recursos específicos. Al elegir esta opción, debe Seleccionar tipos de recursos específicos mediante los siguientes pasos:

  1. En el menú desplegable Seleccionar tipos de recursos, asigne uno o más tipos de recursos.

> **Important**
>
> RDS, Aurora, Neptune y DocumentDB comparten el mismo nombre de recurso de Amazon (ARN). Al suscribirse para administrar uno de estos tipos de recursos con AWS Backup , se suscribe para todos ellos al asignarlos a un plan de copia de seguridad. Para ajustar la selección, utilice etiquetas y operadores condicionales.

Cuando termine, le AWS Backup presenta la lista de tipos de recursos que ha seleccionado y su configuración predeterminada, que consiste en proteger todos los recursos de cada tipo de recurso seleccionado.

2. Si lo desea, si desea excluir recursos específicos de un tipo de recurso que haya seleccionado:

    1. Usa el menú desplegable Elegir recursos y qanule la selección de la opción predeterminada.
    2. Seleccione los recursos específicos para asignarlos a su plan de copia de seguridad.

3. Si lo desea, puede Excluir ID de recursos específicos de los tipos de recursos seleccionados. Utilice esta opción si desea excluir uno o varios recursos de entre muchos, ya que hacerlo puede resultar más rápido que seleccionar muchos recursos en el paso anterior. Debe incluir un tipo de recurso antes de poder excluir los recursos de ese tipo de recurso. Para excluir un identificador de recurso, siga estos pasos:

    1. En Excluir ID de recursos específicos de los tipos de recursos seleccionados, elija uno o más de los tipos de recursos que incluyó en Seleccionar tipos de recursos.
    2. Para cada tipo de recurso, utilice el menú Elegir recursos para seleccionar uno o más recursos para excluirlos.

Además de las opciones anteriores, puede realizar selecciones aún más detalladas mediante la característica opcional Ajustar la selección mediante etiquetas. Esta característica le permite ajustar su selección actual para incluir un subconjunto de sus recursos mediante etiquetas.

Las etiquetas son pares clave-valor que puede asignar a recursos concretos para ayudarle a identificar, organizar y filtrar los recursos. Las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Etiquetado de los recursos de AWS en la Referencia general de AWS .

Al ajustar la selección con dos o más etiquetas, el efecto es una condición AND. Por ejemplo, si ajusta su selección con dos etiquetas, `env: prod` y `role: application`, solo asignas recursos con AMBAS etiquetas a su plan de copia de seguridad.

Para ajustar su selección mediante etiquetas:

1. En Ajustar la selección mediante etiquetas, elija una clave de la lista desplegable.
2. Seleccione una Condición de valor de la lista desplegable.

- El valor hace referencia a la siguiente entrada, el valor del par clave-valor.
- La condición puede ser `Equals`, `Contains`, `Begins with` o `Ends with`, o su inversa: `Does not equal`, `Does not contain`, `Does not begin with` o `Does not end with`.

3. Seleccione un Valor del menú desplegable.
4. Para ajustar aún más utilizando otra etiqueta, elija Agregar etiqueta.

Asignación de recursos mediante programación

Puede definir una asignación de recursos en un documento JSON. En este ejemplo de asignación de recursos se asignan todas las instancias de Amazon EC2 al plan de copia de seguridad *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/*"
    ]
  }
}
```

Suponiendo que este JSON esté almacenado como `backup-selection.json`, puede asignar estos recursos a su plan de copia de seguridad mediante el siguiente comando de la CLI:

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

A continuación, se muestran ejemplos de asignaciones de recursos, junto con el documento JSON correspondiente. Para facilitar la lectura de esta tabla, en los ejemplos se omiten los campos `"BackupPlanId"`, `"SelectionName"` y `"IamRoleArn"`. El comodín `*` representa cero o más caracteres que no sean espacios en blanco.

Example Ejemplo: seleccionar todos los recursos de mi cuenta

```
{
```

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

Example Ejemplo: seleccionar todos los recursos de mi cuenta, pero excluir los volúmenes de EBS

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

Example Ejemplo: seleccione todos los recursos etiquetados con"backup":"true", pero excluya los volúmenes de EBS

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

Example Ejemplo: seleccione todos los volúmenes de EBS y las instancias de base de datos de RDS etiquetadas con ambos caracteres y "backup":"true""stage":"prod"

La aritmética booleana es similar a la de las políticas de IAM: con aquellas en "Resources" combinados utilizando un OR booleano y aquellas en `"Conditions"` combinadas utilizando un AND booleano.

La expresión `"arn:aws:rds:*:*:db:*"` de `"Resources"` solo selecciona instancias de base de datos de RDS porque no hay recursos de Aurora, Neptune o DocumentDB correspondientes.

```
{
  "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 Ejemplo: seleccione todos los volúmenes de EBS e instancias de RDS etiquetados con pero no "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 Ejemplo: seleccione todos los recursos etiquetados con "key1" y un valor que comience por, "include" pero no por, un valor que contenga la palabra "key2""exclude"

Puede utilizar el carácter comodín al principio, al final y al centro de una cadena. Observe el uso del carácter comodín (*) en `include*` y `*exclude*` en el ejemplo anterior. También puede utilizar el carácter comodín en el centro de una cadena, como se muestra en el ejemplo anterior, `arn:aws:rds:*:*:db:*`.

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

```
}
```

Example Ejemplo: seleccione todos los recursos etiquetados con, "backup":"true" excepto los sistemas de archivos FSx y los recursos de RDS, Aurora, Neptune y DocumentDB

Los elementos incluidos `NotResources` se combinan utilizando el booleano OR.

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

Example Ejemplo: seleccione todos los recursos etiquetados con una etiqueta y cualquier valor "backup"

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

```
    }
  }
}
```

Example Ejemplo: seleccione todos los sistemas de archivos FSx, el clúster "my-aurora-cluster" Aurora y todos los recursos etiquetados con"backup":"true", excepto los recursos etiquetados con "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 Ejemplo: seleccione todos los recursos etiquetados con la etiqueta**`"backup":"true"`**, excepto los volúmenes de EBS etiquetados con **`"stage":"test"`**

Utilice dos comandos de la CLI para crear dos selecciones para seleccionar este grupo de recursos. La primera selección se aplica a todos los recursos, excepto a los volúmenes de EBS. La segunda selección se aplica a los volúmenes de 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"
        }
      ]
    }
  }
}
```

Asignación de recursos mediante AWS CloudFormation

Esta end-to-end AWS CloudFormation plantilla crea una asignación de recursos, un plan de respaldo y un almacén de respaldo de destino:

- Un almacén de copias de seguridad denominado *`CloudFormationTestBackupVault`*.
- Nombre de un plan de respaldo *`CloudFormationTestBackupPlan`*. Este plan contiene dos reglas de copia de seguridad, que hacen copias de seguridad todos los días a las 12 del mediodía UTC y las retienen durante 210 días.
- Una selección de recursos denominada *`BackupSelectionName`*.
- • La asignación de recursos hace una copia de seguridad de los siguientes recursos:
  - Cualquier recurso etiquetado con el par clave-valor `backupplan:dsi-sandbox-daily`.
  - Cualquier recurso etiquetado con el valor `prod` o valores que comiencen por `prod/`.
  - La asignación de recursos no hace una copia de seguridad de los siguientes recursos:
    - Cualquier clúster de RDS, Aurora, Neptune o DocumentDB.
    - Cualquier recurso etiquetado con el valor `test` o valores que comiencen por `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/*
```

Cuotas de asignación de recursos

Las siguientes cuotas se aplican a una sola asignación de recursos:

- 500 nombres de recursos de Amazon (ARN) sin caracteres comodín
- 30 ARN con expresiones comodín
- 30 condiciones
- 30 etiquetas por asignación de recurso (y un número ilimitado de recursos por etiqueta)

Eliminación de un plan de copia de seguridad

Puede eliminar un plan de copias de seguridad solo después de haber eliminado todas las selecciones de recursos asociadas. Estas selecciones también se conocen como asignaciones de recursos. Si no se eliminaron antes de eliminar el plan de respaldo, la consola mostrará el siguiente error: «Las selecciones de planes de respaldo relacionadas deben eliminarse antes de eliminar el plan de respaldo». Use la consola o use `DeleteBackupSelection`.

La eliminación de un plan de copias de seguridad elimina la versión actual del plan. Las versiones actual y anterior, si las hay, existen todavía, pero ya no se incluyen en la consola en Backup plans (Planes de copias de seguridad).

> **Note**
>
> Cuando se elimina un plan de copia de seguridad, las copias de seguridad existentes no se eliminan. Para eliminar las copias de seguridad existentes, tiene que suprimirlas en el almacén de copias de seguridad en Eliminación de copias de seguridad.

Para eliminar un plan de respaldo mediante la AWS Backup consola

1. Inicie sesión en la AWS Management Console AWS Backup consola y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación de la izquierda, seleccione Backup plans (Planes de copia de seguridad).
3. Elija el plan de copias de seguridad en la lista.
4. Seleccione las asignaciones de recursos que están asociadas al plan de copia de seguridad.

5. Elija Eliminar.

Actualización de un plan de copia de seguridad

Tras crear un plan de copia de seguridad, puede modificar el plan; por ejemplo, puede agregar etiquetas o puede agregar, modificar o eliminar reglas de copia de seguridad. Los cambios que realice en un plan de copias de seguridad no tienen ningún efecto sobre las copias de seguridad existentes creadas por el plan de copia de seguridad. Los cambios se aplican únicamente a las copias de seguridad que se crean en el futuro.

Por ejemplo, cuando se actualiza el período de retención en una regla de copia de seguridad, el período de retención de las copias de seguridad creadas antes de la actualización sigue siendo el mismo. Las copias de seguridad que cree dicha regla en el futuro muestran el periodo de retención actualizado.

No puede cambiar el nombre de un plan una vez creado.

Para editar un plan de respaldo mediante la AWS Backup consola

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, seleccione Backup plans (Planes de copias de seguridad).
3. En el segundo panel, Planes de Backup, se muestran los planes anteriores existentes. Seleccione el enlace subrayado en la columna Nombre del plan de respaldo para ver los detalles del plan de respaldo elegido.
4. Puede editar una regla de copia de seguridad, ver las asignaciones de recursos, ver los trabajos de copia de seguridad, administrar etiquetas o cambiar la configuración de Windows VSS.
5. Para actualizar una regla de copia de seguridad, seleccione el nombre de la regla de copia de seguridad.

   Seleccione Administrar etiquetas para añadir o eliminar etiquetas.

   Selecciona Editar junto a Configuración avanzada de copias de seguridad para activar o desactivar Windows VSS.
6. Cambie los ajustes que prefiera y, a continuación, seleccione Guardar.

Almacenes de copias de seguridad

> **Note**
>
> A partir del 9 de agosto de 2023, ofrecerá AWS Backup una vista previa para utilizar una bóveda con huecos lógicos. `<Para inscribirte en esta versión preliminar, envía una solicitud por correo` Las características podrían cambiar o ajustarse durante y después del periodo de versión preliminar. Cuando el servicio pase a estar disponible en general (GA), los datos y las configuraciones proporcionados durante la versión preliminar dejarán de estar disponibles. AWS recomienda utilizar datos de prueba en lugar de datos de producción en la versión preliminar.

En AWS Backup, una bóveda de copias de seguridad es un contenedor que almacena y organiza las copias de seguridad.

Al crear un almacén de copias de seguridad, debe especificar la clave de cifrado AWS Key Management Service (AWS KMS) que cifra algunas de las copias de seguridad almacenadas en este almacén. El cifrado de otras copias de seguridad lo administran sus AWS servicios de origen. Para obtener más información acerca del cifrado de copias de seguridad, consulte el gráfico Cifrado para copias de seguridad en AWS.

Su cuenta siempre tendrá un almacén de copias de seguridad predeterminado. Si necesita diferentes claves de cifrado o políticas de acceso para diferentes grupos de copias de seguridad, puede crear varios almacenes de copias de seguridad.

En esta sección se proporciona información general sobre cómo administrar los almacenes de copia de seguridad en AWS Backup.

Temas

Almacenes aislados lógicamente (versión preliminar)

> **Note**
>
> A partir del 9 de agosto de 2023, AWS Backup ofrecerá una vista previa para utilizar una bóveda con huecos lógicos.
> `<Para inscribirte en esta versión preliminar, envía una solicitud por correo`
> Las características podrían cambiar o ajustarse durante y después del periodo de versión preliminar. Cuando el servicio pase a estar disponible en general (GA), los datos y las configuraciones proporcionados durante la versión preliminar dejarán de estar disponibles. AWS recomienda utilizar datos de prueba en lugar de datos de producción en la versión preliminar.

Información general

AWS Backup está previsualizando un tipo de almacén secundario que puede almacenar copias de seguridad en otros almacenes. Un almacén aislado lógicamente es un almacén especializado que ofrece características de seguridad adicionales a las de un almacén de copias de seguridad, así como la posibilidad de compartir el acceso al almacén con otras cuentas y organizaciones, de forma que el tiempo de recuperación (RTO) sea más rápido y flexible en caso de que se produzca un incidente que requiera una restauración rápida de los recursos.

Lógicamente, las bóvedas herméticas vienen equipadas con funciones de protección adicionales: cada una de estas bóvedas está cifrada con una clave propia y cada bóveda tiene una AWS cerradura configurada en modo de conformidad.

Puede optar por compartir un almacén aislado lógicamente entre organizaciones y cuentas para que las copias de seguridad almacenadas en él se puedan restaurar desde una cuenta con la que se comparta el almacén, si es necesario.

Durante el periodo de versión preliminar, no habrá ningún costo adicional por el almacenamiento en almacenes aislados lógicamente. Las copias de seguridad que se encuentren en almacenes de copias de seguridad estándar y las copias entre regiones se seguirán cobrando según las tarifas publicadas (consulte los precios), aunque no se cobrará por ninguna copia de esas copias de seguridad que se encuentre en almacenes aislados lógicamente.

Caso de uso

Una almacén aislado lógicamente es un almacén secundario que sirve como parte de una estrategia de protección de datos. Este almacén puede ayudar a mejorar la retención y la recuperación de su organización cuando quiera un almacén para sus copias de seguridad que

- esté configurado automáticamente con un bloqueo de almacén en modo de cumplimiento;
- contenga copias de seguridad que se puedan compartir y restaurar desde una cuenta diferente a la que creó la copia de seguridad;
- Viene encriptado con una clave propia AWS

Los recursos admitidos en un almacén aislado lógicamente incluyen

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

Esta versión preliminar de los almacenes aislados lógicamente solo está disponible en la región Este de EE. UU. (Norte de Virginia). Como esta característica solo está disponible actualmente en una región, no se admite la copia entre regiones durante este periodo de versión preliminar.

Comparación y contraste con un almacén de copias de seguridad estándar

Una bóveda de respaldo es el tipo de bóveda principal y estándar que se utiliza en AWS Backup. Cada copia de seguridad se almacena en un almacén de copias de seguridad cuando se crea la copia de seguridad. Puede asignar políticas basadas en recursos para administrar las copias de seguridad almacenadas en el almacén, como el ciclo de vida de las copias de seguridad almacenadas.

Un almacén aislado lógicamente es un almacén especializado con seguridad adicional y uso compartido flexible para acelerar el tiempo de recuperación (RTO). Este almacén conserva copias de las copias de seguridad que se crearon inicialmente y se guardaron en un almacén de copias de seguridad estándar.

Los almacenes de copias de seguridad se pueden cifrar con una clave, un mecanismo de seguridad que limita el acceso a los usuarios previstos. Estas claves pueden gestionarse o AWS gestionarse por el cliente. Además, un almacén de copias de seguridad puede estar aún más protegido con una bloqueo de almacén; un almacén aislado lógicamente viene equipado con un bloqueo de almacén en modo de cumplimiento.

Si la AWS KMS clave no se cambió manualmente ni se configuró como una clave administrada por el cliente (CMK) en el momento en que se creó el recurso inicial, la copia de seguridad no se puede copiar en un almacén cerrado de forma lógica.

Característica	Almacén de copias de seguridad	Almacén aislado lógicamente (versión preliminar)
Creación de copia de seguridad	Cuando se crea una copia de seguridad, se almacena como un punto de recuperación	Las copias de seguridad no se almacenan en este almacén al crearlas
Almacenamiento de copias de seguridad	Puede almacenar las copias de seguridad iniciales de los recursos y las copias de las copias de seguridad	Puede almacenar copias de las copias de seguridad de otros almacenes
Seguridad	Opcionalmente, se puede cifrar con una clave (gestiona da o gestionada por el cliente) AWS Opcionalmente, se puede bloquear con un bloqueo de almacén	Se cifra con una AWS clave propia Siempre se bloquea con un bloqueo de almacén en modo de cumplimiento
Uso compartido	El acceso se puede administr ar mediante políticas y AWS Organizations No es compatible con AWS Resource Access Manager	Opcionalmente, se puede compartir entre cuentas mediante AWS RAM

Característica	Almacén de copias de seguridad	Almacén aislado lógicamente (versión preliminar)
Restauración	Las copias de seguridad se pueden restaurar por medio de la misma cuenta propietaria del almacén	Las copias de seguridad se pueden restaurar con una cuenta distinta de la que es propietaria de la copia de seguridad si el almacén se comparte con esa cuenta independiente
Regionalidad	Disponible en todas las regiones en las que AWS Backup opera	Disponible en la región Este de EE. UU. (Norte de Virginia) durante la versión preliminar
Recursos	Puede almacenar copias de seguridad que contienen todos los recursos AWS Backup compatibles	Puede almacenar copias de seguridad que contengan datos de Amazon EC2, Amazon EBS, Amazon EFS, Amazon S3 o Amazon RDS

Creación de un almacén aislado lógicamente desde la consola

> **Important**
>
> Una vez creado el almacén, no es posible cambiar el nombre, el tipo de almacén ni los periodos de retención mínimo y máximo; además, no se puede quitar el bloqueo del almacén. Cuando el servicio esté disponible para el público en general, los datos y las configuraciones proporcionados durante la vista previa dejarán de estar disponibles. AWS recomienda utilizar datos de prueba en lugar de datos de producción en la vista previa.

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, seleccione Almacenes.
3. Se mostrarán ambos tipos de almacén. Seleccione Crear nuevo almacén.

4. Escriba un nombre para su almacén de copias de seguridad. Puede asignar un nombre a su almacén para reflejar lo que almacenará en él o para facilitar la búsqueda de las copias de seguridad que necesite. Por ejemplo, podría denominarlo `FinancialBackups`.
5. Seleccione el botón de opción de almacén aislado lógicamente.
6. Establezca el Periodo de retención mínimo.

   Este valor (en días, meses o años) es el tiempo mínimo que se puede retener una copia de seguridad en este almacén. Las copias de seguridad con periodos de retención inferiores a este valor no se podrán copiar a este almacén.
7. Establezca el Periodo de retención máximo.

   Este valor (en días, meses o años) es el tiempo máximo que se puede retener una copia de seguridad en este almacén. Las copias de seguridad con periodos de retención superiores a este valor no se podrán copiar a este almacén.
8. (Opcional) Agregue etiquetas que le ayuden a buscar e identificar su almacén aislado lógicamente. Por ejemplo, podría añadir una etiqueta `BackupType:Financial`.
9. Seleccione Crear almacén.
10. Revise la configuración. Si todos los ajustes se muestran como esperaba, seleccione Crear almacén aislado lógicamente.
11. La consola le llevará a la página de detalles del nuevo almacén. Compruebe que los detalles del almacén son los esperados.

Visualización de los detalles del almacén aislado lógicamente en la consola

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, seleccione Almacenes.
3. Debajo de las descripciones de los almacenes hay dos listas: Almacenes propiedad de esta cuenta y Almacenes compartidos con esta cuenta. Seleccione la pestaña que desee para ver los almacenes.
4. En Nombre del almacén , haga clic en el nombre del almacén para abrir la página de detalles. Puede ver el resumen, los puntos de recuperación, los recursos protegidos, las cuentas compartidas, la política de acceso y los detalles de las etiquetas.

Copia desde un almacén de copias de seguridad estándar a un almacén aislado lógicamente

Los almacenes aislados lógicamente solo pueden ser el destino de un trabajo de copia en un plan de copia de seguridad o el destino de un trabajo de copia bajo demanda.

Para iniciar un trabajo de copia, debe

- Tener un almacén de copias de seguridad
- Tener un almacén aislado lógicamente
- Tener una copia de seguridad que contenga datos de Amazon EC2, Amazon EBS, Amazon RDS, Amazon S3 o Amazon EFS
- Tener el permiso `kms:CreateGrant` para el rol que se utiliza para crear la copia.
- No hay copias de seguridad cifradas con una clave AWS gestionada como parte de su trabajo de copia en la bóveda, que está aislada de forma lógica

Una vez que confirme lo anterior,

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, seleccione Almacenes.
3. En la página de detalles del almacén, se muestran todos los puntos de recuperación del almacén. Coloque una marca de verificación junto al punto de recuperación que desee copiar.
4. Seleccione Acciones y Editar en el menú desplegable.
5. En la siguiente pantalla, introduzca los detalles del destino.
    a. La región debe ser Este de EE. UU. (Norte de Virginia)
    b. El menú desplegable del almacén de copias de seguridad de destino muestra los almacenes de destino elegibles. Seleccione uno con el tipo `logically air-gapped vault`
6. Seleccione Copiar una vez que todos los detalles estén configurados según sus preferencias.

En la página Trabajos de la consola, puede seleccionar Trabajos de copia para ver los trabajos de copia actuales.

Para obtener más información, consulte Copia de una copia de seguridad, Copia de seguridad entre regiones y Copia de seguridad entre cuentas.

Uso compartido de un almacén aislado lógicamente desde la consola

> **Note**
>
> Solo las cuentas con determinados privilegios de IAM pueden compartir y administrar el uso compartido de cuentas.

Puedes utilizarla AWS RAM para compartir una bóveda cerrada de forma lógica con otras cuentas que tú designes. Para compartir el uso AWS RAM, asegúrate de tener lo siguiente:

- Dos o más cuentas a las que puedan acceder AWS Backup
- Una cuenta que quiera compartir tiene los permisos de RAM necesarios. El permiso `ram:CreateResourceShare` es necesario para realizar este procedimiento. La política `AWSResourceAccessManagerFullAccess` contiene todos los permisos relacionados con RAM necesarios.
- Al menos un almacén aislado lógicamente

Para compartir un almacén aislado lógicamente,

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, seleccione Almacenes.
3. Debajo de las descripciones de los almacenes hay dos listas: Almacenes propiedad de esta cuenta y Almacenes compartidos con esta cuenta. Seleccione la lista que desee para ver los almacenes.
4. En Nombre del almacén , seleccione el nombre del almacén aislado lógicamente para abrir la página de detalles.
5. El panel de uso compartido de cuentas muestra con qué cuentas se comparte el almacén.
6. Para empezar a compartir con otra cuenta o editar las cuentas que ya se comparten, seleccione Administrar el uso compartido.

AWS RAM la consola se abre cuando se selecciona Administrar el uso compartido. Para ver los pasos para compartir un recurso mediante la AWS RAM, consulte Crear un recurso compartido en la AWS RAM.

Asegúrese de tener los permisos adecuados. La Política de IAM de Backup Administrator [AWSBackupFullAccess] y la Política de IAM de Backup Operator [AWSBackupOperatorAccess] contienen el permiso necesario para ver las cuentas compartidas; sin embargo, la función que utilice para compartir necesita permisos de escritura de Resource Access Manager para compartir la cuenta desde la RAM, por ejemplo. `ram:CreateResourceShare`

La cuenta invitada a aceptar una invitación para recibir un recurso compartido tiene 12 horas para aceptarla. Consulte Accepting and rejecting resource share invitations en la Guía del usuario de AWS RAM.

Si ha completado y aceptado los pasos para compartir, la página de resumen del almacén aparecerá en la sección Uso compartido de cuentas = “Compartido; consulte la tabla de cuentas compartidas que aparece a continuación”.

Restauración de una copia de seguridad desde un almacén aislado lógicamente mediante la consola

Puede restaurar una copia de seguridad almacenada en un almacén aislado lógicamente desde la cuenta propietaria del almacén o desde cualquier cuenta con la que se comparta el almacén.

Consulte Restauración de una copia de seguridad para obtener información sobre cómo restaurar un punto de recuperación.

Eliminación de un almacén aislado lógicamente mediante la consola

> **Important**
>
> Cuando el servicio esté disponible para el público en general, los datos y las configuraciones proporcionados durante la vista previa dejarán de estar disponibles. AWS recomienda utilizar datos de prueba en lugar de datos de producción en la vista previa.

Consulte Eliminación de un almacén de copias de seguridad para eliminar un almacén. Los almacenes no se pueden eliminar si aún contienen copias de seguridad (puntos de recuperación). Asegúrese de que el almacén esté vacío antes de iniciar una operación de eliminación.

Almacenes aislados lógicamente mediante CLI/API

Se puede utilizar AWS CLI para realizar operaciones de forma programática en bóvedas con huecos vacíos de forma lógica. Cada CLI es específica del AWS servicio en el que se origina. Los comandos relacionados con el uso compartido llevan el prefijo `aws ram`; todos los demás comandos deben llevar el prefijo `aws backup`.

Creación

El siguiente comando de la CLI de ejemplo, `CreateLogicallyAirGappedBackupVault`, se puede modificar para crear un almacén de copias de seguridad aislado lógicamente:

```
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 (Ver detalles).

El siguiente comando de la CLI de ejemplo, `DescribeBackupVault`, se puede modificar para obtener detalles sobre un almacén:

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

Share

> **Note**
>
> Solo las cuentas con suficientes permisos de IAM pueden compartir y administrar el uso compartido de cuentas.

Puede compartir un almacén aislado lógicamente mediante AWS Resource Access Manager (RAM), un servicio que ayuda a los usuarios a compartir recursos.

AWS RAM usa el comando CLI`create-resource-share`. El acceso a este comando solo está disponible para administradores de cuentas con suficientes permisos. Consulte Creating a resource share in AWS RAM para ver los pasos de la CLI.

Los pasos 1 a 4 se llevan a cabo con la cuenta propietaria del almacén aislado lógicamente. Los pasos 5 a 8 se llevan a cabo con la cuenta con la que se compartirá el almacén aislado lógicamente.

1. Inicie sesión en la cuenta propietaria O solicite que complete estos pasos un usuario de su organización con suficientes credenciales para acceder a la cuenta de origen.

   - Si antes se había creado un recurso compartido y desea agregarle un recurso adicional, utilice, en cambio, la CLI `associate-resource-share` con el ARN del nuevo almacén.

2. Obtenga las credenciales de un rol con permisos suficientes para compartir a través de RAM. Introdúzcalos en la CLI.

   - El permiso `ram:CreateResourceShare` es necesario para realizar este procedimiento. La política AWSResourceAccessManagerFullAccesscontiene todos los permisos relacionados con la RAM.

3. Uso create-resource-share.

   a. Incluya el ARN del almacén aislado lógicamente.

   b. Ejemplo de entrada:

```
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
```

   Ejemplo de salida:

```
{
   "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. Copie el ARN del recurso compartido en el resultado (lo que es necesario para los pasos siguientes). Entregue el ARN al operador de la cuenta a la que invita a recibir el uso compartido.
5. Obtenga el ARN del recurso compartido.

    a. Si no ha realizado los pasos 1 a 4, pídala resourceShareArn a quien lo haya hecho.

    b. Ejemplo: `arn:aws:ram:us-east-1:123456789012:resource-share/12345678-abcd-09876543`
6. En la CLI, asuma las credenciales de la cuenta del destinatario.
7. Obtenga una invitación para compartir recursos con `get-resource-share-invitations`. Para obtener más información, consulte Accepting and rejecting invitations en la Guía del usuario de AWS RAM .
8. Acepte la invitación en la cuenta de destino (recuperación).

    - Use `accept-resource-share-invitation` (también puede `reject-resource-share-invitation`).

Enumeración

El comando de la CLI `ListBackupVaults` se puede modificar para enumerar todos los almacenes que pertenecen a la cuenta y están presentes en ella:

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

Para enumerar solo los almacenes aislados lógicamente, agregue el parámetro

```

--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

Para ver una lista de almacenes compartidas con la cuenta, use

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

```
--by-shared
```

Copiar

Un almacén aislado lógicamente solo puede ser el destino de un trabajo de copia de una copia de seguridad, no el destino de un trabajo de copia de seguridad inicial. Utilice `StartCopyJob` para copiar una copia de seguridad existente en almacén de copias de seguridad a un almacén aislado lógicamente.

El rol que se utilice para crear el trabajo de copia al almacén aislado lógicamente debe incluir el permiso `kms:CreateGrant`.

Ejemplo de entrada de la CLI:

```
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
```

Restaurar

Una vez que se haya compartido una copia de seguridad desde un almacén aislado lógicamente con su cuenta, podrá utilizar `StartRestoreJob` para restaurarla. Ejemplo de entrada de la CLI:

```
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
```

Delete

El siguiente comando de la CLI de ejemplo, `DeleteBackupVault`, se puede utilizar para eliminar un almacén. Un almacén solo se puede eliminar si no hay copias de seguridad (puntos de recuperación) en él.

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

Otras opciones de programación disponibles incluyen:

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

Creación de un almacén de copias de seguridad

Debe crear al menos un almacén antes de crear un plan de copia de seguridad o iniciar un trabajo de copia de seguridad.

La primera vez que utilice la AWS Backup consola en una Región de AWS, la consola creará automáticamente una bóveda predeterminada.

Sin embargo, si se utiliza AWS Backup a través del AWS CLI AWS SDK o AWS CloudFormation, no se crea un almacén predeterminado. Debe crear su propio almacén.

Permisos necesarios

Debe tener los siguientes permisos para crear un almacén de respaldo mediante 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": "*"
    }
  ]
}
```

Creación de un almacén de copias de seguridad (consola)

Para step-by-step obtener instrucciones sobre cómo crear un almacén de copias de seguridad mediante la AWS Backup consola, consulte Paso 3: cree un almacén de copias de seguridad la guía de introducción.

Creación de un almacén de copias de seguridad (mediante programación)

El siguiente AWS Command Line Interface comando crea una bóveda de respaldo:

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

También puede especificar las siguientes configuraciones para un almacén de copias de seguridad.

Nombre del almacén de copias de seguridad

Los nombres de los almacenes de copia de seguridad distinguen entre mayúsculas y minúsculas. Deben tener de 2 a 50 caracteres alfanuméricos, guiones o guiones bajos.

AWS KMS clave de cifrado

La clave AWS KMS de cifrado protege sus copias de seguridad en esta bóveda de copias de seguridad. De forma predeterminada, AWS Backup crea una clave de KMS con el alias `aws/backup` automáticamente. Puede elegir esa clave o cualquier otra clave de su cuenta (las claves de KMS entre cuentas se pueden usar mediante la CLI).

Puede crear una nueva clave de cifrado siguiendo el procedimiento Creating Keys de la Guía para desarrolladores de AWS Key Management Service .

Después de crear una bóveda de respaldo y configurar la clave de AWS KMS cifrado, ya no podrá editar la clave de esa bóveda de respaldo.

La clave de cifrado que se especifica en un AWS Backup almacén se aplica a las copias de seguridad de determinados tipos de recursos. Para obtener más información acerca del cifrado de copias de seguridad, consulte Cifrado de copias de seguridad en AWS Backup en la sección Seguridad. Las copias de seguridad de los demás tipos de recursos se realizan con la clave que se usa para cifrar el recurso de origen.

Etiquetas de almacén de copias de seguridad

Estas etiquetas están asociadas al almacén de copias de seguridad para ayudarle a organizar y realizar un seguimiento de sus almacenes de copias de seguridad.

Definición de políticas de acceso en los almacenes de copias de seguridad

Con él AWS Backup, puede asignar políticas a las bóvedas de respaldo y a los recursos que contienen. La asignación de políticas le permite hacer cosas como conceder acceso a los usuarios para crear planes de copia de seguridad y copias de seguridad bajo demanda, pero limitar su capacidad de eliminar puntos de recuperación una vez creados.

Para obtener información sobre el uso de políticas para conceder o restringir el acceso a recursos, consulte Políticas basadas en identidad y políticas basadas en recursos en la Guía del usuario de IAM. También puede controlar el acceso mediante etiquetas.

Puede utilizar las siguientes políticas de ejemplo como guía para limitar el acceso a los recursos cuando trabaje con AWS Backup almacenes. A diferencia de otras políticas basadas en la IAM, las políticas de AWS Backup acceso no admiten el uso de un comodín en la clave. `Action`

Para obtener una lista de nombres de recursos de Amazon (ARN) que puede utilizar para identificar puntos de recuperación para diferentes tipos de recursos, consulte AWS Backup ARN de recursos de los ARN de puntos de recuperación específicos de recursos.

Las políticas de acceso de Vault solo controlan el acceso de los usuarios a las API. AWS Backup También se puede acceder a algunos tipos de copia de seguridad, como instantáneas de Amazon Elastic Block Store (Amazon EBS) y Amazon Relational Database Service (Amazon RDS), mediante las API de esos servicios. Puede crear políticas de acceso independientes en IAM que controlan el acceso a esas API con el fin de controlar plenamente el acceso a esos tipos de copia de seguridad.

Independientemente de la política de acceso del AWS Backup almacén, se `backup:CopyIntoBackupVault` rechazará el acceso entre cuentas para cualquier acción distinta de la del recurso al que se hace referencia. Es decir, se AWS Backup rechazará cualquier otra solicitud de una cuenta que sea diferente de la cuenta del recurso al que se hace referencia.

Temas

- Denegación del acceso a un tipo de recurso en un almacén de copias de seguridad
- Denegación del acceso a un almacén de copias de seguridad
- Denegación del acceso para eliminar puntos de recuperación en un almacén de copias de seguridad

Denegación del acceso a un tipo de recurso en un almacén de copias de seguridad

Esta política deniega el acceso a las operaciones de API especificadas para todas las instantáneas de Amazon EBS de un almacén de copias de seguridad.

```
{
    "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/*"]
        }
    ]
}
```

Denegación del acceso a un almacén de copias de seguridad

Esta política deniega el acceso a las operaciones de API especificadas dirigidas a un almacén de copias de seguridad.

```
{
    "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"
        }
    ]
}
```

Denegación del acceso para eliminar puntos de recuperación en un almacén de copias de seguridad

El acceso a los almacenes y la capacidad de eliminar puntos de recuperación almacenados en ellos se determinará en función del acceso que conceda a los usuarios.

Siga estos pasos para crear una política de acceso basada en recursos en un almacén de copias de seguridad que impida la eliminación de todas las copias de seguridad del almacén.

Para crear una política de acceso basada en recursos en un almacén de copias de seguridad

1. Inicie sesión y abra la AWS Backup consola en https://console.aws.amazon.com/backup. AWS Management Console
2. En el panel de navegación de la izquierda, elija Backup vaults (Almacenes de copias de seguridad).
3. Elija un almacén de copias de seguridad en la lista.
4. En la sección Access policy (Política de acceso), pegue el siguiente ejemplo de JSON. Esta política impide que cualquier persona que no sea la entidad principal elimine un punto de recuperación en el almacén de copias de seguridad de destino.

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

Para permitir que las identidades de IAM de la lista utilicen su ARN, utilice la clave de condición global `aws:PrincipalArn` del siguiente ejemplo.

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

Para obtener información acerca de cómo obtener un ID único para una entidad de IAM, consulte Obtener el identificador único en la Guía del usuario de IAM.

Si desea limitar esto a tipos de recursos específicos, en lugar de `"Resource": "*"`, puede incluir explícitamente los tipos de puntos de recuperación que se van a denegar. Por ejemplo, para las instantáneas de Amazon EBS, cambie el tipo de recurso por lo siguiente.

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

5. Elija Asociar política.

AWS Backup Vault Lock

> **Note**
>
> AWS Backup Cohasset Associates ha evaluado el uso de Vault Lock en entornos sujetos a las normas SEC 17a-4, la CFTC y la FINRA. Para obtener más información sobre la relación de AWS Backup Vault Lock con estas normas, consulte la evaluación de conformidad de Cohasset Associates.

AWS Backup Vault Lock es una función opcional de las bóvedas de respaldo, que puede resultar útil para proporcionarle seguridad y control adicionales sobre las bóvedas de respaldo. Cuando hay un bloqueo activo en el modo de cumplimiento y finaliza el periodo de gracia, ni el cliente ni el propietario de la cuenta o los datos ni AWS pueden modificar ni eliminar la configuración del almacén. Cada almacén puede tener implementado un bloqueo de almacén.

AWS Backup garantiza que sus copias de seguridad estén disponibles para usted hasta que venzan sus períodos de retención. Si algún usuario (incluido el usuario root) intenta eliminar una copia de seguridad o cambiar las propiedades del ciclo de vida de un almacén bloqueado, AWS Backup denegará la operación.

- Los usuarios con permisos de IAM suficientes pueden eliminar el bloqueo de los almacenes bloqueadas en modo de gobernanza.
- Los almacenes bloqueadas en modo de gobernanza no se pueden eliminar una vez que el periodo de reflexión (“periodo de gracia”) venza. Durante el periodo de gracia, aún puede eliminar el bloqueo del almacén y cambiar la configuración del bloqueo.

Modos de bloqueo del almacén

Al crear un bloqueo de almacén, puede elegir entre dos modos: el modo de gobernanza o el modo de cumplimiento. El modo de gobernanza está diseñado para permitir que solo usuarios con suficientes privilegios de IAM administren el almacén. El modo de gobernanza ayuda a una organización a cumplir los requisitos de gobernanza, ya que garantiza que solo el personal designado pueda hacer cambios en un almacén de copias de seguridad. El modo de cumplimiento está pensado para almacenes de copias de seguridad en los que se espera que el almacén (y, por extensión, su contenido) no se vaya a eliminar ni modificar nunca hasta que se complete el periodo

de retención de datos. Una vez que un almacén en modo de cumplimiento esté bloqueado, es inmutable, lo que significa que el bloqueo no se puede eliminar.

Los usuarios que dispongan de los permisos de IAM adecuados pueden administrar o eliminar un almacén bloqueado en modo gobernanza.

Un bloqueo de almacén en modo de cumplimiento no puede ser modificado ni eliminado por ningún usuario ni por AWS. Un almacén bloqueado en modo de cumplimiento tiene un periodo de gracia que se establece antes de que se bloquee y pase a ser inmutable.

Ventajas del bloqueo de almacenes

AWS Backup Vault Lock ofrece varias ventajas, entre las que se incluyen las siguientes:

- Configuración de WORM (escritura única y lectura múltiple) para todas las copias de seguridad que almacene y cree en un almacén de copias de seguridad.
- Una capa de defensa adicional que protege las copias de seguridad (puntos de recuperación) de sus almacenes de copias de seguridad contra eliminaciones involuntarias o malintencionadas.
- Aplica los períodos de retención, lo que evita que los usuarios con privilegios (incluido el usuario Cuenta de AWS root) las eliminen anticipadamente y cumple con las políticas y los procedimientos de protección de datos de la organización.

Bloqueo de un almacén de copias de seguridad mediante la consola

Puede añadir un candado de bóveda a su AWS Backup bóveda mediante la consola Backup.

Para agregar un bloqueo de almacén a su almacén de copias de seguridad:

1. Inicie sesión en la AWS Management Console AWS Backup consola y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Almacenes de copia de seguridad. Haga clic en el enlace anidado debajo de Almacenes de copia de seguridad denominado Bloqueos de almacén.
3. En Cómo funcionan los bloqueos de almacén o Bloqueos de almacén, haga clic en + crear bloqueo de almacén.
4. En el panel Detalles del bloqueo de almacén, elija el almacén al que desea que se aplique el bloqueo.

5. En Modo de bloqueo de almacenes, elija el modo en el que desea bloquear su almacén. Para obtener más información sobre cómo elegir los modos, consulte Modos de bloqueo del almacén , que aparece antes en esta página.
6. Para el Periodo de retención, elija los periodos de retención mínimo y máximo (los periodos de retención son opcionales). Los nuevos trabajos de copia y copia de seguridad creados en el almacén darán un error si no se ajustan a los periodos de retención que haya establecido; estos periodos no se aplicarán a los puntos de recuperación que ya estén en el almacén.
7. Si ha elegido el modo de cumplimiento, aparecerá una sección denominada Fecha de inicio del bloqueo de almacén. Si ha elegido el modo de gobernanza, esto no se mostrará y podrá omitir este paso.

   En el modo de cumplimiento, un bloqueo de almacén tiene un periodo de reflexión desde su creación hasta que el almacén y su bloqueo se vuelven inmutables e incambiables. Usted elige la duración de este periodo (denominado periodo de gracia), aunque debe ser de al menos 3 días (72 horas).

   > **Important**
   >
   > Una vez transcurrido el periodo de gracia, el almacén y su bloqueo son inmutables. Ningún usuario ni AWS puede cambiarlo ni eliminarlo.

8. Cuando esté satisfecho con las opciones de configuración, haga clic en Crear bloqueo de almacén.
9. Para confirmar que desea crear este bloqueo en el modo elegido, escriba `confirm` en el cuadro de texto y, a continuación, marque la casilla para confirmar que la configuración es la deseada.

Si los pasos se han completado correctamente, aparecerá un banner en la parte superior de la consola que indica que el proceso se ha realizado correctamente.

Bloqueo de un almacén de copias de seguridad mediante programación

Para configurar AWS Backup Vault Lock, utilice la API`PutBackupVaultLockConfiguration`. Los parámetros que se incluyan dependerán del modo de bloqueo de almacén que desee utilizar. Si desea crear un bloqueo de almacén en modo de gobernanza, no incluya `ChangeableForDays`. Si incluye este parámetro, el bloqueo del almacén se creará en modo de cumplimiento.

Este es una CLI de ejemplo de creación de un bloqueo de almacén en modo de cumplimiento:

```
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
```

Este es una CLI de ejemplo de creación de un bloqueo de almacén en modo de gobernanza:

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

Puede configurar cuatro opciones.

1. **`BackupVaultName`**

   El nombre del almacén que se va a bloquear.
2. **`ChangeableForDays`** (se incluye solo para el modo de cumplimiento)

   Este parámetro indica AWS Backup que se cree el bloqueo del almacén en modo de conformidad. Omita este parámetro si desea crear el bloqueo en el modo de gobernanza.

   Este valor se expresa en días. Debe ser un número no inferior a 3 ni superior a 36 500; de lo contrario, se generará un error.

   Desde la creación de este bloqueo de almacén hasta el vencimiento de la fecha especificada, el bloqueo de almacén se puede quitar de la bóveda mediante `DeleteBackupVaultLockConfiguration`. Como alternativa, durante este tiempo, puede cambiar la configuración mediante `PutBackupVaultLockConfiguration`.

   A partir de la fecha especificada, determinada por este parámetro, el almacén de copias de seguridad será inmutable y no se podrá modificar ni eliminar.
3. **`MaxRetentionDays`** (opcional)

   Es un valor numérico expresado en días. Es el periodo máximo de retención durante el cual el almacén retiene sus puntos de recuperación.

   El periodo máximo de retención que elija debe estar en consonancia con las políticas de retención de datos de su organización. Si su organización exige que los datos se retengan durante un

periodo determinado, este valor se puede establecer en ese periodo (en días). Por ejemplo, es posible que sea necesario conservar los datos financieros o bancarios durante 7 años (aproximadamente 2557 días, según los años bisiestos).

Si no se especifica, AWS Backup Vault Lock no aplicará un período máximo de retención. Si se especifica, no se podrán realizar copias ni copias de seguridad en este almacén con periodos de retención del ciclo de vida superiores al periodo máximo de retención. Los puntos de recuperación ya guardados en el almacén antes de la creación del bloqueo no se ven afectados. El periodo de retención máximo más largo que puede especificar es de 36 500 días (aproximadamente 100 años).

4. **`MinRetentionDays`**(opcional; obligatorio para CloudFormation)

   Es un valor numérico expresado en días. Es el periodo mínimo de retención durante el cual el almacén retiene sus puntos de recuperación. Esta configuración debe ajustarse a la cantidad de tiempo que su organización está obligada a mantener los datos. Por ejemplo, si la normativa o las leyes exigen que los datos se conserven durante al menos siete años, el valor en días sería de aproximadamente 2557, según los años bisiestos.

   Si no se especifica, AWS Backup Vault Lock no aplicará un período mínimo de retención. Si se especifica, no se podrán realizar copias ni copias de seguridad en este almacén con periodos de retención del ciclo de vida inferiores al periodo mínimo de retención. Los puntos de recuperación que ya estaban guardados en la bóveda antes del bloqueo de la AWS Backup bóveda no se ven afectados. El periodo de retención mínimo más corto que puede especificar es de 1 día.

Revise la configuración de Vault Lock de una AWS Backup bóveda de respaldo

Puedes revisar los detalles de AWS Backup Vault Lock de una bóveda en cualquier momento llamando a `DescribeBackupVault` `ListBackupVaults` nuestras API.

Para determinar si ha aplicado un bloqueo de almacén a un almacén de copias de seguridad, llama a `DescribeBackupVault` y comprueba la propiedad `Locked`. Si`"Locked": true`, como en el ejemplo siguiente, ha aplicado AWS Backup Vault Lock a su almacén de respaldo.

```
{
    "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"
}
```

El resultado anterior confirma las opciones siguientes:

1. `Locked`es un booleano que indica si ha aplicado AWS Backup Vault Lock a esta bóveda de respaldo. `True`significa que AWS Backup Vault Lock provoca un error en las operaciones de eliminación o actualización de los puntos de recuperación almacenados en el almacén (independientemente de si aún se encuentra o no en el período de gracia de reflexión).
2. `LockDate` es la fecha y hora UTC en las que finaliza el periodo de gracia de reflexión. Pasado este tiempo, no podrá eliminar ni cambiar el bloqueo de este almacén. Utilice cualquier conversor de hora disponible al público para convertir esta cadena a su hora local.

Si `"Locked":false`, como en el ejemplo siguiente, no ha aplicado un bloqueo de almacén (o se ha eliminado uno anterior).

```
{
    "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
}
```

Eliminación del bloqueo del almacén durante el periodo de gracia (modo de cumplimiento)

Para eliminar el bloqueo del almacén durante el tiempo de gracia (es decir, después de bloquear el depósito pero antes del tuyo`LockDate`) mediante la AWS Backup consola,

1. Inicia sesión en la AWS Management Console AWS Backup consola y ábrela en https://console.aws.amazon.com/backup.
2. En el menú de navegación de la izquierda, en Mi cuenta, haga clic en Almacenes de copia de seguridad y, a continuación, en Bloqueo de almacén de copias de seguridad.
3. Haga clic en el bloqueo del almacén que desee eliminar y, a continuación, en Administrar el bloqueo de almacén.
4. Haga clic en Eliminar el bloqueo de almacén.
5. Aparecerá un cuadro de advertencia en el que se le pedirá que confirme su intención de eliminar el bloqueo del almacén. Escriba `confirm` en el cuadro de texto y, a continuación, haga clic en confirmar.

Cuando todos los pasos se hayan completado correctamente, aparecerá un banner en la parte superior de la pantalla de la consola que indica que el proceso se ha realizado correctamente.

Para eliminar el bloqueo del almacén durante el periodo de gracia mediante un comando de la CLI, utilice `DeleteBackupVaultLockConfiguration` como en este ejemplo de CLI:

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

Cuenta de AWS cierre con una bóveda cerrada

Cuando cierras una Cuenta de AWS que contiene una bóveda de copias de seguridad AWS y AWS Backup suspendes tu cuenta durante 90 días con las copias de seguridad intactas. Si no vuelves a abrir tu cuenta durante esos 90 días, AWS borra el contenido del almacén de copias de seguridad, incluso si AWS Backup Vault Lock estaba activado.

Consideraciones adicionales de seguridad

AWS Backup Vault Lock añade un nivel adicional de seguridad a tu defensa en profundidad en materia de protección de datos. El bloqueo de almacenes se puede combinar con estas otras características de seguridad:

- Cifrado de sus puntos de recuperación
- AWS Backup políticas de acceso a almacenes y puntos de recuperación, que permiten conceder o denegar permisos a nivel de almacén,
- AWS Backup las mejores prácticas de seguridad, incluida su biblioteca de políticas administradas por el cliente que le permiten conceder o denegar permisos de copia de seguridad y restauración mediante un servicio AWS compatible, y
- AWS Backup Audit Manager, que le permite automatizar las comprobaciones de conformidad de sus copias de seguridad comparándolas con una lista de controles que usted defina.

  Puede trabajar a través de Crear marcos mediante la AWS Backup API para Las copias de seguridad están protegidas por AWS Backup Vault Lock de control con AWS Backup Audit Manager para asegurarse de que los recursos deseados estén protegidos con un bloqueo de almacén.
- Los mecanismos que inactivan los recursos pueden afectar a la capacidad de restaurarlos. Si bien todavía no se pueden eliminar en una bóveda cerrada, pueden estar en un estado distinto al activo. Por ejemplo, la configuración de Amazon Elastic Compute Cloud que permite deshabilitar una AMI puede bloquear temporalmente la capacidad de restaurar las copias de seguridad de las instancias de EC2. Esto afecta a todos los puntos de recuperación de EC2, incluso a las copias de seguridad afectadas por un bloqueo del almacén o una retención legal.

  Si una copia de seguridad de EC2 está deshabilitada, puede volver a activar una AMI deshabilitada. Una vez que se vuelva a activar, podrá restaurarse. Para bloquear la función de desactivación de la AMI, puede utilizar las políticas de IAM para no `ec2:DisableImage` permitirla.

> **Note**
>
> AWS Backup Vault Lock no es la misma función que Amazon S3 Glacier Vault Lock, que solo es compatible con S3 Glacier.

Eliminación de un almacén de copias de seguridad

Para evitar la eliminación masiva accidental o malintencionada, solo puede eliminar un almacén de copias de seguridad en AWS Backup después de eliminar (o de que su plan de copia de seguridad complete el ciclo de vida) todos los puntos de recuperación del almacén de copias de seguridad. Para eliminar tus puntos de recuperación manualmente, consulta Limpiar recursos.

Cuando se elimina un almacén de copias de seguridad, actualice los planes de copias de seguridad para que apunten a nuevos almacenes de copias de seguridad. Un plan de copias de seguridad que apunte a un almacén de copias de seguridad eliminado provocará un error en la creación de la copia de seguridad.

> **Note**
>
> No puede eliminar dos almacenes de copias de seguridad: el almacén de copias de seguridad AWS Backup predeterminado y el almacén de copias de seguridad automáticas Amazon EFS.

Para eliminar un almacén de copias de seguridad mediante la consola AWS Backup

1. Inicie sesión en la AWS Management Console AWS Backup consola y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Elija el nombre del almacén de copias de seguridad para abrir su página de detalles.
4. Elija y elimine todas las copias de seguridad que estén asociadas al almacén de copias de seguridad.
5. Seleccione Eliminar almacén. Cuando se le pida confirmación, introduzca el nombre del almacén y, a continuación, seleccione Eliminar almacén de Backup.

Trabajo con copias de seguridad

Una copia de seguridad, o punto de recuperación, representa el contenido de un recurso, por ejemplo un volumen de Amazon Elastic Block Store (Amazon EBS) o una tabla de Amazon DynamoDB, en un momento específico. Punto de recuperación es un término que se refiere generalmente a las distintas copias de seguridad de los AWS servicios, como las instantáneas de Amazon EBS y las copias de seguridad de DynamoDB. Los términos punto de recuperación y copia de seguridad se utilizan indistintamente.

AWS Backup guarda los puntos de recuperación en bóvedas de respaldo, que puede organizar de acuerdo con las necesidades de su empresa. Por ejemplo, puede guardar un conjunto de recursos que contengan información financiera para el ejercicio de 2020. Cuando necesite recuperar un recurso, puede utilizar la AWS Backup consola o el AWS Command Line Interface (AWS CLI) para buscar y recuperar el recurso que necesita.

Cada punto de recuperación tiene un identificador único. El identificador único se encuentra al final del nombre de recurso de Amazon (ARN) del punto de recuperación. Para ver ejemplos de los ARN y los ID únicos de los puntos de recuperación, consulte la tabla en Recursos y operaciones.

> **Important**
>
> Para evitar cargos adicionales, configure su política de retención con una duración de almacenamiento en caliente de al menos una semana. Para obtener más información, consulte Medición, costos y facturación.

Las siguientes secciones proporcionan información general acerca de las tareas de administración básicas de copia de seguridad en AWS Backup.

Temas

- Creación de una copia de seguridad
- Copia de una copia de seguridad
- Eliminación de copias de seguridad
- Edición de una copia de seguridad
- Restauración de una copia de seguridad
- Pruebas de restauración

- Visualización de una lista de copias de seguridad

Creación de una copia de seguridad

Con él AWS Backup, puede crear copias de seguridad automáticamente mediante planes de copia de seguridad o manualmente iniciando una copia de seguridad bajo demanda.

Creación de copias de seguridad automáticas

Cuando se crean copias de seguridad automáticamente mediante planes de copias de seguridad, se configuran con la configuración del ciclo de vida que se define en el plan de copias de seguridad. Están organizadas en el almacén de copias de seguridad especificado en el plan de copia de seguridad. Además, a estas copias de seguridad se les asignarán las etiquetas que se indiquen en el plan. Para obtener más información sobre los planes de copia de seguridad, consulte Administración de copias de seguridad mediante planes de copia de seguridad.

Creación de copias de seguridad bajo demanda

Al crear una copia de seguridad bajo demanda, puede configurar esta configuración para la copia de seguridad que se está creando. Cuando se crea una copia de seguridad de forma automática o manual, se inicia un trabajo de copia de seguridad. Para obtener información sobre cómo crear una copia de seguridad bajo demanda, consulte Creación de una copia de seguridad bajo demanda mediante AWS Backup.

Nota: Una copia de seguridad bajo demanda crea un trabajo de copia de seguridad; el trabajo de copia de seguridad cambiará al estado `Running` en el plazo de una hora (o cuando se especifique). Puede elegir una copia de seguridad bajo demanda si desea crear una copia de seguridad en un momento distinto del momento programado definido en un plan de copia de seguridad. Una copia de seguridad bajo demanda se puede utilizar, por ejemplo, para probar la copia de seguridad y su funcionalidad en cualquier momento.

Las copias de seguridad bajo demanda no se pueden utilizar con la point-in-time restauración (PITR), ya que una copia de seguridad bajo demanda conserva los recursos en el estado en que se encontraban cuando se realiza la copia de seguridad, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un período de tiempo.

Estados de los trabajos de copia de seguridad

Cada trabajo de copia de seguridad tiene un ID único. Por ejemplo, `D48D8717-0C9D-72DF-1F56-14E703BF2345`.

Puede ver el estado de un trabajo de copia de seguridad en la página Jobs (Trabajos) de la consola de AWS Backup . Los estados de las tareas de Backup incluyen `CREATED` `PENDING` `RUNNINGABORTING`,`ABORTED`,,`COMPLETED`, `FAILEDEXPIRED`, y`PARTIAL`.

Funcionamiento de las copias de seguridad incrementales

Muchos recursos admiten el respaldo incremental con AWS Backup. Encontrará una lista completa en la sección de copias de seguridad incrementales de la tabla Disponibilidad de características por recurso.

Si bien cada copia de seguridad posterior a la primera es incremental (lo que significa que solo captura los cambios de la copia de seguridad anterior), todas las copias de seguridad realizadas con ellas AWS Backup conservan los datos de referencia necesarios para permitir una restauración completa. Esto es así incluso si la copia de seguridad original (completa) ha llegado al final de su ciclo de vida y se ha eliminado.

Por ejemplo, si la copia de seguridad (completa) del día 1 se eliminó debido a una política de ciclo de vida de 3 días, aún podrá realizar una restauración completa con las copias de seguridad de los días 2 y 3. AWS Backup mantiene los datos de referencia necesarios desde el primer día para hacerlo.

Acceso a los recursos de origen

AWS Backup necesita acceder a los recursos de origen para realizar copias de seguridad de los mismos. Por ejemplo:

- Para hacer una copia de seguridad de una instancia de Amazon EC2, la instancia puede estar en el estado `running` o `stopped`, pero no en el estado `terminated`. Esto se debe a que una `stopped` instancia `running` o se puede comunicar con AWS Backup ella, pero una `terminated` instancia no.
- Para hacer una copia de seguridad de una máquina virtual, su hipervisor debe tener el estado de puerta de enlace de copia de seguridad `ONLINE`. Para obtener más información, consulte Descripción del estado del hipervisor.

- Para hacer una copia de seguridad de una base de datos de Amazon RDS, Amazon Aurora o un clúster de Amazon DocumentDB, esos recursos deben tener el estado `AVAILABLE`.
- Para hacer una copia de seguridad de un Amazon Elastic File System (Amazon EFS), debe tener el estado `AVAILABLE`.
- Para hacer una copia de seguridad de un sistema de archivos de Amazon FSx, debe tener el estado `AVAILABLE`. Si el estado es `UPDATING`, la solicitud de copia de seguridad queda en cola hasta que el sistema de archivos pase a estar `AVAILABLE`.

  FSx para ONTAP no es compatible con copias de seguridad de determinados tipos de volúmenes, incluidos los volúmenes de DP (protección de datos), los volúmenes de LS (carga compartida), los volúmenes completos o los volúmenes de sistemas de archivos que están llenos. Para obtener más información, consulte FSx for ONTAP Working with backups.

AWS Backup conserva las copias de seguridad creadas anteriormente de acuerdo con su política de ciclo de vida, independientemente del estado del recurso de origen.

Temas

Creación de una copia de seguridad bajo demanda mediante AWS Backup

En la AWS Backup consola, la página de recursos protegidos muestra los recursos de los que se ha hecho una copia de seguridad al AWS Backup menos una vez. Si lo utiliza AWS Backup por primera vez, no hay ningún recurso (como volúmenes de Amazon EBS o bases de datos de Amazon RDS) en esta página. No aparecerán aunque haya asignado un recurso a un plan de copias de seguridad si dicho plan no ha ejecutado un trabajo de copia de seguridad programado al menos una vez.

Nota: Una copia de seguridad bajo demanda comienza a hacer copias de seguridad de su recurso de forma inmediata. Puede elegir una copia de seguridad bajo demanda si desea crear una copia de seguridad en un momento distinto del momento programado definido en un plan de copia de seguridad. Una copia de seguridad bajo demanda se puede utilizar, por ejemplo, para probar la copia de seguridad y su funcionalidad en cualquier momento.

Las copias de seguridad bajo demanda no se pueden utilizar con la point-in-time restauración (PITR), ya que una copia de seguridad bajo demanda conserva los recursos en el estado en que se encontraban cuando se realiza la copia de seguridad, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un período de tiempo.

Consideraciones

- Si el rol AWS Backup predeterminado no está presente en tu cuenta, se crea uno para ti con los permisos correctos.
- Cuando las copias de seguridad venzan y estén marcadas para su eliminación como parte de su política de ciclo de vida, AWS Backup las eliminará en un momento elegido al azar durante las 8 horas siguientes. Este intervalo ayuda a garantizar un rendimiento uniforme.
- En el caso de los recursos de Amazon EC2, copia AWS Backup automáticamente las etiquetas de recursos individuales y grupales existentes, además de las etiquetas que añada en este paso.
- AWS Backup realiza copias de seguridad de EC2 con el comportamiento predeterminado de «no reiniciar». AWS Backup actualmente admite recursos que se ejecutan en Amazon EC2 y algunos tipos de instancias no son compatibles. Para obtener más información, consulte Creación de copias de seguridad de Windows VSS.

Para crear una copia de seguridad bajo demanda

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.

2. En el panel, elija Create an on-demand backup (Crear una copia de seguridad bajo demanda). O bien, en el panel de navegación, elija Protected resources (Recursos protegidos) y, a continuación, Create an on-demand backup (Crear una copia de seguridad bajo demanda).
3. En la página de tipos de recursos, elija el tipo de recurso del que desee hacer una copia de seguridad. Por ejemplo, elija DynamoDB para las tablas de Amazon DynamoDB.
4. Elija el nombre o el ID del recurso que desee proteger. Por ejemplo, elija el nombre de la tabla de DynamoDB para Amazon DynamoDB.
5. Asegúrese de que la opción Create backup now (Crear copia de seguridad ahora) esté seleccionada.
6. Si el tipo de recurso admite la transición al almacenamiento en frío, el almacenamiento en frío está presente. Para obtener más información, consulte la columna Del ciclo de vida al almacenamiento en frío de la tabla Disponibilidad de funciones por recurso.

   Para especificar cuándo se almacenará esta copia de seguridad en frío, seleccione Mover las copias de seguridad del almacenamiento en caliente al almacenamiento en frío y, a continuación, especifique el tiempo de almacenamiento en frío.
7. En Período de retención total, especifique el número de días. Si especificó el tiempo de almacenamiento en frío, el período de retención se divide entre almacenamiento en frío y en caliente.
8. Elija un almacén de copias de seguridad existente o cree uno nuevo. Al elegir Create new Backup vault (Crear nuevo almacén de copias de seguridad), se abre una nueva página para crear un almacén y, a continuación, vuelve a la página Create on-demand backup (Crear copia de seguridad bajo demanda) cuando termine.
9. Para el rol de IAM, elija el rol predeterminado o uno que haya creado.
10. Para asignar una etiqueta a la copia de seguridad bajo demanda, expanda las etiquetas añadidas a los puntos de recuperación, seleccione Añadir nueva etiqueta e introduzca una clave de etiqueta y un valor de etiqueta.
11. Si el tipo de recurso es EC2, aparece la configuración de copia de seguridad avanzada. Para realizar instantáneas coherentes con las aplicaciones mediante Windows Volume Shadow Copy Service (VSS), elija Windows VSS.
12. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). Esto abre la página de trabajos, donde puede ver una lista de trabajos y ver su estado.

Copias de seguridad y point-in-time restauración continuas (PITR)

Temas

En el caso de algunos recursos, AWS Backup admite copias de seguridad y point-in-time recuperación continuas (PITR) además de copias de seguridad instantáneas.

Con las copias de seguridad continuas, puede restaurar el recurso AWS Backup compatible retrocediéndolo hasta el momento específico que elija, con un tiempo de precisión de 1 segundo (retrocediendo un máximo de 35 días). La copia de seguridad continua consiste en crear primero una copia de seguridad completa del recurso y, a continuación, realizar copias de seguridad constantes de los registros de transacciones del recurso. La restauración PITR funciona accediendo a la copia de seguridad completa y reproduciendo el registro de transacciones hasta el momento indicado para la recuperación. AWS Backup

Como alternativa, se pueden realizar copias de seguridad instantáneas con una frecuencia de hasta una hora. Las copias de seguridad de instantáneas se pueden almacenar hasta un máximo de 100 años. Las instantáneas se pueden copiar para realizar copias de seguridad completas o incrementales.

Dado que las copias de seguridad continuas y las instantáneas ofrecen diferentes ventajas, le recomendamos que proteja sus recursos con reglas de copia de seguridad continuas e instantáneas.

Nota: Una copia de seguridad bajo demanda comienza a hacer copias de seguridad de su recurso de forma inmediata. Puede elegir una copia de seguridad bajo demanda si desea crear una copia de seguridad en un momento distinto del momento programado definido en un plan de copia de

seguridad. Una copia de seguridad bajo demanda se puede utilizar, por ejemplo, para probar la copia de seguridad y su funcionalidad en cualquier momento.

Las copias de seguridad bajo demanda no se pueden utilizar con la point-in-time restauración (PITR), ya que una copia de seguridad bajo demanda conserva los recursos en el estado en que se encontraban cuando se realiza la copia de seguridad, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un período de tiempo.

Puede optar por realizar copias de seguridad continuas para los recursos compatibles al crear un plan de copias de seguridad AWS Backup mediante la AWS Backup consola o la API.

Para habilitar las copias de seguridad continuas desde la consola

1. Inicie sesión y abra la AWS Backup consola en https://console.aws.amazon.com/backup. AWS Management Console
2. En el panel de navegación principal, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En Reglas de copia de seguridad, elija Agregar regla de copia de seguridad.
4. En la sección Configuración de regla de copia de seguridad, seleccione Habilitar copias de seguridad continuas para los recursos compatibles.

Servicios compatibles para la copia de seguridad continua o la restauración puntual (PITR)

AWS Backup admite copias de seguridad y point-in-time recuperación continuas para los siguientes servicios y aplicaciones:

Amazon S3

Para activar la PITR en las copias de seguridad de S3, las copias de seguridad continuas deben formar parte del plan de copia de seguridad.

Si bien esta copia de seguridad original del bucket de origen puede tener la PITR activa, las copias de destino entre regiones o entre cuentas no tendrán PITR, y la restauración a partir de estas copias será en el momento en el que se crearon (las copias serán copias de instantáneas) en lugar de restaurarse en un momento específico.

RDS

Programaciones de backup: cuando un AWS Backup plan cree tanto instantáneas de Amazon RDS como copias de seguridad continuas, AWS Backup programará de forma inteligente las ventanas de backup para coordinarlas con la ventana de mantenimiento de Amazon RDS y evitar conflictos. Para evitar aún más conflictos, la configuración manual de la ventana de copias de seguridad automatizadas de Amazon RDS no está disponible. RDS toma instantáneas una vez al día, independientemente de si un plan de copia de seguridad tiene una frecuencia de copias de seguridad de instantáneas distinta de una vez al día.

Configuración: después de aplicar una regla de copia de seguridad AWS Backup continua a una instancia de Amazon RDS, no puede crear ni modificar la configuración de copia de seguridad continua de esa instancia en Amazon RDS; las modificaciones deben realizarse a través de la AWS Backup consola o la CLI AWS Backup .

Transición del control del backup continuo de una instancia de Amazon RDS a Amazon RDS:

Console

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, seleccione Backup plans (Planes de copias de seguridad).
3. Elimine todos los planes de copia de seguridad de Amazon RDS con una copia de seguridad continua que proteja ese recurso.
4. Elija Almacenes de Backup. Elimine el punto de recuperación de la copia de seguridad continua de su almacén de copias de seguridad. O bien, espere a que transcurra su período de retención, lo que provocará AWS Backup que se elimine automáticamente el punto de recuperación.

   Después de completar estos pasos, AWS Backup transferirá el control de respaldo continuo de su recurso a Amazon RDS.

AWS CLI

Llame a la operación de la API `DisassociateRecoveryPoint`.

Para obtener más información, consulte DisassociateRecoveryPoint.

Permisos de IAM requeridos para las copias de seguridad continuas de Amazon RDS

- AWS Backup Para configurar copias de seguridad continuas para su base de datos de Amazon RDS, compruebe que el permiso de API `rds:ModifyDBInstance` existe en la función de IAM definida en la configuración del plan de copias de seguridad. Para restaurar las copias de seguridad continuas de Amazon RDS, debe agregar el permiso `rds:RestoreDBInstanceToPointInTime` al rol de IAM que envió para el trabajo de restauración. Puede utilizar `AWS Backup default service role` para realizar copias de seguridad y restauraciones.
- Para describir el rango de tiempos disponibles para la point-in-time recuperación, AWS Backup llame. `rds:DescribeDBInstanceAutomatedBackupsAPI` En la AWS Backup consola, debes tener el permiso de `rds:DescribeDBInstanceAutomatedBackups` API en tu política gestionada AWS Identity and Access Management (IAM). Puede utilizar las políticas administradas `AWSBackupOperatorAccess` o `AWSBackupFullAccess`. Ambas políticas tienen todos los permisos necesarios. Para obtener más información, consulte Políticas administradas de .

Períodos de retención: cuando cambias el período de retención del PITR, AWS Backup se aplica ese cambio de forma inmediata. `ModifyDBInstance` Si tiene otras actualizaciones de configuración pendientes durante el siguiente periodo de mantenimiento, al cambiar el periodo de retención de PITR, esas actualizaciones de configuración también se aplicarán inmediatamente. Para obtener más información, consulte `ModifyDBInstance` en la Referencia de la API de Amazon Relational Database Service .

Copias de copias de seguridad continuas de Amazon RDS:

- Los trabajos de copia de instantáneas incrementales se procesan más rápido que los trabajos de copia de instantáneas completas. Si se mantiene una copia de instantánea anterior hasta que se complete el nuevo trabajo de copia se puede reducir la duración del trabajo de copia. Si decide copiar las instantáneas de las instancias de la base de datos de RDS, es importante tener en cuenta que si elimina primero las copias anteriores, se realizarán copias de instantáneas completas (en lugar de incrementales). Para obtener más información sobre cómo optimizar la copia, consulte Copias de instantáneas incrementales en la Guía del usuario de Amazon RDS.
- Creación de copias de seguridad continuas de Amazon RDS: no puede crear copias de las copias de seguridad continuas de Amazon RDS porque AWS Backup Amazon RDS no permite copiar los registros de transacciones. En su lugar, AWS Backup crea una instantánea y la copia con la frecuencia especificada en el plan de copias de seguridad.

Restauraciones: puede realizar una point-in-time restauración con Amazon RDS AWS Backup o con Amazon RDS. Para obtener instrucciones sobre AWS Backup la consola, consulte Restauración de una base de datos de Amazon RDS. Para obtener instrucciones sobre Amazon RDS, consulte Restauración de una instancia de base de datos a un momento especificado en la Guía del usuario de Amazon RDS.

> **Tip**
>
> Una instancia de base de datos con varias zonas de disponibilidad (AZ) establecida en no `Always On` debería tener la retención de copias de seguridad establecida en cero. Si se producen errores, utilice el AWS CLI comando `disassociate-recovery-point` en lugar de y`delete-recovery-point`, a continuación, cambie la configuración de retención a 1 en la configuración de Amazon RDS.

Para obtener información general sobre el uso de Amazon RDS, consulte la Guía del usuario De Amazon RDS.

Aurora

Para habilitar la copia de seguridad continua de sus recursos de Aurora, consulte los pasos de la primera sección de esta página.

El procedimiento para restaurar un clúster de Aurora a un momento dado es una variación de los pasos para restaurar una instantánea de un clúster de Aurora.

Al realizar una restauración en un momento dado, la consola muestra una sección de hora de restauración. Consulte Restauración a partir de una copia de seguridad continua más abajo en esta página, en Uso de copias de seguridad continuas.

SAP HANA en instancias de Amazon EC2

Puede realizar copias de seguridad continuas, que se pueden utilizar con la point-in-time restauración (PITR) (tenga en cuenta que las copias de seguridad bajo demanda conservan los recursos en el estado en que se utilizan, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un período de tiempo).

Con las copias de seguridad continuas, puede restaurar su base de datos de SAP HANA en una instancia EC2 devolviéndola al momento específico que elija, con una precisión de 1 segundo

(retrocediendo un máximo de 35 días). La copia de seguridad continua consiste en crear primero una copia de seguridad completa del recurso y, a continuación, realizar copias de seguridad constantes de los registros de transacciones del recurso. La restauración mediante PITR funciona accediendo a la copia de seguridad completa y reproduciendo el registro de transacciones hasta el momento indicado para su recuperación. AWS Backup

Puede optar por realizar copias de seguridad continuas al crear un plan de copias de seguridad AWS Backup mediante la AWS Backup consola o la API.

Para habilitar las copias de seguridad continuas desde la consola

1. Inicie sesión en la AWS Management Console AWS Backup consola y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación principal, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En Reglas de copia de seguridad, elija Agregar regla de copia de seguridad.
4. En la sección Configuración de regla de copia de seguridad, seleccione Habilitar copias de seguridad continuas para los recursos compatibles.

Tras deshabilitar el PITR (point-in-timerestauración) para las copias de seguridad de las bases de datos de SAP HANA, se seguirán enviando los registros AWS Backup hasta que caduque el punto de recuperación (el estado es igual a`EXPIRED`). Puede cambiar a una ubicación alternativa de copia de seguridad de registros en SAP HANA para detener la transmisión de registros a AWS Backup.

Un punto de recuperación continuo con un estado igual a `STOPPED` indica que se ha interrumpido un punto de recuperación continuo; es decir, los registros transmitidos desde SAP HANA a AWS Backup ese punto muestran los cambios incrementales en una base de datos que presentan un vacío. Los puntos de recuperación que se producen dentro de este lapso de tiempo tienen un estado de `STOPPED`..

Para ver los problemas que pueden surgir durante los trabajos de restauración de copias de seguridad continuas (puntos de recuperación), consulte la sección de solución Solución de problemas de restauración de SAP HANA de esta guía.

Búsqueda de una copia de seguridad continua

Puede utilizar la AWS Backup consola para buscar su copia de seguridad continua.

Para buscar una copia de seguridad continua mediante la AWS Backup consola

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Almacenes de copia de seguridad y, a continuación, elija el almacén de copias de seguridad de la lista.
3. En la sección Copias de seguridad, orden la columna Tipo de copia de seguridad según los puntos de recuperación Continuos. También puede ordenar según el ID de punto de recuperación para el prefijo continuo.

Restauración de una copia de seguridad continua

Para restaurar una copia de seguridad continua mediante la AWS Backup consola

- Durante el proceso de restauración del PITR, la AWS Backup consola muestra una sección de tiempo de restauración. En esta sección, realice una de las siguientes acciones:
  - Elija restaurar a la Última hora restaurable.
  - Elija Especificar fecha y hora para introducir su propia fecha y hora dentro del periodo de retención.

Para restaurar una copia de seguridad continua mediante la API AWS Backup

1. Para Amazon S3, consulte Usar la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de S3.
2. Para Amazon RDS, consulte Utilizar la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon RDS.

Detención o eliminación de copias de seguridad continuas

Puede detener la creación de copias de seguridad continuas o eliminar copias de seguridad específicas (point-in-time-recovery o puntos PITR).

Si desea detener las copias de seguridad continuas, debe eliminar la regla de la copia de seguridad continua de su plan de copia de seguridad. Si desea detener las copias de seguridad continuas para uno o más recursos, pero no para todos los recursos, cree un nuevo plan de copia de seguridad con la regla de la copia de seguridad continua para los recursos de los que aún desee realizar copias de seguridad continuas. Si, por el contrario, solo elimina un punto de recuperación de la copia de

seguridad continua de su almacén de copias de seguridad, el plan de copia de seguridad seguirá ejecutando la regla de la copia de seguridad continua y se creará un nuevo punto de recuperación.

Sin embargo, incluso después de eliminar la regla de copia de seguridad continua, AWS Backup recuerda el período de retención de la regla de copia de seguridad ahora eliminada. Eliminará automáticamente el punto de recuperación de la copia de seguridad continua del almacén de copias de seguridad en función del periodo de retención especificado.

Al eliminar los puntos de recuperación de Amazon RDS, tenga en cuenta lo siguiente:

- Una instancia de base de datos con varias zonas de disponibilidad (AZ) establecida en no `Always 0`n debería tener la retención de copias de seguridad establecida en cero. Si se producen errores, utilice el AWS CLI comando `disassociate-recovery-point` en lugar de y`delete-recovery-point`, a continuación, cambie la configuración de retención a 1 en la configuración de Amazon RDS.
- Cuando se elimina un punto de point-in-time recuperación (una copia de seguridad creada mediante una copia de seguridad continua) de Amazon RDS, se desencadena el reinicio de la base de datos y se deshabilitan los registros binarios. Para obtener más información, consulte Periodo de retención de copia de seguridad en la Guía del usuario de Amazon RDS.

Al eliminar los puntos de recuperación de Aurora, tenga en cuenta lo siguiente:

Si se selecciona para un punto de recuperación de Amazon Aurora, AWS Backup establece el período de retención en 1 día. Las copias de seguridad de Aurora no se pueden eliminar por completo hasta que también se haya eliminado el clúster de origen.

Copiado de copias de seguridad continuas

Si una regla de copia de seguridad continua también especifica una copia entre cuentas o regiones, AWS Backup toma una instantánea de la copia de seguridad continua y la copia en el almacén de destino. Para obtener más información sobre cómo copiar sus puntos de recuperación entre cuentas y regiones, consulte Copia de una copia de seguridad.

Las copias de seguridad continuas crean copias de seguridad periódicas de acuerdo con la frecuencia establecida en la regla del plan de copias de seguridad en la cuenta o región de destino.

AWS Backup no admite copias bajo demanda de copias de seguridad continuas.

Cambio del periodo de retención

Puede utilizarla AWS Backup para aumentar o reducir el período de retención de su regla de copia de seguridad continua existente. El periodo mínimo de retención es de 1 día. El periodo máximo de retención es de 35 días.

Si aumenta el periodo de retención, el efecto es inmediato. Si reduce el período de retención, AWS Backup esperará hasta que pase suficiente tiempo antes de aplicar el cambio para protegerse contra la pérdida de datos. Por ejemplo, si reduce el período de retención de 35 a 20 días, AWS Backup seguirá conservando 35 días de copia de seguridad continua hasta que hayan transcurrido 15 días. Este diseño protege las copias de seguridad de los últimos 15 días en el momento en que se realizó el cambio.

Eliminación de la única regla de copia de seguridad continua de un plan de copia de seguridad

Al crear un plan de copia de seguridad con una regla de copia de seguridad continua y, a continuación, eliminar esa regla, AWS Backup recuerda el período de retención de la regla que ya se ha eliminado. Eliminará la copia de seguridad continua de su almacén de copias de seguridad cuando haya transcurrido el periodo de retención.

Copias de seguridad continuas superpuestas en el mismo recurso

En general, no debe utilizar más de una regla de copia de seguridad continua para proteger cada recurso. Esto se debe a que las copias de seguridad continuas adicionales son redundantes. Sin embargo, a medida que amplía su espacio de copias de seguridad, es posible que varios planes, reglas y almacenes de copias de seguridad se superpongan en un solo recurso. AWS Backup gestiona estas superposiciones de la siguiente manera.

Si incluye el mismo recurso en más de un plan de respaldo con una regla de respaldo continuo, solo AWS Backup se creará un respaldo continuo para el primer plan de respaldo que evalúe. Creará copias de seguridad instantáneas para todos los demás planes de copia de seguridad.

Si incluye varias reglas de copia de seguridad continua en un solo plan de copia de seguridad:

- Si sus reglas apuntan al mismo almacén de copias de seguridad, AWS Backup solo crea una copia de seguridad continua para la regla con el período de retención más largo. Hace caso omiso de todas las demás reglas.
- Si sus reglas apuntan a almacenes de respaldo diferentes, AWS Backup rechaza el plan por no ser válido.

Consideraciones sobre la recuperación oint-in-time

Tenga en cuenta las siguientes consideraciones para la point-in-time recuperación:

- Recuperación automática a instantáneas: si AWS Backup no puede realizar una copia de seguridad continua, intenta realizar una copia de seguridad instantánea en su lugar.
- No admite copias de seguridad continuas a pedido: AWS Backup no admite las copias de seguridad continuas a pedido, ya que las copias de seguridad a pedido registran un punto en el tiempo, mientras que las copias de seguridad continuas registran los cambios a lo largo de un período de tiempo.
- No admite la transferencia al almacenamiento en frío: las copias de seguridad continuas no admiten la transferencia al almacenamiento en frío porque la transferencia al almacenamiento en frío requiere un periodo de transferencia mínimo de 90 días, mientras que las copias de seguridad continuas tienen un periodo de retención máximo de 35 días.
- Restauración de la actividad reciente: la actividad de Amazon RDS permite restauraciones hasta los últimos 5 minutos de actividad; Amazon S3 permite restauraciones hasta los últimos 15 minutos de actividad.

Copias de seguridad de Amazon S3

AWS Backup admite la copia de seguridad y la restauración centralizadas de aplicaciones que almacenan datos en S3 por sí solas o junto con otros AWS servicios de bases de datos, almacenamiento y computación. Hay muchas características disponibles para las copias de seguridad de S3, incluido Backup Audit Manager.

Puede utilizar una única política de copias de seguridad AWS Backup para automatizar de forma centralizada la creación de copias de seguridad de los datos de sus aplicaciones. AWS Backup organiza automáticamente las copias de seguridad de diferentes AWS servicios y aplicaciones de terceros en una ubicación centralizada y cifrada (conocida como bóveda de copias de seguridad) para que pueda gestionar las copias de seguridad de toda la aplicación mediante una experiencia centralizada. En el caso de S3, puede crear copias de seguridad continuas y restaurar los datos de las aplicaciones almacenados en S3, así como restaurar las copias de seguridad a una point-in-time ubicación única con un solo clic.

Con él AWS Backup, puede crear los siguientes tipos de copias de seguridad de sus depósitos de S3, incluidos los datos de objetos, las etiquetas, las listas de control de acceso (ACL) y los metadatos definidos por el usuario:

- Las copias de seguridad continuas le permiten realizar una restauración a cualquier momento de los últimos 35 días. Las copias de seguridad continuas de un bucket de S3 solo deben configurarse en un plan de copia de seguridad.

  Consulte Recuperación en un momento dado para obtener una lista de los servicios compatibles e instrucciones sobre cómo utilizar AWS Backup para realizar copias de seguridad continuas.
- Las copias de seguridad periódicas utilizan instantáneas de sus datos para que pueda retenerlos durante un periodo especificado de hasta 99 años. Puede programar copias de seguridad periódicas en frecuencias de 1 hora, 12 horas, 1 día, 1 semana o 1 mes. AWS Backup realiza copias de seguridad periódicas durante el intervalo de copia de seguridad que defina en su plan de copia de seguridad.

  Consulte Crear un plan de respaldo para entender cómo AWS Backup se aplica el plan de respaldo a sus recursos.

Hay copias entre cuentas y regiones disponibles para las copias de seguridad de S3, pero las copias de las copias de seguridad continuas no tienen capacidades de point-in-time restauración.

Las copias de seguridad continuas y periódicas de los buckets de S3 deben residir en el mismo almacén de copias de seguridad.

Para ambos tipos de copia de seguridad, la primera es una copia de seguridad completa, mientras que las copias de seguridad posteriores son incrementales a nivel de objeto.

> **Note**
>
> Debe habilitar el control de versiones de S3 en su bucket de S3 AWS Backup para usarlo en Amazon S3. Se ha mantenido este requisito previo porque en AWS se aconseja el control de versiones en S3 como práctica recomendada para la protección de datos.
> Se recomienda establecer un periodo de vencimiento del ciclo de vida para sus versiones de S3. Si no se establece un período de caducidad del ciclo de vida, podría aumentar los costes de S3, ya que se AWS Backup realizan copias de seguridad y se almacenan todas las versiones no vencidas de los datos de S3. Para obtener más información sobre cómo configurar las políticas del ciclo de vida de S3, siga las instrucciones de esta página.

Comparación de tipos de copia de seguridad de S3

Su estrategia de copia de seguridad de los recursos de S3 puede incluir solo copias de seguridad continuas, solo copias de seguridad periódicas (instantáneas) o una combinación de ambas. La siguiente información puede ayudarle a elegir lo que mejor se adapte a su organización:

Solo copias de seguridad continuas:

- Una vez finalizada la primera copia de seguridad completa de los datos existentes, se realiza un seguimiento de los cambios en los datos del bucket de S3 a medida que se producen.
- Los cambios registrados le permiten utilizar el PITR (point-in-time restauración) durante el período de retención de la copia de seguridad continua. Para realizar un trabajo de restauración, elija el momento al que desee realizar la restauración.
- El periodo de retención de cada copia de seguridad continua es de un máximo de 35 días.

Solo copias de seguridad periódicas (instantáneas), programadas o bajo demanda:

- AWS Backup escanea todo el depósito de S3, recupera la ACL y las etiquetas de cada objeto e inicia una solicitud Head para cada objeto que estaba en la instantánea anterior pero que no se encontró en la instantánea que se está creando.
- La copia de seguridad es coherente point-in-time .
- La fecha y la hora de la copia de seguridad registradas son la hora en la que se AWS Backup completa el recorrido del depósito, no la hora en que se creó la tarea de copia de seguridad.
- La primera copia de seguridad de un bucket es una copia de seguridad completa. Cada copia de seguridad posterior es incremental y representa el cambio en los datos desde la última instantánea.
- La instantánea realizada por la copia de seguridad periódica puede tener un periodo de retención de hasta 99 años.

Copias de seguridad continuas combinadas con copias de seguridad periódicas o instantáneas:

- Una vez finalizada la primera copia de seguridad completa de los datos existentes (cada bucket), se realiza un seguimiento de los cambios en el bucket a medida que se producen.
- Puede realizar una point-in-time restauración desde un punto de recuperación continuo.
- Las instantáneas son point-in-time coherentes.

- Las instantáneas se toman directamente del punto de recuperación continuo, lo que elimina la necesidad de volver a escanear un bucket para facilitar procesos más rápidos.
- Las instantáneas y los puntos de recuperación continuos comparten un linaje de datos; el almacenamiento de datos entre puntos de recuperación continuos e instantáneas no se duplica.

Clases de almacenamiento de S3 compatibles

AWS Backup le permite hacer copias de seguridad de los datos de S3 almacenados en las siguientes clases de almacenamiento de S3:

- S3 Standard
- Estándar S3: acceso poco frecuente (IA)
- S3 One Zone-IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

Las copias de seguridad de un objeto de la clase de almacenamiento S3 Intelligent-Tiering (INT) acceden a esos objetos. Este acceso hace que S3 Intelligent-Tiering mueva automáticamente esos objetos a Frequent Access.

Las copias de seguridad que acceden a los niveles de acceso poco frecuente, incluidas las clases S3 Standard: Infrequently Access (IA) y S3 One Zone-IA, se transfieren al cargo de almacenamiento de S3 de acceso frecuente (se aplica a los niveles de acceso poco frecuente o Archive Instant Access).

Con la excepción de Glacier Instant Retrieval, no se admiten las clases de almacenamiento archivado.

Para obtener más información sobre los precios de almacenamiento de Amazon S3, consulte los precios de Amazon S3.

Consideraciones AWS Backup para Amazon S3

Tenga en cuenta lo siguiente cuando haga copias de seguridad de recursos de S3:

- Compatibilidad con metadatos de objetos específicos: AWS Backup admite los siguientes metadatos: etiquetas, listas de control de acceso (ACL), metadatos definidos por el usuario,

fecha de creación original e ID de versión. También puede restaurar todos los datos y metadatos de la copia de seguridad, excepto la fecha de creación original, el ID de la versión, la clase de almacenamiento y las etiquetas electrónicas.

- El nombre de clave de un objeto de S3 puede estar compuesto por la mayoría de las cadenas codificables en UTF-8. Se admiten los siguientes caracteres Unicode: `#x9` | `#xA` | `#xD` | `#x20 to #xD7FF` | `#xE000 to #xFFFD` | `#x10000 to #x10FFFF`.

  Los nombres de clave de objeto que incluyen caracteres que no figuran en esta lista podrían quedar excluidos de las copias de seguridad. Para obtener más información, consulte la especificación W3C respecto a los caracteres.
- Transición al almacenamiento en frío: AWS Backup la política de gestión del ciclo de vida de las copias de seguridad le permite definir el plazo de caducidad de las copias de seguridad, pero actualmente no se admite la transición al almacenamiento en frío de las copias de seguridad de S3.
- Por el momento, no se admiten copias de seguridad de buckets de S3 con varias versiones del mismo objeto que se crearon en el mismo segundo.
- En el caso de las copias de seguridad periódicas, AWS Backup hace todo lo posible por realizar un seguimiento de todos los cambios en los metadatos de los objetos. Sin embargo, si actualiza una etiqueta o una ACL varias veces en un minuto, es posible que AWS Backup no capture todos los estados intermedios.
- AWS Backup actualmente no ofrece soporte para copias de seguridad de objetos cifrados con SSE-C. AWS Backup tampoco admite actualmente copias de seguridad de las configuraciones de los buckets, incluidas las políticas, los ajustes, el nombre o el punto de acceso del bucket.
- AWS Backup actualmente no admite copias de seguridad de S3 en adelante AWS Outposts.

> **Important**
>
> En las cuentas que registran eventos de lectura de datos, los buckets de S3 con CloudTrail los registros activados necesitan que sus registros de acceso se guarden en un bucket de destino diferente; si CloudTrail los registros se guardan en el mismo bucket en el que se registran, se forma un bucle infinito. Este bucle puede provocar cargos inesperados y no deseados.
>
> Para obtener más información, consulte los eventos de datos en la Guía del CloudTrail usuario.

Intervalos de conclusión de la copia de seguridad de S3

La siguiente tabla muestra ejemplos de buckets de varios tamaños para ayudarle a estimar el tiempo de conclusión de la copia de seguridad completa inicial de un bucket de S3. Los tiempos de copias de seguridad variarán según el tamaño, el contenido, la configuración y los ajustes de cada bucket.

Tamaño del bucket	Número de objetos	Tiempo estimado para completar la copia de seguridad inicial
425 GB (gigabytes)	135 millones	31 horas
800 TB (terabytes)	670 millones	38 horas
6 PB (petabytes)	5000 millones	100 horas
370 TB (terabytes)	7500 millones	180 horas

Permisos y políticas para la copia de seguridad y restauración de Amazon S3

Para realizar copias de seguridad, copiar y restaurar los recursos de S3, debe tener las políticas correctas en su rol. Para agregar estas políticas, vaya a Políticas administradas de AWS. Añada la AWSBackupServiceRolePolicyForS3Backupy AWSBackupServiceRolePolicyForS3Restorea las funciones que desee utilizar para realizar copias de seguridad y restaurar los buckets de S3.

Si no tiene suficientes permisos, solicite al administrados de la cuenta administrativa (admin) de su organización que agregue las políticas a los roles previstos.

Para obtener más información, consulte Políticas administradas y políticas insertadas en la Guía del usuario de IAM.

AWS Backup para S3 se basa en la recepción de eventos de S3 a través de Amazon EventBridge. Si este ajuste está deshabilitado en la configuración de notificaciones del bucket de S3, se detendrán las copias de seguridad continuas de esos buckets con el ajuste desactivado. Para obtener más información, consulte Uso EventBridge.

Prácticas recomendadas y consideraciones de costo para las copias de seguridad de S3

Prácticas recomendadas

Para buckets con más de 300 millones de objetos:

- En el caso de los buckets con más de 300 millones de objetos, la velocidad de copia de seguridad puede alcanzar hasta 17 000 objetos por segundo durante la copia de seguridad completa inicial del bucket (las copias de seguridad incrementales tendrán una velocidad diferente); las copias de seguridad de los buckets que contengan menos de 300 millones de objetos tendrán una velocidad cercana a los 1000 objetos por segundo.
- Se recomienda realizar copias de seguridad continuas.
- Si está previsto que el ciclo de vida de las copias de seguridad sea de más de 35 días, también puede habilitar copias de seguridad instantáneas para el bucket en el mismo almacén en el que se almacenan las copias de seguridad continuas.

Consideraciones sobre los costos

- Las políticas de ciclo de vida de S3 incluyen una característica opcional denominada Eliminar marcadores de eliminación de objetos vencidos. Cuando esta característica está desactivada, los marcadores de eliminación, que a veces son millones, vencen sin un plan de depuración. Cuando se hace una copia de seguridad de los buckets sin esta característica, hay dos problemas que afectan al tiempo y al costo:
  - Se hacen copias de seguridad de los marcadores de eliminación, al igual que de los objetos. El tiempo de copia de seguridad y el tiempo de restauración pueden verse afectados en función de la proporción entre objetos y marcadores de eliminación.
  - Cada objeto y marcador del que se haga una copia de seguridad tiene un costo mínimo. Cada marcador de eliminación se cobra igual que un objeto de 128 KB.
- En el caso de las cuentas que realizan copias de seguridad al menos a diario o con mayor frecuencia, puede ser beneficioso desde el punto de vista económico el uso de copias de seguridad continuas si los datos de las copias de seguridad sufren cambios mínimos entre las copias de seguridad.
- Los buckets más grandes que no cambian con frecuencia pueden beneficiarse de las copias de seguridad continuas, ya que esto puede reducir los costos cuando los escaneos de todo el

bucket junto con numerosas solicitudes por objeto no necesitan realizarse en objetos preexistentes (objetos que permanecen inalterados desde la copia de seguridad anterior).

- Los buckets que contengan más de 100 millones de objetos y que tengan una tasa de eliminación pequeña en comparación con el tamaño total de la copia de seguridad pueden beneficiarse desde el punto de vista económico de un plan de copia de seguridad que incluya tanto una copia de seguridad continua con un periodo de retención de 2 días como instantáneas con una retención más prolongada.
- El tiempo de copia de seguridad periódica (instantánea) se alinea con el inicio del proceso de copia de seguridad cuando no es necesario escanear los buckets. No es necesario realizar escaneos en un bucket que contenga copias de seguridad continuas e instantáneas, ya que en estos casos las instantáneas se toman desde un punto de recuperación continua.
- Para cada objeto de un solo S3-GIR (Amazon S3 Glacier Instant Retrieval), AWS Backup realiza varias llamadas, lo que generará gastos de recuperación cuando se realice una copia de seguridad.

  Se aplican costos de recuperación similares a los depósitos con objetos de las clases de almacenamiento S3-IA y S3 One Zone-IA.
- AWS KMS CloudTrail, y CloudWatch las funciones de Amazon que forman parte de su estrategia de respaldo pueden generar costos adicionales más allá del almacenamiento de datos en cubos de S3. Para obtener más información sobre cómo ajustar estas características, consulte lo siguiente:
  - Reducción del costo de SSE-KMS con las claves de bucket de Amazon S3 en la Guía del usuario de Amazon S3.
  - Puede reducir CloudTrail los costos excluyendo los AWS KMS eventos y deshabilitando los eventos de datos de S3:
    - Excluir AWS KMS eventos: en la Guía del CloudTrail usuario, al crear una ruta en la consola (selectores de eventos básicos), se ofrece la opción de excluir AWS KMS eventos para filtrarlos de la ruta (la configuración predeterminada incluye todos los eventos de KMS):
    - La opción para registrar o excluir eventos de KMS solo se encuentra disponible si registra eventos de administración en su registro de seguimiento. Si elige no registrar eventos de administración, no se registran eventos de KMS y no podrá cambiar la configuración del registro de eventos de KMS.
    - AWS KMS acciones como`Encrypt`, por ejemplo`Decrypt`, y `GenerateDataKey` suelen generar un gran volumen (más del 99%) de eventos. Estas acciones se registran ahora como eventos de lectura. Las acciones relevantes y de bajo volumen de KMS, como `Disable`,

`Delete` y `ScheduleKey` (que normalmente representan menos del 0,5 % del volumen de eventos de KMS), se registran como eventos de Escritura.

- Para excluir eventos de gran volumen como `Encrypt`, `Decrypt` y `GenerateDataKey`, y seguir registrando eventos relevantes como `Disable`, `Delete` y `ScheduleKey`, elija registrar eventos de administración de Escritura y desmarque la casilla de verificación Excluir eventos de AWS KMS .
- Deshabilitar eventos de datos de S3: de forma predeterminada, los registros y los almacenes de datos de eventos no registran eventos de datos. Deshabilite los eventos de datos de S3 antes de la copia de seguridad inicial para reducir los costos.

- Para reducir CloudWatch los costes, puedes dejar de enviar CloudTrail eventos a CloudWatch los registros al actualizar un registro para deshabilitar la configuración de CloudWatch los registros.

Restauración de copias de seguridad de S3

Puede restaurar los datos de S3 de los que hizo una copia de seguridad AWS Backup en la clase de almacenamiento estándar de S3. Puede restaurar los datos de S3 en un bucket existente, incluido el bucket original. Durante la restauración, también puede crear un nuevo bucket de S3 como destino de la restauración. Puede restaurar las copias de seguridad de S3 solo en el mismo Región de AWS lugar donde se encuentra la copia de seguridad.

Puede restaurar todo el bucket de S3, o las carpetas u objetos incluidos en elbucket. AWS Backup restaura la versión actual de ese objeto.

Para restaurar sus datos de S3 mediante AWS Backup, consulteRestauración de datos de S3.

Copias de seguridad de máquinas virtuales

AWS Backup admite la protección de datos centralizada y automatizada para las máquinas virtuales VMware (VM) locales, junto con las máquinas virtuales de VMware Cloud™ (VMC) on AWS y VMware Cloud™ (VMC) on. AWS Outposts Puede realizar copias de seguridad desde sus máquinas virtuales locales y de VMC hasta. AWS Backup A continuación, puede restaurar desde AWS Backup a las máquinas virtuales en las instalaciones, las máquinas virtuales en VMC o VMC en AWS Outposts.

AWS Backup también le proporciona funciones de gestión de copias de seguridad de máquinas virtuales AWS nativas y totalmente gestionadas, como la detección de máquinas virtuales, la programación de copias de seguridad, la gestión de la retención, un nivel de almacenamiento de

bajo coste, copia entre regiones y entre cuentas, compatibilidad con AWS Backup Vault Lock y Audit Manager AWS Backup , cifrado independiente de los datos de origen y políticas de acceso a las copias de seguridad. Consulte la tabla Disponibilidad de características por recurso para obtener una lista completa de capacidades y detalles.

Puede utilizarlas AWS Backup para proteger sus máquinas virtuales en VMware Cloud™ on. AWS Outposts AWS Backup almacena las copias de seguridad de sus máquinas virtuales en la Región de AWS que AWS Outposts está conectado su VMware Cloud™ on. Puede usarlo AWS Backup para proteger su VMware Cloud™ en las AWS Backup máquinas virtuales cuando usa VMware Cloud™ on AWS Outposts para satisfacer sus necesidades de procesamiento de datos local y de baja latencia para los datos de sus aplicaciones. En función de sus requisitos de residencia de datos, puede optar por AWS Backup almacenar las copias de seguridad de los datos de su aplicación en el servidor principal Región de AWS al que esté conectado. AWS Outposts

Máquinas virtuales compatibles

AWS Backup puede realizar copias de seguridad y restaurar máquinas virtuales administradas por un vCenter de VMware.

Actualmente se admiten:

- vSphere 8, 7.0 y 6.7
- Tamaños de disco virtual que son múltiplos de 1 KiB
- Almacenes de datos de NFS, VMFS y VSAN locales y en VMC en AWS
- Modos de transporte SCSI Hot-Add y Network Block Device Secure Sockets Layer (NBDSSL) para copiar datos de las máquinas virtuales de origen a dispositivos VMware locales AWS
- Modo Hot-Add para proteger las máquinas virtuales en VMware Cloud on AWS

Actualmente no se admite:

- Discos RDM (mapeo de discos sin procesar) o controladores NVMe y sus discos
- Modos de disco independiente-persistente e independiente-no persistente

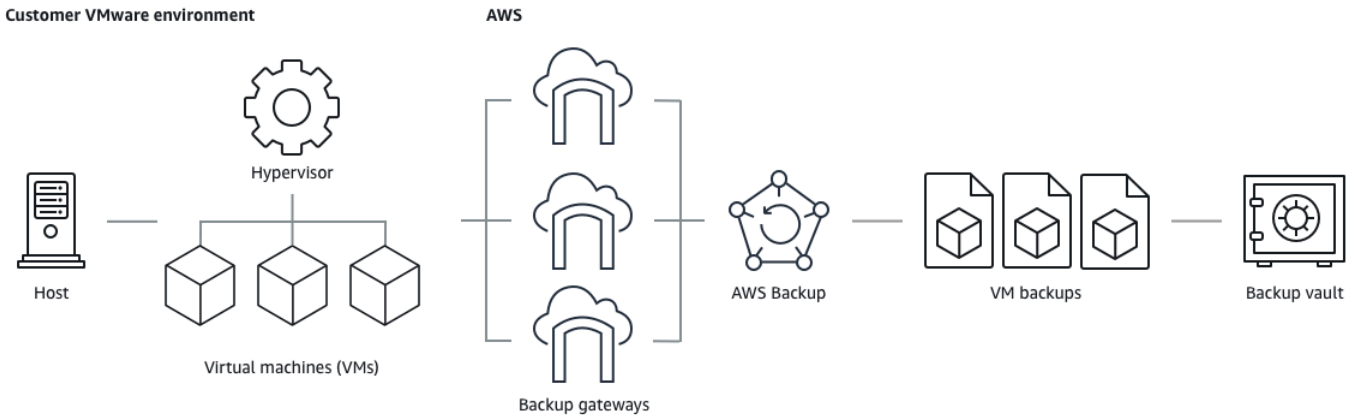
Coherencia de la copia de seguridad

De forma predeterminada,AWS Backup captura copias de seguridad de las máquinas virtuales coherentes con la aplicación mediante la configuración de inactividad de VMware Tools en la

máquina virtual. Sus copias de seguridad son coherentes con la aplicación si estas son compatibles con VMware Tools. Si la función de inactividad no está disponible, captura copias de seguridad consistentes en caso de bloqueos. AWS Backup Pruebe sus restauraciones para comprobar que las copias de seguridad cumplan con las necesidades de la organización.

Puerta de enlace de copia de seguridad

Backup Gateway es un AWS Backup software descargable que se implementa en la infraestructura de VMware para conectar las máquinas virtuales de VMware. AWS Backup La puerta de enlace se conecta a su servidor de administración de máquinas virtuales para detectar las máquinas virtuales, cifrar datos y transferirlos eficazmente a AWS Backup. El siguiente diagrama ilustra cómo se conecta la puerta de enlace de copia de seguridad a las máquinas virtuales:



Para descargar el software de puerta de enlace de copia de seguridad, siga el procedimiento para Uso de puertas de enlace.

Para obtener información sobre los puntos finales de VPC (nube privada virtual), consulte AWS Backup conectividad. AWS PrivateLink

La puerta de enlace de copia de seguridad incluye su propia API, que se mantiene por separado de la API de AWS Backup . Para ver una lista de las acciones de la API de la puerta de enlace de copia de seguridad, consulte Acciones de la puerta de enlace de copia de seguridad. Para ver una lista de los tipos de datos de la API de la puerta de enlace de copia de seguridad, consulte Tipos de datos de la puerta de enlace de copia de seguridad.

puntos de conexión

Los usuarios existentes que actualmente utilizan un punto de conexión público y que desean cambiar a un punto de conexión de VPC (nube privada virtual) pueden crear una nueva puerta de enlace con

un punto de conexión de VPC mediante AWS PrivateLink, asociar el hipervisor existente a la puerta de enlace y, a continuación, eliminar la puerta de enlace que contiene el punto de conexión público.

Configuración de la infraestructura para usar una puerta de enlace de copia de seguridad

La puerta de enlace de copia de seguridad requiere las siguientes configuraciones de red, firewall y hardware para realizar copias de seguridad y restaurar las máquinas virtuales.

Configuración de red

La puerta de enlace de copia de seguridad requiere que se permita el funcionamiento de determinados puertos. Permita los siguientes puertos:

1. TCP 443 saliente
   - Origen: puerta de enlace de copia de seguridad
   - Destino: AWS
   - Uso: Permite que Backup Gateway se comunique con AWS.
2. TCP 80 entrante
   - Fuente: el host que utiliza para conectarse al AWS Management Console
   - Destino: puerta de enlace de copia de seguridad
   - Uso: usado por los sistemas locales para obtener la clave de activación de la puerta de enlace de copia de seguridad. El puerto 80 solo se usa durante la activación de Backup Gateway. AWS Backup no requiere que el puerto 80 sea de acceso público. El nivel de acceso exigido al puerto 80 depende de la configuración de la red. Si activa la puerta de enlace desde el AWS Management Console, el host desde el que se conecta a la consola debe tener acceso al puerto 80 de la puerta de enlace.
3. UDP 53 saliente
   - Origen: puerta de enlace de copia de seguridad
   - Destino: servidor del servicio de nombres de dominio (DNS)
   - Uso: permite que la puerta de enlace de copia de seguridad se comunique con el DNS.
4. TCP 22 saliente
   - Origen: puerta de enlace de copia de seguridad
   - Destino: AWS Support

- Uso: permite acceder AWS Support a su puerta de enlace para ayudarlo con los problemas. No necesita abrir este puerto para el funcionamiento normal de la puerta de enlace, pero es necesario para la solución de problemas.

5. UDP 123 saliente
   - Origen: cliente NTP
   - Destino: servidor NTP
   - Uso: utilizado por los sistemas locales para sincronizar la hora de la VM con la hora del host.
6. TCP 443 saliente
   - Origen: puerta de enlace de copia de seguridad
   - Destino: VMware vCenter
   - Uso: permite que la puerta de enlace de copia de seguridad se comunique con VMware vCenter.
7. TCP 443 saliente
   - Origen: puerta de enlace de copia de seguridad
   - Destino: hosts ESXi
   - Uso: permite que la puerta de enlace de copia de seguridad se comunique con hosts ESXi.
8. TCP 902 saliente
   - Origen: puerta de enlace de copia de seguridad
   - Destino: hosts VMware ESXi
   - Uso: se utiliza para la transferencia de datos a través de la puerta de enlace de copia de seguridad.

Los puertos anteriores son necesarios para Backup Gateway. Consulte Creación de un punto final AWS Backup de VPC para obtener más información sobre cómo configurar los puntos de enlace de Amazon VPC para. AWS Backup

Configuración del firewall

Backup Gateway requiere acceso a los siguientes puntos finales de servicio para poder comunicarse con Amazon Web Services ellos. Si utiliza un firewall o un router para filtrar o limitar el tráfico de red, debe configurar el firewall y el router para dar permiso a los puntos de conexión de servicio para mantener comunicaciones de salida con AWS. No se admite el uso de un proxy HTTP entre la puerta de enlace de copia de seguridad y los puntos de servicio.

```
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
```

Configuración de la puerta de enlace para varias NIC en VMware

Puede mantener redes separadas para el tráfico interno y externo conectando varias conexiones de interfaz de red virtual (NIC) a la puerta de enlace y, a continuación, dirigiendo el tráfico interno (de la puerta de enlace al hipervisor) y el tráfico externo (de la puerta de enlace a) por separado. AWS

De forma predeterminada, las máquinas virtuales conectadas a la AWS Backup puerta de enlace tienen un adaptador de red (). `eth0` Esta red incluye el hipervisor, las máquinas virtuales y la puerta de enlace de red (Backup Gateway) que se comunica con el resto de Internet.

A continuación, se muestra un ejemplo de una configuración con varias interfaces de red virtuales:

```
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
```

- En este ejemplo, la conexión es a un hipervisor con IP `10.0.3.123`, la puerta de enlace utilizará `eth0` ya que la IP del hipervisor forma parte del bloque `10.0.3.0/24`
- Para conectarse a un hipervisor con IP `10.0.0.234`, la puerta de enlace utilizará `eth1`
- Para conectarse a una IP fuera de las redes locales (p. ej. `34.193.121.211`), la puerta de enlace volverá a la puerta de enlace predeterminada, `10.0.0.1`, que está en el bloque `10.0.0.0/24` y, por lo tanto, pasará por `eth1`

La primera secuencia para agregar un adaptador de red adicional se produce en el cliente de vSphere:

1. En el cliente de VMware vSphere, abra el menú contextual (haga clic con el botón derecho) de la máquina virtual de la puerta de enlace y elija Edit Settings.

2. En la pestaña Virtual Hardware del cuadro de diálogo Virtual Machine Properties, abra el menú Add New Device y seleccione Network Adapter para agregar un nuevo adaptador de red.
3.
   a. Amplíe los detalles de New Network para configurar el nuevo adaptador.
   b. Asegúrese de que la opción Connect At Power On esté seleccionada.
   c. Para el Adapter Type, consulte los tipos de adaptadores de red en la Documentación de ESXi y vCenter Server.
4. Haga clic en Okay para guardar la nueva configuración del adaptador de red.

La siguiente secuencia de pasos para configurar un adaptador adicional se realiza en la consola de AWS Backup puerta de enlace (tenga en cuenta que esta no es la misma interfaz que la consola de AWS administración, donde se administran las copias de seguridad y otros servicios).

Una vez que se agregue la nueva NIC a la máquina virtual de puerta de enlace, debe

- Ir a `Command Prompt` y encender los nuevos adaptadores.
- Configurar las IP estáticas para cada NIC nueva
- Establecer la NIC preferida como predeterminada

Para ello:

1. En el cliente VMware vSphere, seleccione la máquina virtual de puerta de enlace e inicie Web Console para acceder a la consola local de Backup Gateway.
   - Para obtener más información sobre el acceso a una consola local, consulte Accessing the Gateway Local Console with VMware ESXi
2. Salga de la línea de comandos y vaya a Configuración de red > Configurar IP estática y siga las instrucciones de configuración para actualizar la tabla de enrutamiento.
   a. Asigne una IP estática dentro de la subred del adaptador de red.
   b. Establezca una máscara de red.
   c. Elija la dirección IP de la puerta de enlace de aparece por defecto. Esta es la puerta de enlace de red que se conecta a todo el tráfico fuera de la red local.
3. Seleccione Establecer adaptador predeterminado para designar el adaptador que se conectará a la nube como dispositivo predeterminado.

4. Todas las direcciones IP de la puerta de enlace se pueden mostrar tanto en la consola local como en la página de resumen de la máquina virtual en VMware vSphere.

Requisitos de hardware

Debe poder dedicar los siguientes recursos mínimos en un host de máquina virtual para la puerta de enlace de copia de seguridad:

- 4 procesadores virtuales
- 8 GiB de RAM reservada

Permisos de VMware

En esta sección se enumeran los permisos mínimos de VMware necesarios para su uso AWS Backup gateway. Estos permisos son necesarios para que la puerta de enlace de copia de seguridad detecte, realice copias de seguridad y restaure máquinas virtuales.

Para usar Backup Gateway con VMware Cloud™ activado AWS o VMware Cloud™ activado AWS Outposts, debe usar el usuario administrador predeterminado `cloudadmin@vmc.local` o asignar la CloudAdmin función a su usuario dedicado.

Para usar Backup Gateway con máquinas virtuales locales de VMware, cree un usuario dedicado con los permisos que se indican a continuación.

Global

- Deshabilitar métodos
- Habilitar métodos
- Licencias
- Registrar eventos
- Administrar atributos personalizados
- Establecer atributos personalizados

Etiquetar vSphere

- Asignar o anular la asignación de etiquetas de vSphere

DataStore

- Asignar espacio
- Explorar el almacén de datos
- Configurar el almacén de datos (para el almacén de datos de vSAN)
- Operaciones de archivos de bajo nivel
- Actualizar los archivos de la máquina virtual

Host

- Configuración
  - Configuración avanzada
  - Configuración de la partición de almacenamiento

Carpeta

- Crear carpeta

Network

- Asignar red

Grupo de dvPort

- Creación
- Delete

Recurso

- Asignar una máquina virtual al grupo de recursos

Máquina virtual

- Cambio de configuración
  - Adquirir un arrendamiento de disco

  - Agregar un disco existente
  - Agregar un disco nuevo
  - Configuración avanzada
  - Cambiar la configuración del .
  - Configurar dispositivo sin procesar
  - Modificar la configuración del dispositivo
  - Eliminar un disco
  - Establecer anotación
  - Activar el seguimiento de cambios de disco
- Editar inventario
  - Crear desde elemento existente
  - Crear nuevo
  - Regístrese
  - Remove
  - Anular registro
- Interacción
  - Apagar
  - Encender
- Aprovisionar
  - Permitir acceso al disco
  - Permitir acceso de solo lectura al disco
  - Permitir la descarga de la máquina virtual
- Administración de instantáneas
  - Crear una instantánea
  - Eliminar instantánea
  - Revertir a la instantánea

Uso de puertas de enlace

Para realizar copias de seguridad y restaurar sus máquinas virtuales (VM) mediante AWS Backup, primero debe instalar una puerta de enlace de respaldo. Una puerta de enlace es un software en

forma de plantilla OVF (Open Virtualization Format) que conecta Amazon Web Services Backup con su hipervisor, lo que le permite detectar automáticamente sus máquinas virtuales y le permite realizar copias de seguridad y restaurarlas.

Una sola puerta de enlace puede ejecutar hasta 4 trabajos de copia de seguridad o restauración a la vez. Para ejecutar más de 4 trabajos a la vez, cree más puertas de enlace y asócielas al hipervisor.

Creación de una puerta de enlace

Para crear una puerta de enlace:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Puertas de enlace.
3. Seleccione Crear puerta de enlace.
4. En la sección Configurar puerta de enlace, siga estas instrucciones para descargar e implementar la plantilla de OVF.

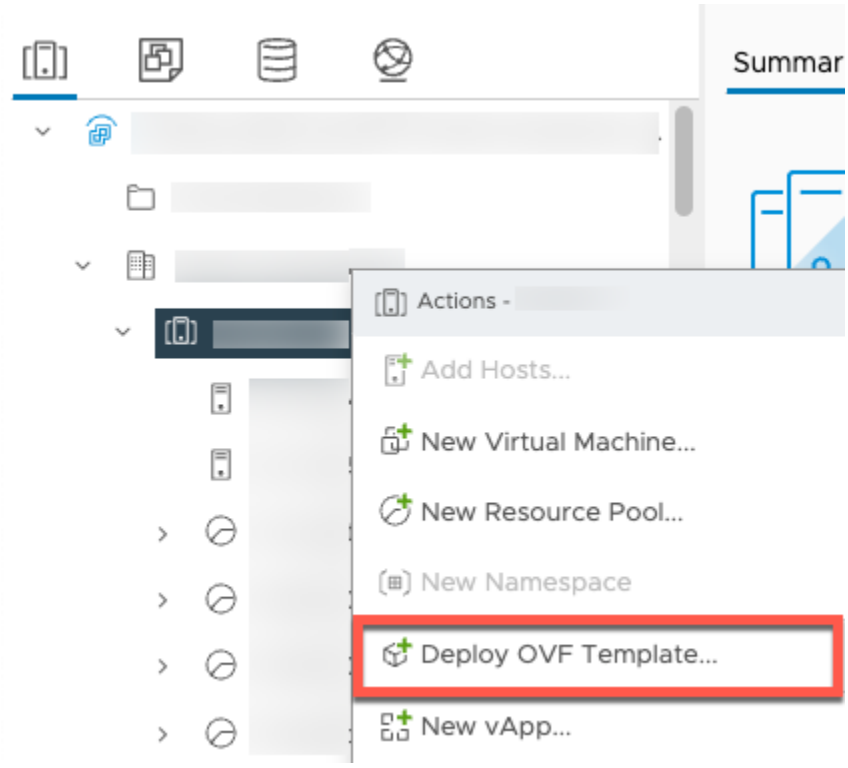
Descargar el software de VMware

Conexión con el hipervisor

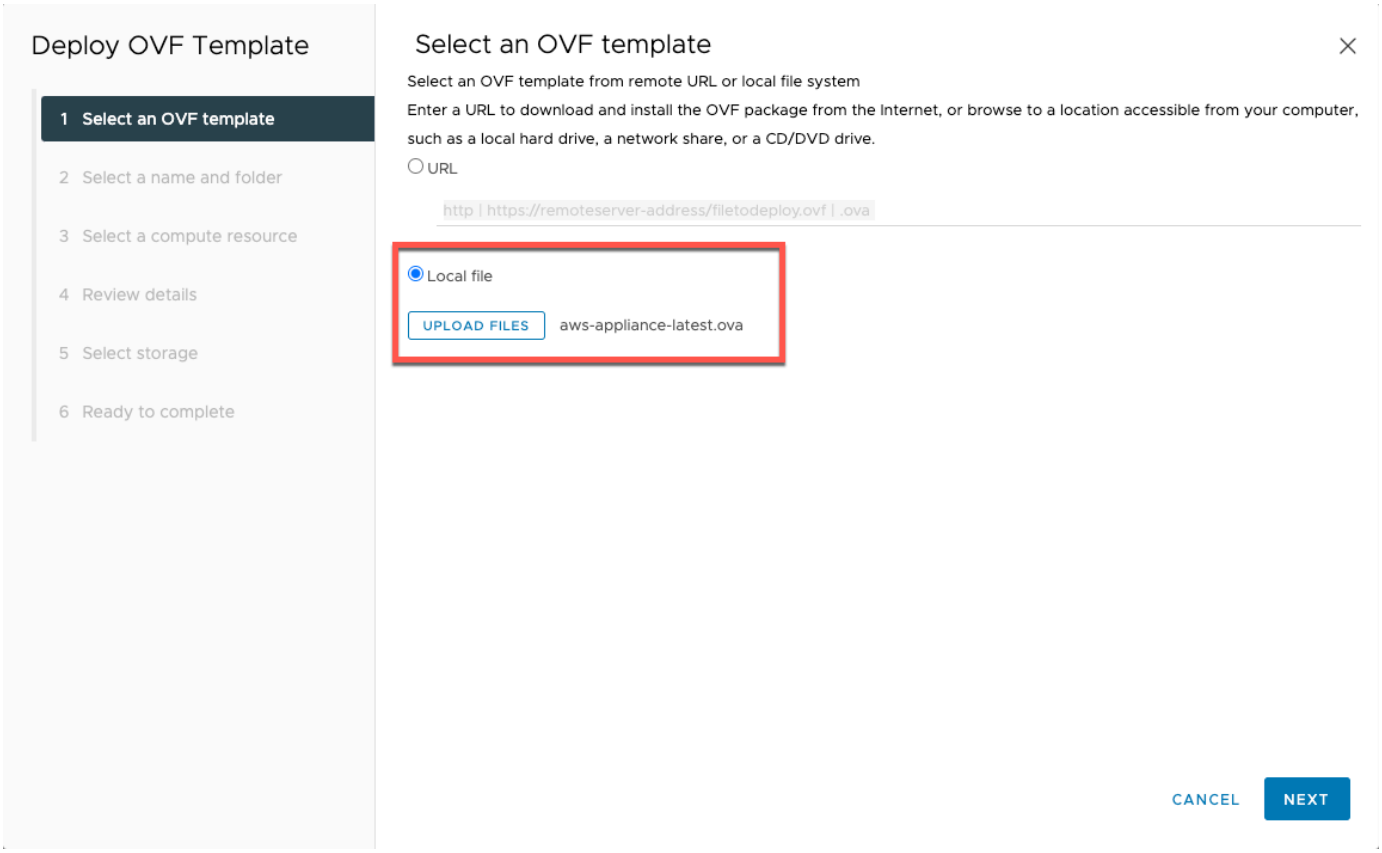
Las pasarelas AWS Backup se conectan al hipervisor para que pueda crear y almacenar copias de seguridad de sus máquinas virtuales. Para configurar su puerta de enlace en VMware ESXi, descargue la plantilla de OVF. El proceso de descarga puede llevar unos 10 minutos.

Una vez que se haya completado, continúe con los siguientes pasos:

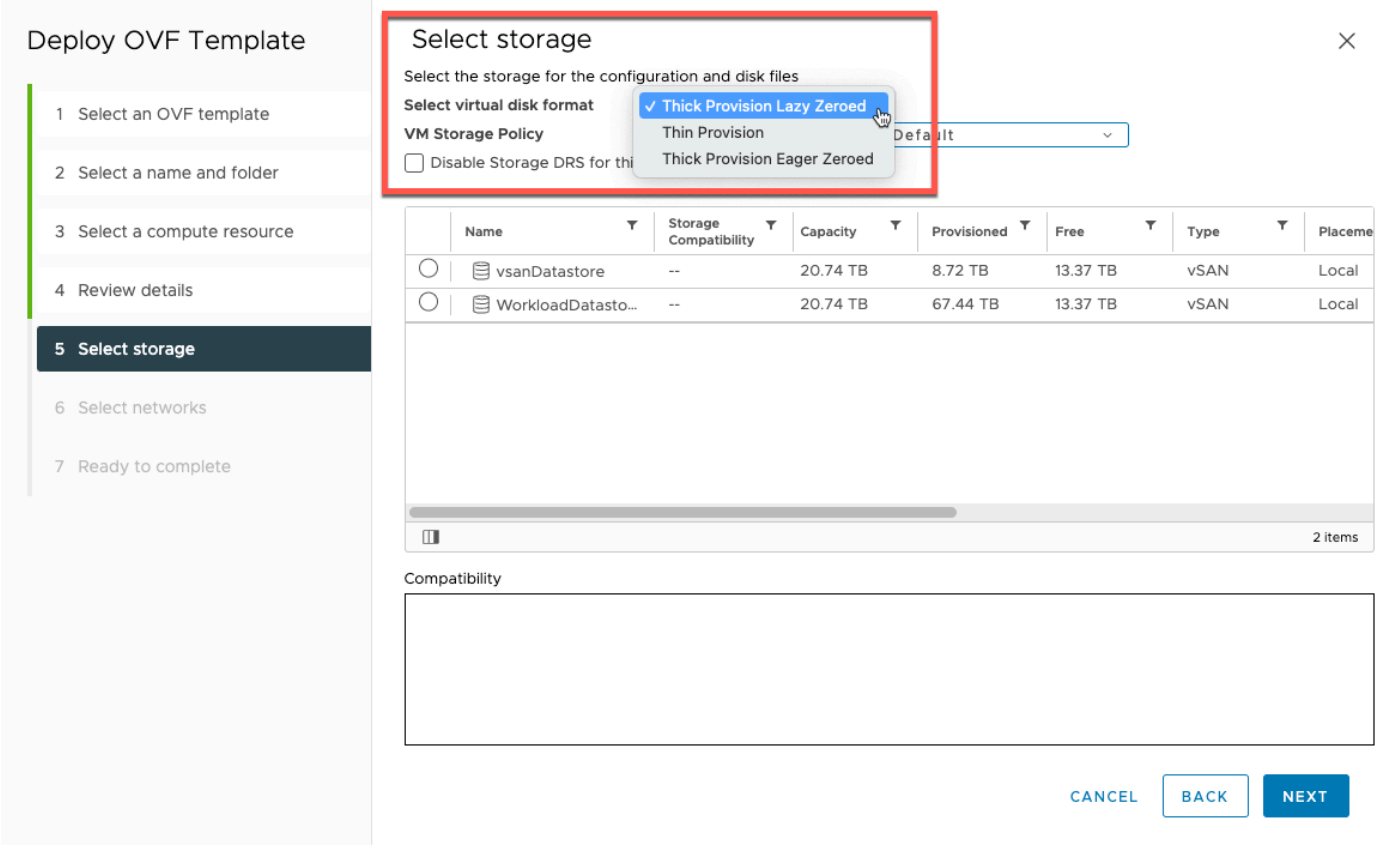
1. Conéctese al hipervisor de su máquina virtual mediante VMware vSphere.
2. Haga clic con el botón derecho en un objeto principal de una máquina virtual y seleccione Implementar plantilla de OVF.



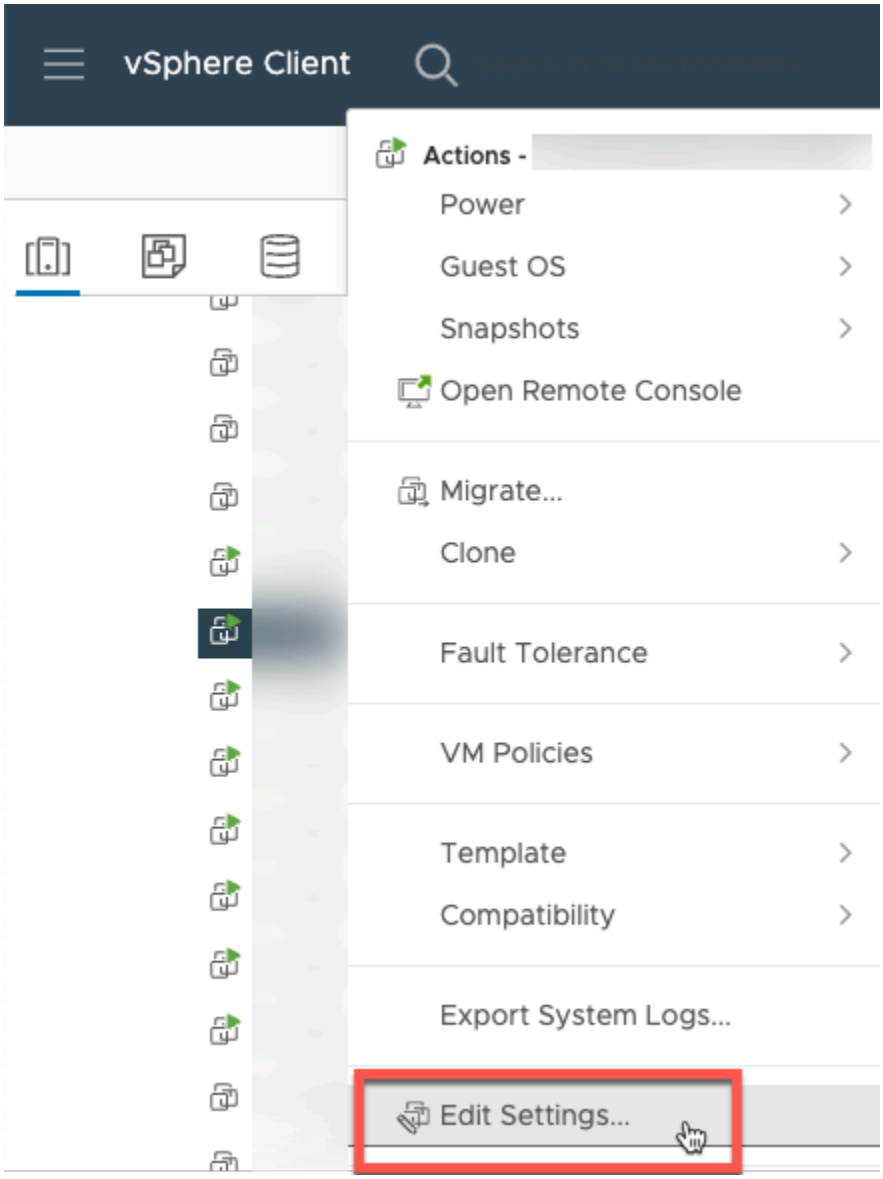
3. Elija Archivo local y cargue el aws-appliance-latestarchivo.ova que descargó.



4. Siga los pasos del asistente de implementación para implementarlo. En la página Seleccionar almacenamiento, seleccione el formato de disco virtual Thick Provision Lazy Zeroed.

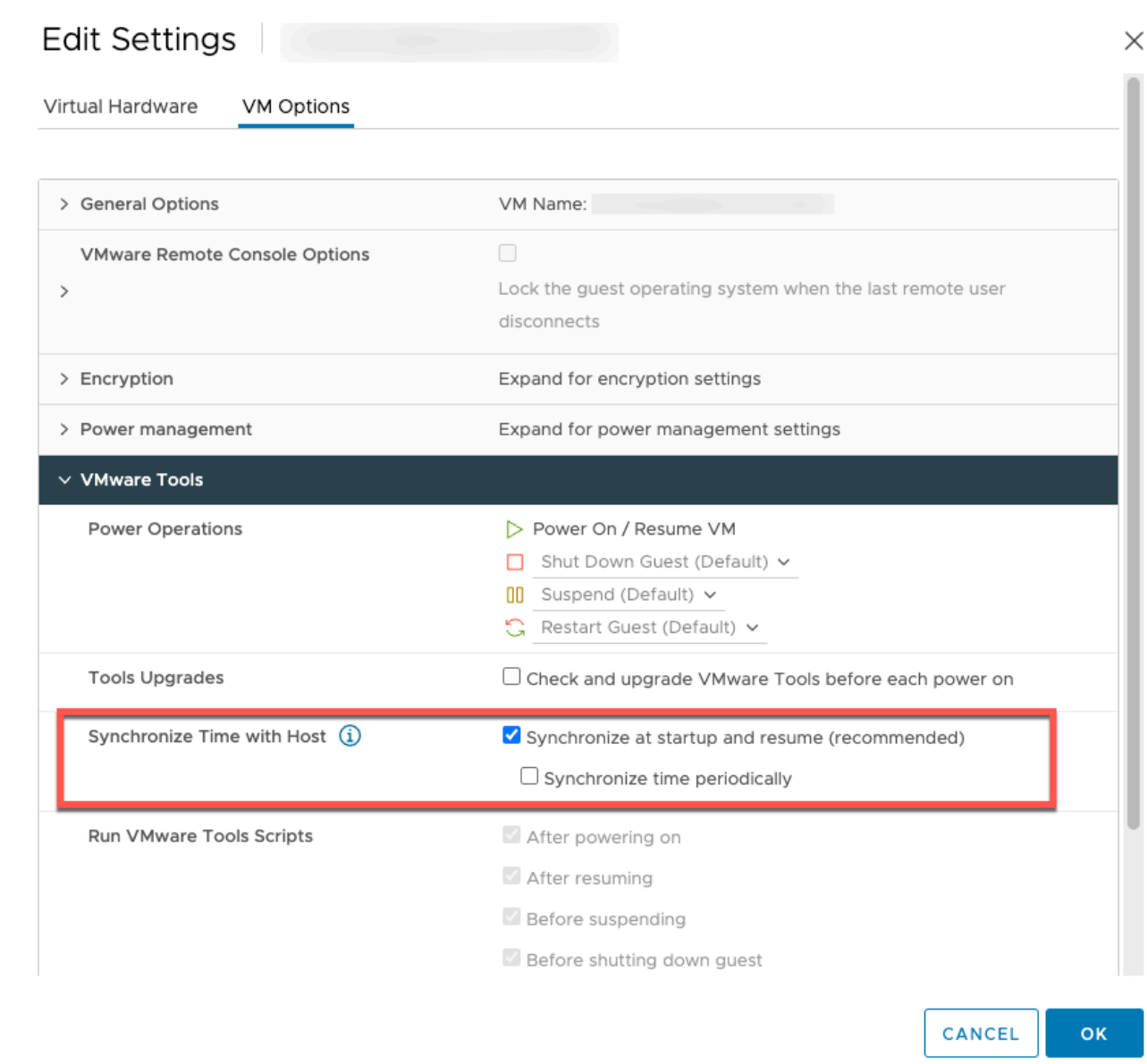


5. Tras implementar el OVF, haga clic con el botón derecho en la puerta de enlace y elija Editar configuración.

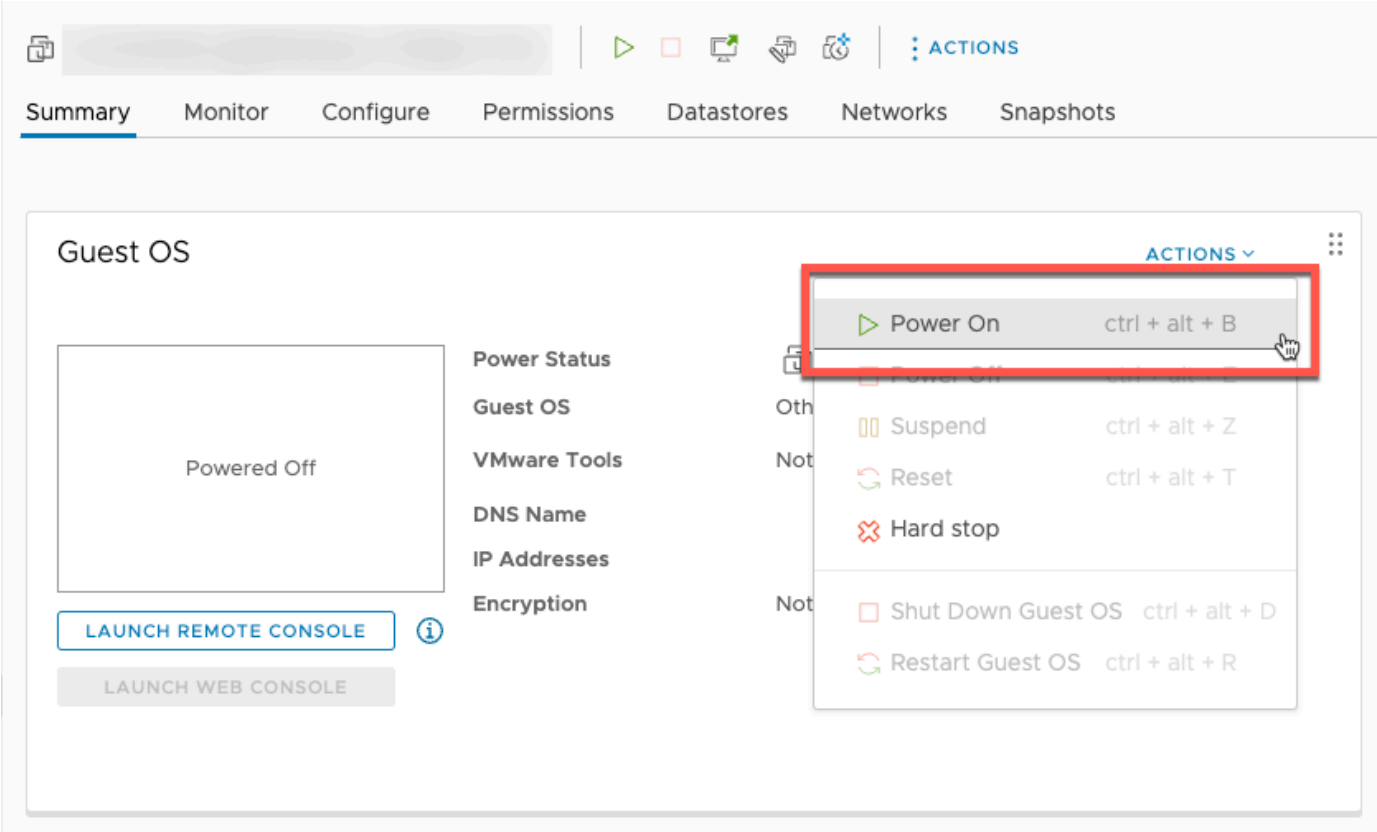


a. En Opciones de máquina virtual, vaya a Herramientas de máquina virtual.

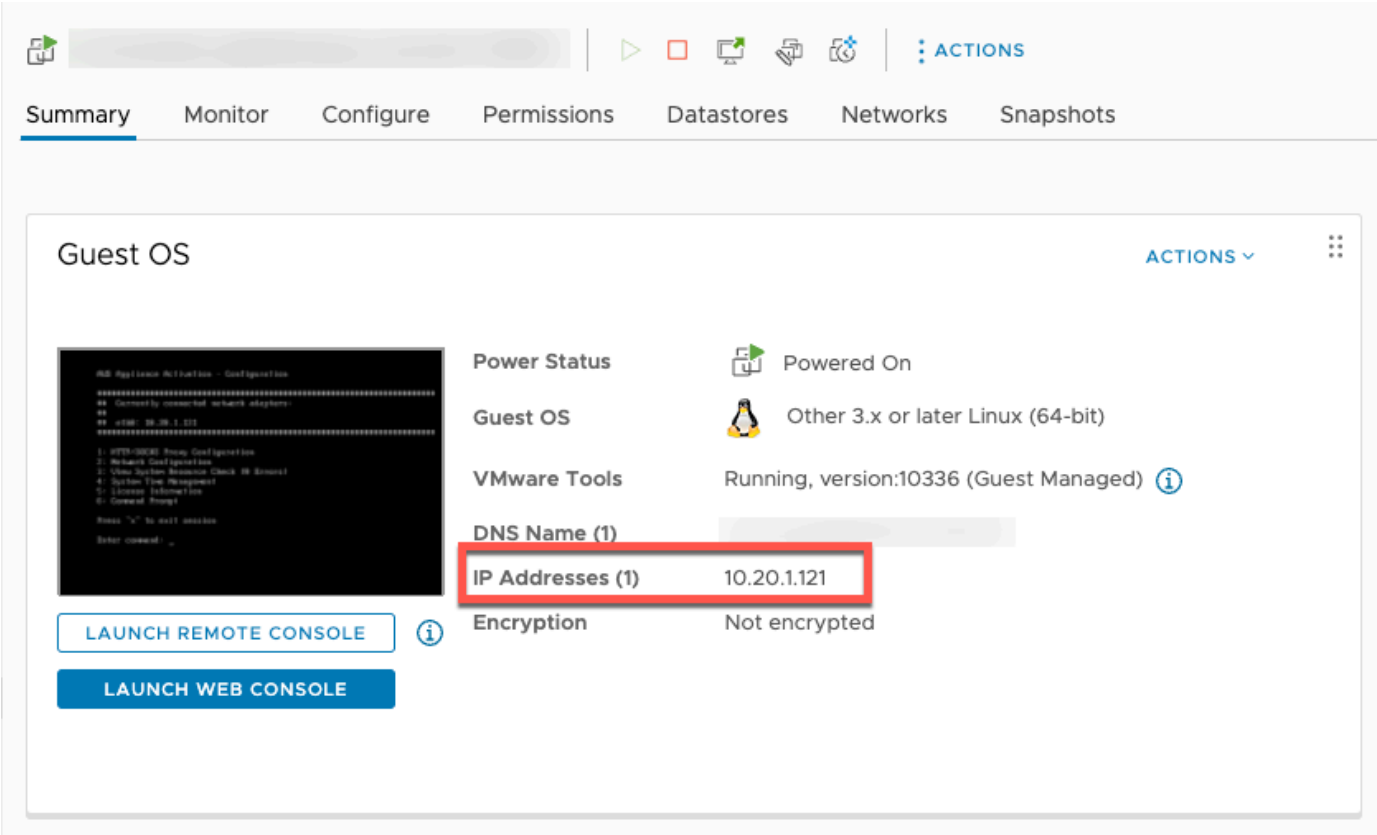
b. Asegúrese de que en Sincronizar la hora con el host, esté seleccionada la opción Sincronizar al inicio y al reanudar.



6. Encienda la máquina virtual con la opción de encender en el menú Acciones.



7. Copie la dirección IP del resumen de la máquina virtual e introdúzcala a continuación.



Tenga en cuenta lo siguiente cuando descargue el software de VMware:

1. En la sección Conexión de la puerta de enlace, escriba la dirección IP de la puerta de enlace.
   a. Para buscar esta dirección IP, vaya a vSphere Client.
   b. Seleccione su puerta de enlace en la pestaña Resumen.
   c. Copie la dirección IP y péguela en la barra de texto de la AWS Backup consola.
2. En la sección Configuración de puerta de enlace,
   a. Escriba el Nombre de la puerta de enlace.
   b. Compruebe la AWS región.
   c. Elija si el punto de conexión es de acceso público o está alojado en su nube privada virtual (VPC).
   d. Según el punto de conexión elegido, introduzca el nombre de DNS del punto de conexión de la VPC.

      Para obtener más información, consulte Creación de un punto de conexión de VPC.
3. [Opcional] En la sección Etiquetas de puerta de enlace, puede asignar etiquetas si introduce la clave y el valor opcional. Para agregar más de una etiqueta, haga clic en Agregar otra etiqueta.
4. Para completar el proceso, haga clic en Crear puerta de enlace, que lo llevará a la página de detalles de la puerta de enlace.

Edición o eliminación de una puerta de enlace

Para editar o eliminar una puerta de enlace:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Puertas de enlace.
2. En la sección Puertas de enlace, elija una puerta de enlace por su Nombre de puerta de enlace.
3. Para editar el nombre de la puerta de enlace, elija Editar.
4. Para eliminar la puerta de enlace, elija Eliminar y, a continuación, elija Eliminar puerta de enlace.

   No puede reactivar una puerta de enlace eliminada. Si desea volver a conectarse al hipervisor, siga el procedimiento que se indica en Creación de una puerta de enlace.
5. Para conectarse a un hipervisor, en la sección Hipervisor conectado, elija Conectar.

Cada puerta de enlace se conecta a un único hipervisor. Sin embargo, puede conectar varias puertas de enlace al mismo hipervisor para aumentar el ancho de banda entre ellas por encima del ancho de banda de la primera puerta de enlace.

6. Para asignar, editar o administrar etiquetas, en la sección Etiquetas, elija Administrar etiquetas.

Limitación del ancho de banda de Backup Gateway

> **Note**
>
> Esta característica estará disponible en las nuevas puertas de enlace que se implementen después del 15 de diciembre de 2022. Para las puertas de enlace existentes, esta nueva capacidad estará disponible mediante una actualización automática del software a más tardar el 30 de enero de 2023. Para actualizar manualmente la puerta de enlace a la última versión, utilice AWS CLI el comando. `UpdateGatewaySoftwareNow`

Puede limitar el rendimiento de carga desde su puerta de enlace AWS Backup para controlar la cantidad de ancho de banda de red que utiliza la puerta de enlace. De forma predeterminada, una puerta de enlace activada no tiene límites de carga o descarga.

Puede configurar un programa de límite de velocidad de ancho de banda mediante la AWS Backup consola o mediante la AWS CLI API mediante (). `PutBandwidthRateLimitSchedule` Cuando utiliza una programación de límite de velocidad de ancho de banda, puede configurar los límites para que cambien automáticamente a lo largo del día o de la semana.

La limitación de la velocidad de ancho de banda funciona equilibrando el rendimiento de todos los datos que se cargan, promediado en cada segundo. Si bien es posible que las cargas superen brevemente el límite de velocidad de ancho de banda durante un microsegundo o milisegundo determinado, esto no suele provocar picos importantes durante periodos de tiempo más prolongados.

Puede agregar un máximo de 20 intervalos. El valor máximo de la velocidad de carga es de 8 000 000 (millones) de megabytes por segundo (Mbps).

Consulta y edita el programa de límite de velocidad de ancho de banda de tu puerta de enlace mediante la consola. AWS Backup

En esta sección, se describe cómo ver y editar la programación de límite de velocidad de ancho de banda de su puerta de enlace.

Para ver y editar la programación de límite de velocidad de ancho de banda

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, seleccione Puertas de enlace. En el panel Puertas de enlace, se muestran las puertas de enlace por nombre. Haga clic en el botón de opción situado junto al nombre de la puerta de enlace que desee administrar.
3. Una vez que haya seleccionado un botón de opción, podrá hacer clic en el menú desplegable Acción. Haga clic en Acciones y, a continuación, en Editar programación de límite de velocidad de ancho de banda. Aparece la programación actual. De forma predeterminada, una puerta de enlace nueva o sin editar no tiene límites de velocidad de ancho de banda definidos.

   > **Note**
   >
   > También puede hacer clic en Administrar programación en la página de detalles de la puerta de enlace para ir a la página Editar ancho de banda.

4. (Opcional) Seleccione Agregar intervalo para agregar un nuevo intervalo configurable a la programación. Para cada intervalo, introduzca la siguiente información:

   a. Días de la semana: seleccione el día o los días periódicos a los que desee que se aplique el intervalo. Cuando los elija, los días de aparece en el menú desplegable. Para eliminarlos, haga clic en la X situada junto al día.

   b. Hora de inicio: introduzca la hora de inicio del intervalo de ancho de banda con el formato HH:MM de 24 horas. La hora debe especificarse de acuerdo con el horario universal coordinado (UTC).

      Nota: El bandwidth-rate-limit intervalo comienza al comienzo del minuto especificado.

   c. Hora de finalización: introduzca la hora de finalización del intervalo de ancho de banda con el formato HH:MM de 24 horas. La hora debe especificarse de acuerdo con el horario universal coordinado (UTC).

> **Important**
>
> El bandwidth-rate-limit intervalo finaliza al final del minuto especificado. Para programar un intervalo que finalice al final de una hora, introduzca 59. Para programar intervalos continuos consecutivos, con transferencia al principio de la hora, sin interrupción entre los intervalos, introduzca 59 para el minuto final del primer intervalo. Introduzca `00` para el minuto de inicio del siguiente intervalo.

d. Velocidad de carga: introduzca el límite de velocidad de carga, en megabits por segundo (Mbps). El valor mínimo es de 102 megabytes por segundo (Mbps).

5. (Opcional) Repita el paso anterior como desee hasta completar la programación de límite de velocidad de ancho de banda. Si necesita eliminar un intervalo de la programación, elija Eliminar.

> **Important**
>
> Los intervalos de límite de velocidad de ancho de banda no se pueden superponer. La hora de inicio de un intervalo debe producirse después de la hora de finalización del intervalo anterior y antes de la hora de inicio del intervalo siguiente; la hora de finalización debe producirse antes de la hora de inicio del intervalo siguiente.

6. Cuando haya terminado, haga clic en el botón Guardar cambios.

Consulte y edite la programación de límite de velocidad de ancho de banda de su puerta de enlace mediante la AWS CLI

La acción `GetBandwidthRateLimitSchedule` se puede utilizar para ver la programación de limitación del ancho de banda de una puerta de enlace concreta. Si no se ha definido una programación, esta será una lista vacía de intervalos. A continuación, se muestra un ejemplo en el AWS CLI que se utiliza para obtener el programa de ancho de banda de una puerta de enlace:

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

Para editar la programación de limitación del ancho de banda de una puerta de enlace, puedes usar la acción `PutBandwidthRateLimitSchedule`. Tenga en cuenta que solo puede actualizar la programación de una puerta de enlace en su conjunto, en lugar de modificar, agregar o eliminar

intervalos individuales. Al llamar a esta acción, se sobrescribirá la programación anterior de limitación del ancho de banda de la puerta de enlace.

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

Uso de hipervisores

Cuando terminaCreación de una puerta de enlace, puede conectarlo a un hipervisor para que pueda AWS Backup trabajar con las máquinas virtuales administradas por ese hipervisor. Por ejemplo, el hipervisor para las máquinas virtuales de VMware es VMware vCenter Server. Asegúrese de que el hipervisor esté configurado con los permisos necesarios para AWS Backup.

Adición de un hipervisor

Para agregar un hipervisor:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.
2. Seleccione Agregar hipervisor.
3. En la sección Configuración del hipervisor, escriba un Nombre del hipervisor.
4. Para Host del servidor vCenter, utilice el menú desplegable para seleccionar la dirección IP o el FQDN (nombre de dominio completo). Escriba el valor correspondiente.
5. AWS Backup Para permitir la detección de las máquinas virtuales en el hipervisor, introduzca el nombre de usuario y la contraseña del hipervisor.
6. Cifre la contraseña. Para especificar este cifrado, seleccione una clave de KMS específica administrada por el servicio o una clave de KMS administrada por el cliente mediante el menú desplegable o a través de Crear clave de KMS. Si no selecciona una clave específica, AWS Backup cifrará su contraseña con una clave propiedad del servicio.
7. En la sección Conexión con la puerta de enlace, utilice la lista desplegable para especificar la puerta de enlace que desee conectar al hipervisor.
8. Seleccione Probar la conexión de la puerta de enlace para verificar las entradas anteriores.
9. Si lo desea, en la sección Etiquetas de hipervisor, puede agregar etiquetas al hipervisor mediante Añadir nueva etiqueta.
10. Asignación opcional de etiquetas de VMware: puede añadir hasta 10 etiquetas de VMware que utilice actualmente en sus máquinas virtuales para generar AWS etiquetas.

11. En el panel de configuración del grupo de registros, puede optar por integrarlo con Amazon CloudWatch Logs para mantener los registros de su hipervisor (se aplicará el precio estándar de CloudWatch Logs en función del uso). Cada hipervisor puede pertenecer a un grupo de registro.

    a. Si aún no ha creado un grupo de registro, seleccione el botón de opción Crear un nuevo grupo de registro. El hipervisor que está editando se asociará a este grupo de registro.

    b. Si ha creado anteriormente un grupo de registro para un hipervisor diferente, puede usar ese grupo de registro para este hipervisor. Seleccione Utilizar un grupo de registro existente.

    c. Si no desea CloudWatch registrar, seleccione Desactivar el registro.

12. Elija Agregar hipervisor para acceder a su página de detalles.

> **Tip**
>
> Puede utilizar Amazon CloudWatch Logs (consulte el paso 11 anterior) para obtener información sobre el hipervisor, incluida la supervisión de errores, la conexión de red entre la puerta de enlace y el hipervisor y la información de configuración de la red. Para obtener información sobre los grupos de CloudWatch registros, consulte Trabajar con grupos de registros y transmisiones de registros en la Guía del CloudWatch usuario de Amazon.

Visualización de máquinas virtuales administradas por un hipervisor

Para ver las máquinas virtuales en un hipervisor:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.
2. En la sección Hipervisores, elija un hipervisor en Nombre del hipervisor para ir a su página de detalles.
3. En la sección titulada Resumen del hipervisor, elija la pestaña Máquinas virtuales.
4. En la sección Máquinas virtuales conectadas, se rellena automáticamente una lista de máquinas virtuales.

Visualización de las puertas de enlace conectadas a un hipervisor

Par ver las puertas de enlace conectadas al hipervisor:

1. Seleccione la pestaña Puertas de enlace.
2. En la sección Puertas de enlace conectadas, se rellena automáticamente una lista de puertas de enlace.

Conexión de un hipervisor a puertas de enlace adicionales

Las velocidades de copia de seguridad y restauración pueden estar limitadas por el ancho de banda de la conexión entre la puerta de enlace y el hipervisor. Para aumentar estas velocidades, puede conectar una o más puertas de enlace adicionales al hipervisor. Puede hacerlo en la sección Puertas de enlace conectadas de la siguiente manera:

1. Elija Conectar.
2. Seleccione otra puerta de enlace mediante el menú desplegable. También puede elegir Crear puerta de enlace para crear una nueva puerta de enlace.
3. Elija Conectar.

Edición de la configuración de un hipervisor

Si no utiliza la característica Probar la conexión de la puerta de enlace, podría agregar un hipervisor con un nombre de usuario o contraseña incorrectos. En ese caso, el estado de conexión del hipervisor es siempre `Pending`. Como alternativa, puede rotar el nombre de usuario o la contraseña para acceder al hipervisor. Actualice esta información mediante el siguiente procedimiento.

Para editar un hipervisor ya agregado:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.
2. En la sección Hipervisores, elija un hipervisor en Nombre del hipervisor para ir a su página de detalles.
3. Elija Editar.
4. El panel superior se denomina Configuración del hipervisor.
    a. En Host del servidor vCenter, también puede editar el FQDN (nombre de dominio completo) o la dirección IP.

b. Si lo desea, introduzca el Nombre de usuario y la Contraseña del hipervisor.

5. En el panel de configuración del grupo de registros, puede optar por integrarlo con Amazon CloudWatch para mantener los registros de su hipervisor (se aplicará un CloudWatch precio estándar en función del uso). Cada hipervisor puede pertenecer a un grupo de registro.

   a. Si aún no ha creado un grupo de registro, seleccione el botón de opción Crear un nuevo grupo de registro. El hipervisor que está editando se asociará a este grupo de registro.

   b. Si ha creado anteriormente un grupo de registro para un hipervisor diferente, puede usar ese grupo de registro para este hipervisor. Seleccione Utilizar un grupo de registro existente.

   c. Si no desea CloudWatch registrar, seleccione Desactivar el registro.

> **Tip**
>
> Puede utilizar Amazon CloudWatch Logs (consulte el paso 5 anterior) para obtener información sobre el hipervisor, incluida la supervisión de errores, la conexión de red entre la puerta de enlace y el hipervisor y la información de configuración de la red. Para obtener información sobre los grupos de CloudWatch registros, consulte Trabajar con grupos de registros y transmisiones de registros en la Guía del CloudWatch usuario de Amazon.

Para actualizar un hipervisor mediante programación, utilice el comando de CLI update-hypervisor y la llamada a la API. UpdateHypervisor

Eliminación de la configuración de un hipervisor

Si necesita eliminar un hipervisor ya agregado, elimine la configuración del hipervisor y agregue otra. Esta operación de eliminación se aplica a la configuración para conectarse al hipervisor. No elimina el hipervisor.

Para eliminar la configuración para conectarse a un hipervisor ya agregado:

1. En el panel de navegación de la izquierda, en la sección Recursos externos, elija Hipervisores.
2. En la sección Hipervisores, elija un hipervisor en Nombre del hipervisor para ir a su página de detalles.
3. Elija Eliminar, y, a continuación, elija Eliminar hipervisor.

4. Opcional: sustituya la configuración del hipervisor eliminada mediante el procedimiento para Adición de un hipervisor.

Descripción del estado del hipervisor

A continuación se describen cada uno de los posibles estados del hipervisor y, si corresponde, los pasos de corrección. El estado `ONLINE` es el estado normal del hipervisor. Un hipervisor debe tener este estado todo el tiempo o la mayor parte del tiempo que se use para realizar copias de seguridad y recuperar máquinas virtuales administradas por el hipervisor.

Estados del hipervisor

Status	Significado y corrección
`ONLINE`	Ha agregado un hipervisor AWS Backup, lo ha asociado a una puerta de enlace y puede conectarse a esa puerta de enlace a través de la red para realizar copias de seguridad y recuperación de las máquinas virtuales administradas por el hipervisor. Puede realizar copias de seguridad programadas y bajo demanda de esas máquinas virtuales en cualquier momento.
`PENDING`	Ha agregado un hipervisor, pero: AWS Backup • No está asociado a ninguna puerta de enlace, o • Está asociado a una o más puertas de enlace, pero todas esas puertas de enlace se eliminaron o no están activas por algún otro motivo. Para cambiar el estado de un hipervisor de `PENDING` a `ONLINE`, cree una puerta de enlace y conecte el hipervisor a esa puerta de enlace.

Status	Significado y corrección
`OFFLINE`	Ha agregado un hipervisor AWS Backup y lo ha asociado a una puerta de enlace, pero la puerta de enlace no puede conectarse al hipervisor a través de la red. Para cambiar el estado de un hipervisor de `OFFLINE` a`ONLINE`, compruebe que la configuración de red sea correcta. Si el problema persiste, compruebe que la dirección IP o el nombre de dominio completo del hipervisor sean correctos. Si son incorrectos, vuelva a agregar el hipervisor con la información correcta y pruebe la conexión de la puerta de enlace.
`ERROR`	Ha agregado un hipervisor AWS Backup y lo ha asociado a una puerta de enlace, pero la puerta de enlace no puede comunicarse con el hipervisor. Para cambiar el estado de un hipervisor de `ERROR` a `ONLINE`, compruebe que el nombre de usuario y la contraseña del hipervisor sean correctos. Si son incorrectos, edite la configuración del hipervisor.

Pasos siguientes

Para hacer una copia de seguridad de las máquinas virtuales en el hipervisor, consulte Copia de seguridad de máquinas virtuales.

Copia de seguridad de máquinas virtuales

Después de Adición de un hipervisor, la puerta de enlace de copia de seguridad muestra automáticamente las máquinas virtuales. Para ver sus máquinas virtuales, seleccione Hipervisores o Máquinas virtuales en el panel de navegación izquierdo.

- Elija Hipervisores para ver solo las máquinas virtuales administradas por un hipervisor concreto. Con esta vista, puede trabajar con una máquina virtual a la vez.
- Elija Máquinas virtuales para ver todas las máquinas virtuales de todos los hipervisores que ha agregado a la suya. Cuenta de AWS Con esta vista, puede trabajar con algunas o todas sus máquinas virtuales en varios hipervisores.

Independientemente de la vista que elija, para realizar una operación de copia de seguridad en una máquina virtual específica, elija el Nombre de máquina virtual para abrir su página de detalles. La página de detalles de la máquina virtual es el punto de partida de los siguientes procedimientos.

Creación de una copia de seguridad bajo demanda de una máquina virtual

Una copia de seguridad bajo demanda es una copia de seguridad completa y única que se inicia manualmente. Puede utilizar copias de seguridad bajo demanda para probar las capacidades AWS Backup de copia de seguridad y restauración.

Para crear una copia de seguridad bajo demanda de una máquina virtual:

1. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda).
2. Configure la copia de seguridad bajo demanda.
3. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda).
4. Compruebe si su trabajo de copia de seguridad tiene el estado `Completed`. En el panel de navegación izquierdo, elija Trabajos.
5. Elija el ID de trabajo de copia de seguridad para ver la información del trabajo de copia de seguridad, como el Tamaño de copia de seguridad y el tiempo transcurrido entre la fecha de Fecha de creación y la Fecha de finalización.

Copias de seguridad incrementales de máquinas virtuales

Las versiones más recientes de VMware incluyen una característica denominada Changed Block Tracking, que realiza un seguimiento de los bloques de almacenamiento de las máquinas virtuales

a medida que cambian con el paso del tiempo. Cuando realiza una copia de seguridad de una máquina virtual, AWS Backup intenta utilizar los datos CBT si están disponibles. AWS Backup AWS Backup utiliza datos CBT para acelerar el proceso de copia de seguridad; sin datos CBT, los trabajos de copia de seguridad suelen ser más lentos y utilizan más recursos del hipervisor. La copia de seguridad aún se puede completar correctamente incluso si los datos de CBT no son válidos o no están disponibles. Por ejemplo, es posible que los datos de CBT no sean válidos o no estén disponibles si la máquina virtual o el host ESXi se apagan bruscamente.

En los casos en que los datos de CBT no sean válidos o no estén disponibles, el estado de la copia de seguridad aparecerá con un mensaje `Successful`. En estos casos, el mensaje indicará que, ante la ausencia de datos CBT, AWS Backup utilizó su propio mecanismo de detección de cambios para completar la copia de seguridad en lugar de utilizar los datos CBT de VMware. Las copias de seguridad posteriores volverán a intentar utilizar los datos de CBT y, en la mayoría de los casos, los datos de CBT serán válidos y estarán disponibles correctamente. Si el problema persiste, consulte Solución de problemas de VMware para ver los pasos de resolución.

Para que el CBT funcione de forma correcta, debe cumplirse lo siguiente:

- El host debe ser ESXi 4.0 o posterior
- La máquina virtual propietaria de los discos debe tener la versión de hardware 7 o posterior
- CBT debe estar habilitada para la máquina virtual (está habilitado de forma predeterminada)

Para comprobar si un disco virtual tiene CBT habilitado:

1. Abra vSphere Client y seleccione una máquina virtual apagada.
2. Haga clic con el botón derecho en la máquina virtual y vaya a Edit Settings > Options > Advanced/ General > Configuration Parameters.
3. La opción `ctkEnabled` debe ser `True`.

Automatización de la copia de seguridad de la máquina virtual mediante la asignación de recursos a un plan de copia de seguridad

Un plan de copia de seguridad es una política de protección de datos definida por el usuario que automatiza la protección de datos en muchos servicios de AWS y aplicaciones de terceros. Primero debe crear su plan de copia de seguridad en el que especificará la frecuencia de copia de seguridad, el periodo de retención, la política de ciclo de vida y muchas otras opciones. Para crear un plan de copia de seguridad, consulte el tutorial de introducción.

Después de crear su plan de respaldo, debe asignar los recursos AWS Backup compatibles, incluidas las máquinas virtuales, a ese plan de respaldo. AWS Backup ofrece muchas formas de asignar recursos, incluida la asignación de todos los recursos de su cuenta, la inclusión o exclusión de recursos específicos individuales, o la adición de recursos con determinadas etiquetas.

Además de las funciones de asignación de recursos existentes, la AWS Backup compatibilidad con máquinas virtuales presenta varias funciones nuevas que le ayudarán a asignar rápidamente las máquinas virtuales a los planes de respaldo. Desde la página Máquinas virtuales, puede asignar etiquetas a varias máquinas virtuales o utilizar la nueva característica Asignar recursos para planificar. Utilice estas funciones para asignar las máquinas virtuales ya descubiertas por AWS Backup Gateway.

Si prevé detectar y asignar máquinas virtuales adicionales en el futuro y desea automatizar el paso de asignación de recursos para incluir esas máquinas virtuales futuras, utilice la nueva característica Crear asignación de grupo.

Etiquetas de VMware

Las etiquetas son pares clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos.

Una etiqueta de VMware se compone de una categoría y un nombre de etiqueta. Las etiquetas de VMware se utilizan para agrupar máquinas virtuales. Un nombre de etiqueta es una etiqueta asignada a una máquina virtual. Una categoría es una colección de nombres de etiquetas.

En las AWS etiquetas, puede usar caracteres entre letras, números, espacios y caracteres especiales en UTF-8. `+ - = . _ : /`

Si utiliza etiquetas en sus máquinas virtuales, puede agregar hasta 10 etiquetas coincidentes en AWS Backup para ayudar con la organización. Puede asignar hasta 10 etiquetas de VMware a AWS etiquetas. En la AWS Backup consola, se encuentran en Mi organización > Máquinas virtuales > AWS etiquetas o etiquetas de VMware.

Asignación de etiquetas de VMware

Si utiliza etiquetas en sus máquinas virtuales, puede agregar hasta 10 etiquetas coincidentes en AWS Backup para aumentar la claridad y la organización. Las asignaciones se aplican a cualquier máquina virtual del hipervisor.

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En la consola, vaya a Editar hipervisor (haga clic en Recursos externos, luego en Hipervisores, luego en el nombre del hipervisor y, a continuación, en Administrar asignaciones).

3. El último panel, el mapeo de etiquetas de VMware, contiene cuatro campos de cuadro de texto en los que puede introducir la información de las etiquetas de VMware existentes en las etiquetas correspondientes AWS . Los cuatro campos son la categoría de etiqueta de VMware, el nombre de la etiqueta de VMware,AWS la clave de la AWS etiqueta y el valor de la etiqueta (por ejemplo: Categoría = SO; nombre de etiqueta = Windows; clave de AWS etiqueta = OS-Windows y valor de AWS etiqueta = Windows).
4. Una vez que haya introducido sus valores preferidos, haga clic en Agregar mapeo. Si comete un error, puede hacer clic en Eliminar para eliminar la información ingresada.
5. Tras agregar las asignaciones, especifique el rol de IAM que va a utilizar para aplicar estas etiquetas de AWS a las máquinas virtuales de VMware.

   La política `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` contiene todos los permisos necesarios. Puede asociar esta política al rol que utilice (o pedir a un administrador que lo haga) o puede crear una política personalizada para el rol que se utilice.
6. Por último, haga clic en Agregar hipervisor o en Guardar.

La relación de confianza entre los roles de IAM debe modificarse para agregar los servicios backup-gateway.amazonaws.com y backup.amazonaws.com. Sin este servicio, es probable que se produzca un error al asignar etiquetas. Para editar la relación de confianza para un rol existente,

1. Inicie sesión en la consola de IAM.
2. En el panel de navegación de la consola, elija Roles .
3. Elija el nombre del rol que desea modificar y seleccione la pestaña Relaciones de confianza en la página de detalles.
4. En Documento de política, pegue lo siguiente:

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

```
    }
  ]
}
```

5. Elija Actualizar política de confianza.

Consulte Editing the trust relationship for an existing role en la Guía de administración de AWS Directory Service para obtener más detalles.

Visualización de asignaciones de etiquetas de VMware

En la Consola de AWS Backup, haga clic en Recursos externos, luego en Hipervisores y, a continuación, en el enlace con el nombre del hipervisor para ver las propiedades del hipervisor seleccionado. En el panel de resumen, hay cuatro pestañas, la última de las cuales es Asignaciones de etiquetas de VMware. Tenga en cuenta que si aún no tiene asignaciones, se mostrará: “No hay asignaciones de etiquetas de VMware” .

Desde aquí, puede sincronizar los metadatos de las máquinas virtuales descubiertas por el hipervisor, copiar las asignaciones en sus hipervisores, agregar AWS etiquetas asignadas a las etiquetas de VMware a la selección de copias de seguridad de un plan de copias de seguridad o administrar las asignaciones.

En la consola, para ver qué etiquetas se aplican a una máquina virtual seleccionada, haga clic en Máquinas virtuales, luego en el nombre de la máquina virtual y, a continuación, en Etiquetas de AWS o Etiquetas de VMware. Puede ver las etiquetas asociadas a esta máquina virtual y, además, puede administrarlas.

Asignación de máquinas virtuales al plan mediante asignaciones de etiquetas de VMware

Para asignar máquinas virtuales a un plan de copia de seguridad mediante asignaciones de etiquetas, haga lo siguiente:

1. Abra la consola en https://console.aws.amazon.com/backup. AWS Backup
2. En la consola, vaya a las asignaciones de etiquetas de VMware en la página de detalles del hipervisor (haga clic en Recursos externos, luego en Hipervisores y, a continuación en el nombre del hipervisor).
3. Seleccione la casilla de verificación situada junto a varias etiquetas asignadas para asignarlas al mismo plan de copia de seguridad.
4. Haga clic en Agregar a la asignación de recursos.

5. Elija un Plan de copia de seguridad existente de la lista desplegable. También puede elegir Crear plan de copia de seguridad para crear un plan nuevo.
6. Haga clic en Confirmar. Esto abre la página Asignar recursos con la opción Ajustar la selección mediante etiquetas con valores rellenados previamente.

Etiquetas de VMware mediante AWS CLI

AWS Backup utiliza la llamada PutHypervisorPropertyMappingsa la API para asignar las propiedades de las entidades del hipervisor locales a las propiedades internas. AWS

En AWS CLI, utilice la operación: `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
```

A continuación se muestra un ejemplo:

```
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
```

También se puede utilizar GetHypervisorPropertyMappings para obtener información de asignación de propiedades. En el AWS CLI, utilice la operación`get-hypervisor-property-mappings`. A continuación, se muestra una plantilla de ejemplo:

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

A continuación se muestra un ejemplo:

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
```

```
--region us-east-1
```

Sincronice los metadatos de las máquinas virtuales descubiertas por el hipervisor AWS mediante API, CLI o SDK

Puede sincronizar los metadatos de las máquinas virtuales. Cuando lo haga, se sincronizarán las etiquetas de VMware presentes en la máquina virtual que formen parte de las asignaciones. Además, las etiquetas de AWS asignadas a las etiquetas de VMware presentes en la máquina virtual se aplicarán al recurso de máquina virtual de AWS .

AWS Backup utiliza la llamada `StartVirtualMachinesMetadataSync`a la API para sincronizar los metadatos de las máquinas virtuales descubiertas por el hipervisor. Para sincronizar los metadatos de las máquinas virtuales detectadas por el hipervisor mediante la AWS CLI, utilice la operación `start-virtual-machines-metadata-sync`.

Ejemplo de plantilla:

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Ejemplo:

```
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
```

También puede utilizar `GetHypervisor` para obtener información del hipervisor, como el host, el estado o el estado de la última sincronización de metadatos, y también para recuperar la hora de la última sincronización correcta de los metadatos. En el AWS CLI, utilice la operación. `get-hypervisor`

Ejemplo de plantilla:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

Ejemplo:

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

Para obtener más información, consulte la documentación de la API VmwareTagy VmwareToAwsTagMapping.

Esta característica estará disponible en las nuevas puertas de enlace que se implementen después del 15 de diciembre de 2022. Para las puertas de enlace existentes, esta nueva capacidad estará disponible mediante una actualización automática del software a más tardar el 30 de enero de 2023. Para actualizar la puerta de enlace a la última versión de forma manual, usa AWS CLI el comando UpdateGatewaySoftwareNow.

Ejemplo:

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

Asignación de máquinas virtuales mediante etiquetas

Puede asignar las máquinas virtuales que encuentre actualmente AWS Backup, junto con otros AWS Backup recursos, asignándoles una etiqueta que ya haya asignado a uno de sus planes de backup existentes. También puede crear un nuevo plan de copia de seguridad y una nueva asignación de recursos basada en etiquetas. Los planes de copia de seguridad comprueban los recursos recién asignados cada vez que ejecutan un trabajo de copia de seguridad.

Para etiquetar varias máquinas virtuales con la misma etiqueta:

1. En el panel de navegación izquierdo, elija Máquinas virtuales.
2. Seleccione la casilla de verificación situada junto al Nombre de máquina virtual para elegir todas las máquinas virtuales. También puede seleccionar la casilla de verificación situada junto a los nombres de las máquinas virtuales que desee etiquetar.
3. Elija Add tags (Añadir etiquetas).
4. Escriba una Clave de etiqueta.
5. Recomendado: escriba un Valor de etiqueta.
6. Elija Confirmar.

Asignación de máquinas virtuales mediante la característica Asignar recursos para planificar

Puede asignar las máquinas virtuales descubiertas actualmente AWS Backup a un plan de respaldo nuevo o existente mediante la función Asignar recursos al plan.

Para asignar máquinas virtuales mediante la característica Asignar recursos para planificar:

1. En el panel de navegación izquierdo, elija Máquinas virtuales.
2. Seleccione la casilla de verificación situada junto al Nombre de máquina virtual para elegir todas las máquinas virtuales. También puede seleccionar la casilla de verificación situada junto a varios nombres de máquinas virtuales para asignarlas al mismo plan de copia de seguridad.
3. Seleccione Asignaciones y, a continuación, elija Asignar recursos para planificar.
4. Escriba un Nombre de asignación de recursos.
5. Elija una rol de IAM en la asignación de recursos para crear copias de seguridad y administrar los puntos de recuperación. Si no desea utilizar un rol de IAM específico, le recomendamos el Rol predeterminado, que tiene los permisos correctos.
6. En la sección Plan de copia de seguridad, elija un Plan de copia de seguridad existente de la lista desplegable. También puede elegir Crear plan de copia de seguridad para crear un plan nuevo.
7. Elija Asignar recursos.
8. De forma opcional, para comprobar que sus máquinas virtuales están asignadas a un plan de copia de seguridad, seleccione Ver plan de copia de seguridad. A continuación, en la sección Asignaciones de recursos, elija el Nombre de la asignación de recursos.

Asignación de máquinas virtuales mediante la característica Crear asignación de grupo

A diferencia de las dos funciones de asignación de recursos anteriores para máquinas virtuales, la función Crear asignación de grupos no solo asigna las máquinas virtuales detectadas actualmente AWS Backup, sino también las máquinas virtuales descubiertas en el futuro en una carpeta o hipervisor que defina.

Además, no tiene que seleccionar ninguna casilla de verificación para utilizar la característica Crear asignación de grupo.

Para asignar máquinas virtuales mediante la característica Asignar recursos para planificar:

1. En el panel de navegación izquierdo, elija Máquinas virtuales.

2. Elija Asignaciones y, a continuación, elija Crear asignación de grupo.
3. Escriba un Nombre de asignación de recursos.
4. Elija una rol de IAM en la asignación de recursos para crear copias de seguridad y administrar los puntos de recuperación. Si no desea utilizar un rol de IAM específico, le recomendamos el Rol predeterminado, que tiene los permisos correctos.
5. En la sección Grupo de recursos, seleccione el menú desplegable Tipo de grupo. Las opciones son Carpeta o Hipervisor.

    a. Elija Carpeta para asignar todas las máquinas virtuales de una carpeta en un hipervisor. Seleccione Nombre del grupo de carpetas, por ejemplo `datacenter/vm`, mediante el menú desplegable. También puede optar por incluir Subcarpetas.

    > **Note**
    >
    > Para realizar asignaciones basadas en carpetas, durante el proceso de detección, AWS Backup etiqueta las máquinas virtuales con la carpeta en la que las encuentra durante el proceso de detección. Si más adelante mueve una máquina virtual a una carpeta diferente, AWS Backup no podrá actualizar la etiqueta por usted debido a las prácticas recomendadas de AWS etiquetado. Este método de asignación puede dar lugar a que se sigan realizando copias de seguridad de las máquinas virtuales que haya sacado de la carpeta asignada.

    b. Elija Hipervisor para asignar todas las máquinas virtuales administradas por un hipervisor. Seleccione un Nombre del grupo de ID de hipervisor mediante el menú desplegable.
6. En la sección Plan de copia de seguridad, elija un Plan de copia de seguridad existente de la lista desplegable. También puede elegir Crear plan de copia de seguridad para crear un plan nuevo.
7. Elija Crear asignación de grupo.
8. De forma opcional, para comprobar que sus máquinas virtuales están asignadas a un plan de copia de seguridad, seleccione Ver plan de copia de seguridad. En la sección Asignaciones de recursos, elija el Nombre de la asignación de recursos.

Pasos siguientes

Para restaurar una máquina virtual, consulte Restauración de una máquina virtual mediante AWS Backup.

Información sobre componentes de origen de terceros para la puerta de enlace de copia de seguridad

En esta sección, encontrará información sobre las herramientas y licencias de terceros de las que dependemos para ofrecer la funcionalidad de puerta de enlace de copia de seguridad.

El código fuente de algunos componentes de software de código abierto que se incluyen con el software de la puerta de enlace de copia de seguridad se puede descargar en las siguientes ubicaciones:

- Para puertas de enlace implementadas en VMware ESXi, descargue sources.tzg.

Este producto incluye software desarrollado por el proyecto OpenSSL para su uso en el kit de herramientas OpenSSL (https://www.openssl.org/).

Este producto incluye software desarrollado por el VMware® vSphere Software Development Kit (https://www.vmware.com).

Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulte Licencias de terceros.

Componentes de código abierto para AWS Appliance

Se utilizan varias herramientas y licencias de terceros para ofrecer la funcionalidad de puerta de enlace de copia de seguridad.

Utilice los siguientes enlaces para descargar el código fuente de determinados componentes de software de código abierto que se incluyen con el software de Appliance: AWS

- Para gateways implementadas en VMware ESXi, descargue sources.tar

Este producto incluye software desarrollado por el proyecto OpenSSL para su uso en el kit de herramientas OpenSSL (https://www.openssl.org/). Para obtener las licencias pertinentes para todas las herramientas de terceros dependientes, consulte Licencias de terceros.

Solución de problemas de máquinas virtuales

Problemas y mensajes relacionados con copias de seguridad incrementales o CBT

Mensaje de error: **"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 este mensaje continúa, restablezca el CBT según las instrucciones de VMware.

Mensaje que indica que CBT no estaba activado o no estaba disponible: "VMware Change Block Tracking (CBT) was not available for this virtual machine, but the incremental backup was successfully completed with our proprietary change mechanism."

Asegúrese de que el CBT esté activado. Para comprobar si un disco virtual tiene CBT habilitado:

1. Abra vSphere Client y seleccione una máquina virtual apagada.
2. Haga clic con el botón derecho en la máquina virtual y vaya a Edit Settings > Options > Advanced/ General > Configuration Parameters.
3. La opción `ctkEnabled` debe ser `True`.

Si está activado, asegúrese de utilizar las funciones de VMware. up-to-date El host debe ser ESXi 4.0 o posterior y la máquina virtual propietaria de los discos a los que debe realizarse el seguimiento debe tener la versión de hardware 7 o posterior.

Si el CBT está activado (habilitado) y el software y el hardware están actualizados, apague la máquina virtual y vuelva a encenderla. Asegúrese de que el CBT esté activado. A continuación, vuelva a realizar la copia de seguridad.

Copia de seguridad avanzada de DynamoDB

AWS Backup admite funciones adicionales y avanzadas para sus necesidades de protección de datos en Amazon DynamoDB. Después AWS Backup de habilitar las funciones avanzadas en su Región de AWS, desbloqueará las siguientes funciones para todas las copias de seguridad de tablas de DynamoDB nuevas que cree:

- Ahorro de costos y optimización:
  - Organizar las copias de seguridad en niveles para almacenarlas en frío para reducir los costos de almacenamiento

  - Etiquetado de asignación de costos para su uso con Cost Explorer
- Continuidad empresarial:
  - Copia entre regiones
  - Copia entre cuentas
- Seguridad:
  - Guarde las copias de seguridad en almacenes de AWS Backup cifrados, que puede proteger con el Bloqueo de almacenes de AWS Backup, las políticas de AWS Backup y las claves de cifrado.
  - Las copias de seguridad heredan las etiquetas de sus tablas de DynamoDB de origen, lo que le permite utilizarlas para establecer permisos y políticas de control de servicios (SCP).

Los nuevos clientes que se incorporen AWS Backup después de noviembre de 2021 tienen las funciones avanzadas de copia de seguridad de DynamoDB habilitadas de forma predeterminada. En concreto, las características avanzadas de copia de seguridad de DynamoDB están habilitadas de forma predeterminada para los clientes que no hayan creado un almacén de copias de seguridad antes del 21 de noviembre de 2021.

Recomendamos a todos los AWS Backup clientes actuales que habiliten las funciones avanzadas de DynamoDB. Después de activar las características avanzadas, no hay diferencia en los precios del almacenamiento de copias de seguridad en caliente. Puede ahorrar dinero al organizar las copias de seguridad en niveles para almacenarlas en frío y optimizar sus costos mediante el uso de etiquetas de asignación de costos. También puede empezar a aprovechar las funciones de seguridad y continuidad empresarial AWS Backup de la empresa.

> **Note**
>
> Si utilizas un rol o una política personalizados en lugar AWS Backup del rol de servicio predeterminado, debes agregar o usar las siguientes políticas de permisos (o agregar sus permisos equivalentes) a tu rol personalizado:
>
> - `AWSBackupServiceRolePolicyForBackup` para realizar copias de seguridad avanzadas de DynamoDB.
> - `AWSBackupServiceRolePolicyForRestores` para restaurar copias de seguridad avanzadas de DynamoDB.

Para obtener más información sobre las políticas AWS administradas y ver ejemplos de políticas administradas por el cliente, consulte. Políticas gestionadas para AWS Backup

Temas

Habilitación de copias de seguridad avanzadas de DynamoDB mediante la consola

Puede activar las funciones AWS Backup avanzadas para las copias de seguridad de DynamoDB mediante la consola AWS Backup o DynamoDB.

Para activar las funciones avanzadas de copia de seguridad de DynamoDB desde la consola: AWS Backup

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el menú de navegación izquierdo, elija Configuración.
3. En la sección Servicios admitidos, compruebe que DynamoDB esté Habilitado.

   Si no es así, elija Activación y habilite DynamoDB como servicio admitido por AWS Backup .
4. En la sección Características avanzadas para copias de seguridad de DynamoDB, elija Habilitar.
5. Elija Enable features (Habilitar características).

Para obtener información sobre cómo habilitar las funciones AWS Backup avanzadas mediante la consola de DynamoDB, consulte AWS Backup Habilitación de funciones en la Guía del usuario de Amazon DynamoDB.

Habilitación de copias de seguridad avanzadas de DynamoDB mediante programación

También puede activar las funciones AWS Backup avanzadas para las copias de seguridad de DynamoDB mediante la AWS Command Line Interface (CLI). Para habilitar las copias de seguridad avanzadas de DynamoDB, debe establecer los dos valores siguientes en `true`:

Para habilitar mediante programación las funciones AWS Backup avanzadas de las copias de seguridad de DynamoDB:

1. Compruebe si ya ha activado las funciones AWS Backup avanzadas de DynamoDB mediante el siguiente comando:

   ```
   $ aws backup describe-region-settings
   ```

   Si `"DynamoDB":true` en `"ResourceTypeManagementPreference"` y `"ResourceTypeOptInPreference"`, ya ha habilitado la copia de seguridad avanzada de DynamoDB.

   Si, como en el siguiente resultado, tiene al menos una instancia de `"DynamoDB":false`, aún no ha habilitado la copia de seguridad avanzada de DynamoDB. Continúe con el siguiente paso.

   ```
   {
     "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. Utilice la siguiente operación `UpdateRegionSettings` para configurar `"ResourceTypeManagementPreference"` y `"ResourceTypeOptInPreference"` en `"DynamoDB":true`:

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

Edición de una copia de seguridad avanzada de DynamoDB

Al crear una copia de seguridad de DynamoDB después de AWS Backup activar las funciones avanzadas, puede utilizarla para: AWS Backup

- Copiar una copia de seguridad entre regiones
- Copiar una copia de seguridad entre cuentas
- Cambia el momento en el que se AWS Backup coloca una copia de seguridad en almacenamiento en frío
- Etiquetar la copia de seguridad

Para usar esas características avanzadas en una copia de seguridad existente, consulte Edición de una copia de seguridad.

Si más adelante deshabilita las funciones AWS Backup avanzadas de DynamoDB, podrá seguir realizando esas operaciones en las copias de seguridad de DynamoDB que haya creado durante el período en que activó las funciones avanzadas.

Restauración de una copia de seguridad avanzada de DynamoDB

Puede restaurar las copias de seguridad de DynamoDB realizadas AWS Backup con las funciones avanzadas habilitadas del mismo modo que restaura las copias de seguridad de DynamoDB realizadas antes de activar las funciones avanzadas. AWS Backup Puede realizar una restauración mediante DynamoDB AWS Backup o DynamoDB.

Puede especificar cómo cifrar la tabla recién restaurada con las siguientes opciones:

- Al restaurar en la misma región que la tabla original, si lo desea, puede especificar una clave de cifrado para la tabla restaurada. Si no especifica una clave de cifrado, AWS Backup cifrará automáticamente la tabla restaurada con la misma clave que cifró la tabla original.

- Al restaurar en una región diferente a la de la tabla original, debe especificar una clave de cifrado.

Para restaurar mediante AWS Backup, consulteRestauración de una tabla de Amazon DynamoDB.

Para restaurar con DynamoDB, consulte Restoring a DynamoDB table from a backup en la Guía del usuario de Amazon DynamoDB.

Eliminación de una copia de seguridad avanzada de DynamoDB

No puede eliminar las copias de seguridad creadas mediante estas características avanzadas de DynamoDB. Debe utilizar AWS Backup para eliminar las copias de seguridad a fin de mantener la coherencia global en todo su entorno de AWS .

Para eliminar una copia de seguridad de DynamoDB, consulte Eliminación de copias de seguridad.

Otros beneficios de la administración completa de AWS Backup cuando se habilita la copia de seguridad avanzada de DynamoDB

Al habilitar las funciones AWS Backup avanzadas de DynamoDB, proporciona una administración completa de las copias de seguridad de DynamoDB a. AWS Backup Al hacer esto, obtendrá los siguientes beneficios adicionales:

Cifrado

AWS Backup cifra automáticamente las copias de seguridad con la clave KMS del almacén de destino. AWS Backup Antes, se cifraban con el mismo método de cifrado que la tabla de DynamoDB de origen. Esto aumenta el número de defensas que puede utilizar para proteger sus datos. Para obtener más información, consulte Cifrado de copias de seguridad en AWS Backup.

Nombre de recurso de Amazon (ARN)

El espacio de nombres de servicio de cada ARN de copia de seguridad es `awsbackup`. Antes, el espacio de nombres de servicio era `dynamodb`. Dicho de otro modo, el principio de cada ARN cambiará de `arn:aws:dynamodb` a `arn:aws:backup`. Consulte los ARN de AWS Backup en la Referencia de autorización de servicios.

Con este cambio, usted o su administrador de copias de seguridad pueden crear políticas de acceso para las copias de seguridad mediante el espacio de nombres de servicio `awsbackup` que ahora se aplica a las copias de seguridad de DynamoDB creadas después de activar las características

avanzadas. Al utilizar el espacio de nombres de servicio `awsbackup`, también puede aplicar políticas a otras copias de seguridad realizadas por AWS Backup. Para obtener más información, consulte Control de acceso.

Ubicación de los cargos en el extracto de facturación

Los cargos por copias de seguridad (incluidos el almacenamiento, las transferencias de datos, las restauraciones y la eliminación anticipada) aparecen en la sección «Respaldo» de tu AWS factura. Antes, los cargos aparecían en la sección “DynamoDB” de la factura.

Este cambio garantiza que puedas utilizar la AWS Backup facturación para supervisar de forma centralizada los costes de las copias de seguridad. Para obtener más información, consulte Medición, costos y facturación.

Copias de seguridad de Amazon Timestream

Amazon Timestream es una base de datos de serie temporal escalable que permite almacenar y analizar hasta billones de puntos de datos de serie temporal por día. Timestream se ha optimizado para ahorrar costos y tiempo, ya que mantiene los datos recientes en la memoria y almacena los datos históricos en un nivel de almacenamiento con costos optimizados de acuerdo con sus políticas.

Una base de datos de Timestream tiene tablas. Estas tablas contienen registros y cada registro es un único punto de datos de una serie temporal. Una serie temporal es una secuencia de registros registrados durante un intervalo de tiempo, como el precio de una acción, el nivel de uso de la memoria de una instancia Amazon EC2 o una lectura de temperatura. AWS Backup puede realizar copias de seguridad y restaurar de forma centralizada las tablas de Timestream. Puede copiar estas copias de seguridad de las tablas a otras cuentas y a varias más Regiones de AWS de la misma organización.

Actualmente, Timestream no ofrece servicios nativos de copia de seguridad y restauración, por lo que AWS Backup utilizarlos para crear copias seguras de las tablas de Timestream puede añadir un nivel adicional de seguridad y resiliencia a sus recursos.

Copia de seguridad de tablas de Timestream

Puede hacer copias de seguridad de las tablas de Timestream a través de la consola o mediante. AWS Backup AWS CLI

Hay dos formas de utilizar la AWS Backup consola para hacer copias de seguridad de una tabla de Timestream: a pedido o como parte de un plan de copia de seguridad.

Creación de copias de seguridad de Timestream bajo demanda

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y Crear copia de seguridad bajo demanda.
3. En la página Crear copia de seguridad bajo demanda, elija Amazon Timestream.
4. Elija el Tipo de recurso Timestream y, a continuación, elija el nombre de la tabla de la que desea hacer una copia de seguridad.
5. En la ventana de copia de seguridad, asegúrese de que Crear copia de seguridad ahora esté seleccionado. De esta manera, se inicia una copia de seguridad de inmediato y puede ver antes los clústeres en la página Recursos protegidos.
6. En el menú desplegable Transferir al almacenamiento en frío, puede configurar los ajustes de transferencia.
7. En Periodo de retención, puede elegir durante cuánto tiempo desea conservar la copia de seguridad.
8. Elija un almacén de copias de seguridad existente o cree uno nuevo. Al elegir Create new backup vault (Crear nuevo almacén de copias de seguridad) se abre una nueva página para crear un almacén y a continuación, vuelve a la página Create on-demand backup (Crear copia de seguridad bajo demanda) cuando termine.
9. En Función de IAM, selecciona Función predeterminada (si la función AWS Backup predeterminada no está presente en tu cuenta, se creará automáticamente con los permisos correctos).
10. Si lo desea, puede agregar etiquetas a su punto de recuperación. Si desea asignar una o varias etiquetas a su copia de seguridad bajo demanda, introduzca una key (clave) y un value (valor) opcional y elija Add tag (Añadir etiqueta).
11. Seleccione Create on-demand backup (Crear copia de seguridad bajo demanda). Esto le lleva a la página Jobs (Trabajos), donde verá una lista de trabajos.
12. Elija el ID de trabajo de copia de seguridad del clúster para ver los detalles de ese trabajo. Mostrará un estado de `Completed`, `In Progress` o `Failed`. Haga clic en el botón de actualización para actualizar el estado.

Creación de copias de seguridad programadas de Timestream en un plan de copia de seguridad

Las copias de seguridad programadas pueden incluir tablas de Timestream si son un recurso protegido. Para optar por la protección de las tablas de Amazon Timestream:

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos.
3. Mueva a la posición de activación el conmutador de Amazon Timestream.
4. Consulte Asignación de recursos mediante la consola para incluir las tablas de Timestream en un plan nuevo o existente.

En Administrar planes de copia de seguridad, puede elegir crear un plan de copia de seguridad e incluir tablas de Timestream o actualizar uno existente para que incluya tablas de Timestream. Al agregar el tipo de recurso Timestream, puede optar por agregar Todas las tablas de Timestream o marcar las casillas situadas junto a las tablas que desee agregar en Seleccionar tipos de recursos específicos.

La primera copia de seguridad que se haga con tablas de Timestream será una copia de seguridad completa. Las copias de seguridad posteriores serán copias de seguridad incrementales.

Una vez que haya creado o modificado su plan de copia de seguridad, vaya a Planes de copia de seguridad en el menú de navegación de la izquierda. El plan de copia de seguridad que especificó debe mostrar sus clústeres en Asignaciones de recursos.

Copia de seguridad mediante programación

También puede utilizar la operación denominada `start-backup-job`. Incluya los siguientes parámetros:

```
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 Región de AWS \
--endpoint-url URL
```

Visualización de las copias de seguridad de las tablas de Timestream

Para ver y modificar las copias de seguridad de las tablas de Timestream en la consola:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Elija Almacenes de Backup. A continuación, haga clic en el nombre del almacén de copias de seguridad que contiene las tablas de Timestream.

3. El almacén de copias de seguridad mostrará un resumen y una lista de copias de seguridad.

   a. Puede hacer clic en el enlace de la columna ID de punto de recuperación, o

   b. Puede marcar la casilla situada a la izquierda del ID de punto de recuperación y hacer clic en Acciones para eliminar los puntos de recuperación que ya no sean necesarios.

Restauración de una tabla de Timestream

Consulte cómo restaurar una tabla de Timestream.

Copia de seguridad de bases de datos de SAP HANA en instancias de Amazon EC2

> **Note**
>
> Servicios compatibles con Región de AWScontiene las regiones compatibles actualmente en las que están disponibles las copias de seguridad de bases de datos de SAP HANA en instancias de Amazon EC2.

AWS Backup admite copias de seguridad y restauraciones de bases de datos de SAP HANA en instancias de Amazon EC2.

Temas

- Descripción general de las bases de datos de SAP HANA con AWS Backup
- Requisitos previos para realizar copias de seguridad de las bases de datos de SAP HANA mediante AWS Backup
- Operaciones de backup de SAP HANA en la consola AWS Backup
- Vea las copias de seguridad de bases de datos de SAP
- Úselo AWS CLI para las bases de datos de SAP HANA con AWS Backup
- Solución de problemas de backup de bases de datos de SAP HANA
- Glosario de términos de SAP HANA utilizados AWS Backup
- AWS Backup soporte de bases de datos de SAP HANA en instancias EC2: notas de la versión

Descripción general de las bases de datos de SAP HANA con AWS Backup

Además de la capacidad de crear copias de seguridad y restaurar bases de datos, la integración de AWS Backup con Amazon EC2 Systems Manager for SAP permite a los clientes identificar y etiquetar las bases de datos de SAP HANA.

AWS Backup está integrado con AWS Backint Agent para realizar copias de seguridad y restauraciones de SAP HANA. Para obtener más información, consulte AWS Backint.

Requisitos previos para realizar copias de seguridad de las bases de datos de SAP HANA mediante AWS Backup

Se deben cumplir varios requisitos previos antes de poder realizar las actividades de copia de seguridad y restauración. Tenga en cuenta que necesitará acceso administrativo a su base de datos de SAP HANA y permisos para crear nuevas funciones y políticas de IAM en su AWS cuenta para llevar a cabo estos pasos.

Complete estos requisitos previos en Amazon EC2 Systems Manager.

1. Configure los permisos necesarios para la instancia de Amazon EC2 que ejecute la base de datos de SAP HANA
2. Registre las credenciales en AWS Secrets Manager
3. Instale AWS Backint y AWS Systems Manager para los agentes de SAP
4. Verifique el agente SSM
5. Verifique los parámetros
6. Registre la base de datos de SAP HANA

Se recomienda registrar cada instancia de HANA solo una vez. Los registros múltiples pueden generar varios ARN para la misma base de datos. Mantener un único ARN y registro simplifica la creación y el mantenimiento del plan de respaldo y también puede ayudar a reducir la duplicación no planificada de copias de seguridad.

Operaciones de backup de SAP HANA en la consola AWS Backup

Una vez cumplidos los requisitos previos y el SSM para las configuraciones de SAP, puede realizar copias de seguridad y restaurar sus bases de datos de SAP HANA en EC2.

Activación de la protección de los recursos de SAP HANA

Para poder utilizar SAP HANA AWS Backup para proteger sus bases de datos de SAP HANA, SAP HANA debe estar activado como uno de los recursos protegidos. Para ello:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Configuración.
3. En Activación del servicio, seleccione Configurar recursos.
4. Active SAP HANA en Amazon EC2.
5. Haga clic en Confirmar.

La suscripción del servicio para SAP HANA en Amazon EC2 ahora estará habilitada.

Cree una copia de seguridad programada de las bases de datos de SAP HANA

Puede editar un plan de copia de seguridad existente y agregarle recursos de SAP HANA, o puede crear un nuevo plan de copia de seguridad solo para los recursos de SAP HANA.

Si decide crear un nuevo plan de copia de seguridad, tendrá tres opciones:

1. Opción 1: comience con una plantilla
    1. Elija una plantilla de plan de copia de seguridad.
    2. Especifique un nombre de plan de copia de seguridad.
    3. Haga clic en Crear plan.
2. Opción 2: cree un plan nuevo
    1. Especifique un nombre de plan de copia de seguridad.
    2. Si lo desea, especifique las etiquetas que se agregarán al plan de copia de seguridad.
    3. Especifique la configuración de la regla de copia de seguridad.
        a. Especifique un nombre para la regla de copia de seguridad.
        b. Seleccione un almacén de copias de seguridad existente o cree uno nuevo. Aquí es donde se guardan las copias de seguridad.
        c. Especifique la frecuencia de las copias de seguridad.
        d. Especifique un intervalo de copia de seguridad.

Tenga en cuenta que actualmente no se admite la transferencia al almacenamiento en frío.

e. Especifique el periodo de retención.

Actualmente no se admite la copia al destino

f. (Opcional) Especifique las etiquetas que desee agregar a los puntos de recuperación.

4. Haga clic en Crear plan.

3. Opción 3: defina un plan con JSON

1. Para especificar el JSON de su plan de copia de seguridad, modifique la expresión JSON de un plan de copia de seguridad existente o cree una nueva expresión.
2. Especifique un nombre de plan de copia de seguridad.
3. Haga clic en Validar JSON.

Una vez que el plan de copia de seguridad se haya creado correctamente, puede asignar recursos al plan de copia de seguridad en el siguiente paso.

Sea cual sea el plan que utilice, asegúrese de asignar recursos. Puede elegir qué bases de datos de SAP HANA desea asignar, incluidas bases de datos del sistema y de inquilinos. También tiene la opción de excluir ID de recursos concretos.

Cree una copia de seguridad bajo demanda de las bases de datos de SAP HANA

Puede crear una copia de seguridad completa bajo demanda que se ejecute inmediatamente después de su creación. Tenga en cuenta que las copias de seguridad bajo demanda de las bases de datos de SAP HANA en instancias de Amazon EC2 son copias de seguridad completas; no se admiten copias de seguridad incrementales.

La copia de seguridad bajo demanda ya está creada. Comenzará a hacer copias de seguridad de los recursos especificados. La consola lo llevará a la página de Trabajos de copia de seguridad, donde podrá ver el progreso del trabajo. Tome nota del identificador del trabajo de copia de seguridad en el banner azul situado en la parte superior de la pantalla, ya que lo necesitará para encontrar fácilmente el estado del trabajo de copia de seguridad. Cuando se complete la copia de seguridad, el estado pasará a `Completed`. Las copias de seguridad pueden tardar varias horas.

Actualice la Lista de trabajos de copia de seguridad para ver el cambio de estado. También puede buscar y hacer clic en el ID de trabajo de copia de seguridad para ver el estado detallado del trabajo.

Copias de seguridad continuas de las bases de datos de SAP HANA

Puede realizar copias de seguridad continuas, que se pueden utilizar con la point-in-time restauración (PITR) (tenga en cuenta que las copias de seguridad bajo demanda conservan los recursos en el estado en que se utilizan, mientras que la PITR utiliza copias de seguridad continuas que registran los cambios a lo largo de un período de tiempo).

Con las copias de seguridad continuas, puede restaurar su base de datos de SAP HANA en una instancia EC2 devolviéndola al momento específico que elija, con una precisión de 1 segundo (retrocediendo un máximo de 35 días). La copia de seguridad continua consiste en crear primero una copia de seguridad completa del recurso y, a continuación, realizar copias de seguridad constantes de los registros de transacciones del recurso. La restauración mediante PITR funciona accediendo a la copia de seguridad completa y reproduciendo el registro de transacciones hasta el momento indicado para su recuperación. AWS Backup

Puede optar por realizar copias de seguridad continuas al crear un plan de copias de seguridad AWS Backup mediante la AWS Backup consola o la API.

Para habilitar las copias de seguridad continuas desde la consola

1. Inicie sesión en la AWS Management Console AWS Backup consola y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación principal, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En Reglas de copia de seguridad, elija Agregar regla de copia de seguridad.
4. En la sección Configuración de regla de copia de seguridad, seleccione Habilitar copias de seguridad continuas para los recursos compatibles.

Tras deshabilitar el PITR (point-in-timerestauración) para las copias de seguridad de las bases de datos de SAP HANA, se seguirán enviando los registros AWS Backup hasta que caduque el punto de recuperación (el estado es igual a`EXPIRED`). Puede cambiar a una ubicación alternativa de copia de seguridad de registros en SAP HANA para detener la transmisión de registros a AWS Backup.

Un punto de recuperación continuo con un estado igual a `STOPPED` indica que se ha interrumpido un punto de recuperación continuo; es decir, los registros transmitidos desde SAP HANA a AWS

Backup ese punto muestran los cambios incrementales en una base de datos que presentan un vacío. Los puntos de recuperación que se producen dentro de este lapso de tiempo tienen un estado de `STOPPED`..

Para ver los problemas que pueden surgir durante los trabajos de restauración de copias de seguridad continuas (puntos de recuperación), consulte la sección de solución Solución de problemas de restauración de SAP HANA de esta guía.

Vea las copias de seguridad de bases de datos de SAP

Consulte el estado de los trabajos de copia de seguridad:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, seleccione Trabajos.
3. Elija trabajos de copia de seguridad, trabajos de restauración o trabajos de copia para ver la lista de sus trabajos.
4. Busque el ID del trabajo y haga clic en él para ver los estados detallados de los trabajos.

Consulte todos los puntos de recuperación de un almacén:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. Busque un almacén de copias de seguridad y haga clic en él para ver todos los puntos de recuperación dentro del almacén.

Consulte los detalles de los recursos protegidos:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Protected resources (Recursos protegidos).
3. También puede filtrar por tipo de recurso para ver todas las copias de seguridad de ese tipo de recurso.

Úselo AWS CLI para las bases de datos de SAP HANA con AWS Backup

Cada acción de la consola de copia de seguridad tiene una llamada a la API correspondiente.

Para configurar AWS Backup y gestionar sus recursos mediante programación, utilice la llamada `StartBackupJob`a la API para hacer una copia de seguridad de una base de datos de SAP HANA en una instancia EC2.

Utilice `start-backup-job` como el comando de la CLI.

Solución de problemas de backup de bases de datos de SAP HANA

Si encuentra errores durante su flujo de trabajo, consulte los siguientes ejemplos de errores y las soluciones sugeridas:

Requisitos previos de Python

- Error: error de Zypper relacionado con la versión de Python desde SSM para SAP y requiere AWS Backup Python 3.6, pero SUSE 12 SP5 es compatible de forma predeterminada con Python 3.4.

  Solución: instale varias versiones de Python en SUSE12 SP5 siguiendo estos pasos:

  1. Ejecute un comando update-alternatives para crear un enlace simbólico para Python 3 en '/usr/local/bin/' en lugar de usar directamente '/usr/bin/python3'. Estos comandos establecerán Python 3.4 como la versión por defecto. El comando es: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.4 5`
  2. Añada Python 3.6 a la configuración de alternativas ejecutando el siguiente comando: `# sudo update-alternatives –install /usr/local/bin/python3 python3 /usr/bin/python3.6 2`
  3. Cambie la configuración alternativa a Python 3.6 ejecutando el siguiente comando: `# sudo update-alternatives –config python3`

     Debería mostrarse el siguiente resultado:

     ```
     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. Introduzca el número correspondiente a Python 3.6.
  5. Compruebe la versión de Python y confirme que se está utilizando Python 3.6.

6. (Opcional, pero recomendado) Comprueba que los comandos de Zypper funcionen según lo esperado.

Amazon EC2 Systems Manager para descubrimiento y registro de SAP

- Error: SSM para SAP no pudo detectar la carga de trabajo debido al bloqueo del acceso a un punto final público para AWS Secrets Manager el SSM.

  Solución: compruebe si se puede acceder a los puntos finales desde su base de datos de SAP HANA. Si no se puede acceder a ellos, puede crear puntos de enlace de Amazon VPC para SAP AWS Secrets Manager y SSM para SAP.

  1. Pruebe el acceso a Secrets Manager desde el host Amazon EC2 para HANA DB ejecutando el siguiente comando:. `aws secretsmanager get-secret-value –secret-id hanaeccsbx_hbx_database_awsbkp` Si el comando no devuelve un valor, el firewall bloquea el acceso al punto final del servicio Secrets Manager. El registro se detendrá en el paso «Recuperación de secretos de Secrets Manager».
  2. Ejecute el comando para probar la conectividad con el terminal SSM para SAP. `aws ssm-sap list-registration` Si el comando no devuelve un valor, el firewall bloquea el acceso al punto final SSM for SAP.

     Ejemplo de error:`Connection was closed before we received a valid response from endpoint URL: “https://ssm-sap.us-west-2.amazonaws.com/register-application"`.

  Hay dos opciones para continuar si no se puede acceder a los puntos finales.

  - Abra los puertos del firewall para permitir el acceso al punto final del servicio público para Secrets Manager y SSM para SAP; o
  - Cree puntos de conexión de VPC para Secrets Manager y SSM para SAP y, a continuación:
    - Asegúrese de que Amazon VPC esté habilitado para DNSSupport y DNSHostName.
    - Asegúrese de que su punto de conexión de VPC haya habilitado la opción Permitir nombre de DNS privado.
    - Si la detección de SSM para SAP se completó correctamente, el registro mostrará que se ha descubierto el host.
- Error: AWS Backup y la conexión de Backint falla debido al bloqueo del acceso a los puntos finales públicos AWS Backup del servicio. `aws-backint-agent.log`puede mostrar errores similares a este: `time="2024-01-03T11:39:15-08:00" level=error msg="Storage`

`configuration validation failed: missing backup data plane Id"` o. `level=fatal msg="Error performing backup missing backup data plane Id` Además, la AWS Backup consola puede mostrar `Fatal Error: An internal error occured.`

Resolución: hay dos opciones para proceder si no se puede acceder a los puntos finales:

- Abra los puertos del firewall para permitir el acceso a los puntos finales de servicio público (HTTPS). Una vez utilizada esta opción, el DNS resolverá las solicitudes a AWS los servicios a través de direcciones IP públicas.
- Cree puntos finales de VPC que dirija de forma privada el tráfico hacia y desde los AWS servicios necesarios para ello. AWS Backup Una vez utilizada esta opción, el DNS resolverá las solicitudes de esos servicios a través de direcciones IP privadas. Esta opción puede requerir actualizaciones en el servidor DNS para agregar reglas que reenvíen las solicitudes a los puntos finales privados.

- Error: el registro de SSM para SAP falla debido a que la contraseña de HANA contiene caracteres especiales. Los ejemplos de errores pueden incluir `Error connecting to database HBX/HBX when validating its credentials.` o `Discovery failed because credentials for HBX/SYSTEMDB either not provided or cannot be validated.` después de probar una conexión utilizando `hdbsql systemdb` y `tenantdb` que se probó desde una instancia Amazon EC2 de la base de datos HANA.

  En la AWS Backup consola de la página de trabajos, los detalles del trabajo de respaldo pueden mostrar el estado del `FAILED` error`Miscellaneous: b’* 10: authentication failed SQLSTATE: 28000\n’`.

  Solución: asegúrese de que la contraseña no contenga caracteres especiales, como $.

- Error: **`b’* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time...`**

  Solución: es posible que la instalación del AWS BackInt agente para SAP HANA no se haya completado correctamente. Vuelva a intentar el proceso para implementar el AWS Backint Agent y el agente Amazon EC2 Systems Manager en el servidor de aplicaciones SAP.

- Error: la consola no coincide con los archivos de registro tras el registro.

  El registro de detección muestra un error de registro al intentar conectarse a HANA DB debido a que la contraseña contiene caracteres especiales, aunque la consola SSM para SAP Application Manager para SAP indica que el registro se ha realizado correctamente. No confirma que el

registro se haya realizado correctamente. Si la consola muestra un registro correcto pero los registros no, las copias de seguridad fallarán.

Confirme el estado del registro:

1. Inicie sesión en la consola SSM
2. Seleccione Ejecutar comando en el panel de navegación de la izquierda.
3. En el campo de textoInstance ID:Equal:, introduzca el historial de comandos con un valor igual al de la instancia que utilizó para el registro. Esto filtrará el historial de comandos.
4. Usa la columna de identificador de comandos para buscar comandos con estadoFailed. A continuación, busque el nombre del documento de AWSSystemsManagerSAP-Discovery.
5. En AWS CLI, ejecute el comandoaws ssm-sap register-application status. Si aparece el valor devueltoError, significa que el registro no se ha realizado correctamente.

Solución: asegúrese de que su contraseña de HANA no contenga caracteres especiales (como '$').

Crear una copia de seguridad de una base de datos de SAP HANA

- Error: AWS Backup la consola muestra el mensaje «Error grave» cuando se crea una copia de seguridad bajo demanda para SystemDB o TenantDB. Esto ocurre porque no se puede acceder al terminal público cell-1.prod.us-west-2.storage.cryo.aws.a2z.com. Esto se debe a un firewall del lado del cliente que bloquea el acceso a este punto final.

  aws-backint-agent.logpuede mostrar errores como level=error msg="Storage configuration validation failed: missing backup data plane Id" o level=fatal msg="Error performing backup missing backup data plane Id."

  Solución: abra el acceso mediante firewall al terminal público cell-1.prod.us-west-2.storage.cryo.aws.a2z.com.

- **Database cannot be backed up while it is stopped**Error:.

  Solución: asegúrese de que la base de datos de la que se va a hacer la copia de seguridad esté activa. Solo se puede hacer una copia de seguridad de los datos y registros de la base de datos cuando la base de datos está en línea.

- Error: Getting backup metadata failed. Check the SSM document execution for more details.

Solución: asegúrese de que la base de datos de la que se va a hacer la copia de seguridad esté activa. Solo se puede hacer una copia de seguridad de los datos y registros de la base de datos cuando la base de datos está en línea.

Supervisión de los registros de respaldo

- Error: `Encountered an issue with log backups, please check SAP HANA for details.`

  Solución: compruebe SAP HANA para asegurarse de que las copias de seguridad de los registros se envían AWS Backup desde SAP HANA.
- Error: `One or more log backup attempts failed for recovery point.`

  Solución: consulte SAP HANA para obtener más información. Asegúrese de que las copias de seguridad de los registros se envíen AWS Backup desde SAP HANA.
- Error: `Unable to determine the status of log backups for recovery point.`

  Solución: consulte SAP HANA para obtener más información. Asegúrese de que las copias de seguridad de los registros se envíen AWS Backup desde SAP HANA.
- Error: `Log backups for recovery point %s were interrupted due to a restore operation on the database.`

  Solución: espere a que se complete el trabajo de restauración. Las copias de seguridad de los registros deberían reanudarse.

Glosario de términos de SAP HANA utilizados AWS Backup

Tipos de copias de seguridad de datos: SAP HANA admite dos tipos de copias de seguridad de datos: completas e INC (incrementales). AWS Backup optimiza el tipo que se utiliza durante cada operación de respaldo.

Copias de seguridad del catálogo: SAP HANA mantiene su propio manifiesto denominado catálogo. AWS Backup interactúa con este catálogo. Cada nueva copia de seguridad creará una entrada en el catálogo.

Copia de seguridad continua de registros (registros de transacciones): para las funciones de recuperación en un momento dado (PITR), SAP HANA hace un seguimiento de todas las transacciones a partir de la copia de seguridad más reciente.

Copia del sistema: un trabajo de restauración en el que la base de datos de destino de la restauración es diferente de la base de datos de origen a partir de la cual se creó el punto de recuperación.

Restauración destructiva: una restauración destructiva es un tipo de trabajo de restauración durante el cual una base de datos restaurada elimina o sobrescribe la base de datos de origen o existente.

COMPLETA: una copia de seguridad completa es una copia de seguridad completa de una base de datos.

INC: una copia de seguridad incremental es una copia de seguridad de todos los cambios en una base de datos de SAP HANA desde la copia de seguridad anterior.

Para obtener más información, consulte el Glosario de AWS.

AWS Backup soporte de bases de datos de SAP HANA en instancias EC2: notas de la versión

Algunas funcionalidades no son compatibles en este momento:

- No se admiten copias entre cuentas ni entre regiones.
- No se admite Backup Audit Manager ni la generación de informes.
- Servicios compatibles con Región de AWScontiene las regiones actualmente compatibles para las copias de seguridad de bases de datos de SAP HANA en instancias de Amazon EC2.

Copias de seguridad de Amazon Redshift

Amazon Redshift es un almacenamiento de datos en la nube escalable y completamente administrado que acelera el tiempo necesario para obtener información mediante análisis rápidos, fáciles y seguros. Puede utilizarla AWS Backup para proteger sus almacenes de datos con copias de seguridad inmutables, políticas de acceso independientes y una gestión organizativa centralizada de las tareas de copia de seguridad y restauración.

Un almacén de datos de Amazon Redshift es un conjunto de recursos informáticos denominados nodos, que se organizan en un grupo denominado clúster. AWS Backup puede hacer copias de seguridad de estos clústeres.

Para obtener información sobre Amazon Redshift, consulte la Guía de introducción de Amazon Redshift, la Guía para desarrolladores de bases de datos de Amazon Redshift y la Guía de administración de clústeres de Amazon Redshift.

Copia de seguridad de clústeres aprovisionados de Amazon Redshift

Puede proteger sus clústeres de Amazon Redshift mediante la AWS Backup consola o mediante programación mediante API o CLI. Se pueden hacer copias de seguridad de estos clústeres de forma periódica como parte de un plan de copia de seguridad. También se pueden realizar copias de seguridad según sea necesario mediante copias de seguridad bajo demanda.

Puede restaurar una sola tabla (lo que también se conoce como restauración a nivel de elemento) o un clúster completo. Tenga en cuenta que no se pueden hacer copias de seguridad de las tablas por sí mismas; se hacen copias de seguridad de las tablas como parte de un clúster cuando se hace una copia de seguridad del clúster.

AWS Backup El uso le permite ver sus recursos de forma centralizada; sin embargo, si Amazon Redshift es el único recurso que utiliza, puede seguir utilizando el programador automático de instantáneas de Amazon Redshift. Tenga en cuenta que no podrá seguir gestionando la configuración manual de las instantáneas con Amazon Redshift si decide gestionarla a través de. AWS Backup

Puede hacer copias de seguridad de los clústeres de Amazon Redshift a través de la AWS Backup consola o mediante. AWS CLI

Hay dos formas de utilizar la AWS Backup consola para hacer copias de seguridad de un clúster de Amazon Redshift: a pedido o como parte de un plan de copias de seguridad.

Creación de copias de seguridad de Amazon Redshift bajo demanda

Consulte la página Creación de una copia de seguridad bajo demanda para obtener más información.

Para crear una instantánea manual, deje sin marcar la casilla de verificación de copia de seguridad continua cuando cree un plan de copia de seguridad que incluya recursos de Amazon Redshift.

Creación de copias de seguridad programadas de Amazon Redshift en un plan de copia de seguridad

Las copias de seguridad programadas pueden incluir clústere de Amazon Redshift si son un recurso protegido. Para optar por la protección de las tablas de Amazon Redshift:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos.
3. Mueva a la posición de activación el conmutador de Amazon Redshift.
4. Consulte Asignación de recursos mediante la consola para incluir los clústeres de Amazon Redshift en un plan nuevo o existente.

En Administrar planes de copia de seguridad, puede elegir crear un plan de copia de seguridad e incluir clústeres de Amazon Redshift o actualizar uno existente para que incluya clústeres de Amazon Redshift. Al agregar el tipo de recurso Amazon Redshift, puede optar por agregar Todos los clústeres de Amazon Redshift o marcar las casillas situadas junto a los clústeres.

Copia de seguridad mediante programación

También puede definir su plan de respaldo en un documento JSON y proporcionarlo mediante la AWS Backup consola o AWS CLI. Consulte Crear planes de respaldo mediante un documento JSON y la AWS Backup CLI para obtener información sobre cómo crear un plan de respaldo mediante programación.

Puede realizar las siguientes operaciones mediante la API:

- Iniciar un trabajo de copia de seguridad
- Describir un trabajo de copia de seguridad
- Obtener los metadatos de los puntos de recuperación
- Enumerar los puntos de recuperación por recursos
- Enumerar las etiquetas para el punto de recuperación

Visualización de copias de seguridad de los clústeres de Amazon Redshift

Para ver y modificar las copias de seguridad de las tablas de Amazon Redshift en la consola:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Elija Almacenes de Backup. A continuación, haga clic en el nombre del almacén de copias de seguridad que contiene los clústeres de Amazon Redshift.
3. El almacén de copias de seguridad mostrará un resumen y una lista de copias de seguridad. Puede hacer clic en el enlace de la columna ID de punto de recuperación.

4. Para eliminar uno o más puntos de recuperación, marque las casillas que desea eliminar. En el botón Acciones, puede seleccionar Eliminar.

Restauración de un clúster de Amazon Redshift

Para obtener más información, consulte Restauración de un clúster de Amazon Redshift.

Copias de seguridad de Amazon Relational Database Service

Amazon RDS y AWS Backup

Cuando considere las opciones para realizar copias de seguridad de sus instancias y clústeres de Amazon RDS, es importante que aclare qué tipo de copia de seguridad desea crear y utilizar. Varios AWS recursos, incluido Amazon RDS, ofrecen sus propias soluciones de backup nativas.

Amazon RDS ofrece la opción de realizar copias de seguridad automáticas y copias de seguridad manuales. En la terminología de Amazon RDS, todos los puntos de recuperación creados por AWS Backup, incluidos los de un plan de respaldo, están considerando realizar copias de seguridad manuales.

Cuando crea una copia de seguridad (punto de recuperación) de una instancia de Amazon RDS, AWS Backup comprueba si ha utilizado anteriormente Amazon RDS para crear una copia de seguridad automática. AWS Backup Si existe una copia de seguridad automática, AWS Backup crea una copia de esta instantánea (`copy-db-snapshot`operación). Si no existe ninguna copia de seguridad existente, AWS Backup crea una instantánea de la instancia que usted indique, en lugar de una copia (`create-db-snapshot`operación).

La primera instantánea creada por AWS Backup cualquiera de las dos operaciones dará como resultado una instantánea completa. Todas las copias subsiguientes serán copias de seguridad incrementales, siempre que exista la copia de seguridad completa.

> **Important**
>
> Cuando un plan de AWS Backup backup está programado para crear varias instantáneas diarias de una instancia de Amazon RDS y cuando una de esas ventanas de Start AWS Backup Backup programadas coincide con la ventana Amazon RDS Backup, el linaje de datos de las copias de seguridad puede ramificarse en copias de seguridad no idénticas, lo que crea copias de seguridad no planificadas y conflictivas. Para evitarlo, asegúrese de

que su plan AWS Backup de respaldo o la ventana de Amazon RDS no coincidan en sus horarios.

Backups continuos de Amazon RDS y restauración puntual

Las copias de seguridad continuas implican AWS Backup crear una copia de seguridad completa de su recurso de Amazon RDS y, a continuación, capturar todos los cambios en un registro de transacciones. Puede lograr una mayor granularidad si retrocede hasta el punto en el que desea realizar la restauración, en lugar de elegir una instantánea anterior tomada en intervalos de tiempo fijos.

Consulte las copias de seguridad continuas y los servicios compatibles con el PITR y la administración de la configuración de las copias de seguridad continuas para obtener más información.

Copias de seguridad en varias zonas de disponibilidad de Amazon RDS

AWS Backup realiza copias de seguridad y es compatible con las opciones de implementación Multi-AZ (zona de disponibilidad) de Amazon RDS for MySQL y PostgreSQL con una instancia de base de datos principal y dos en espera legibles.

Las copias de seguridad en varias zonas de disponibilidad están disponibles en las siguientes regiones: Asia-Pacífico (Sídney), Asia-Pacífico (Tokio), Europa (Irlanda), Este de EE. UU. (Ohio),Oeste de EE. UU. (Oregón),Europa (Estocolmo), Asia-Pacífico (Singapur), Este de EE. UU. (Norte de Virginia) y Europa (Fráncfort).

La opción de implementación Multi-AZ optimiza las transacciones de escritura y es ideal cuando las cargas de trabajo requieren capacidad de lectura adicional, menor latencia de las transacciones de escritura, mayor resiliencia ante la inestabilidad de la red (que afecta a la coherencia de la latencia de las transacciones de escritura) y alta disponibilidad y durabilidad.

Para crear un clúster Multi-AZ, puede elegir MySQL o PostgreSQL como tipo de motor.

En la AWS Backup consola, hay tres opciones de implementación:

- Clúster de base de datos Multi-AZ: crea un clúster de base de datos con una instancia de base de datos principal y dos instancias de base de datos en espera legibles, cada una de las cuales se encuentra en una zona de disponibilidad diferente. Proporciona alta disponibilidad y redundancia de datos y aumenta la capacidad para cargas de trabajo preparadas para el servidor.

- Clúster de base de datos Multi-AZ: crea una instancia de base de datos principal y una instancia de base de datos en espera en una zona de disponibilidad diferente. Esto proporciona alta disponibilidad y redundancia de datos, pero la instancia de base de datos en espera no admite conexiones para cargas de trabajo de lectura.
- Instancia de base de datos única: crea una instancia de base de datos única sin ninguna instancia de base de datos en espera.

Para crear una copia de seguridad para Amazon RDS, consulte Creación de una copia de seguridad para programar una copia de seguridad como parte de sus planes de copia de seguridad o crear una copia de seguridad bajo demanda.

> **Note**
>
> La recuperación en un momento dado (PITR) puede admitir instancias, pero no clústeres. No se admite la copia de una instantánea de un clúster de base de datos Multi-AZ.

Diferencias entre un clúster Multi-AZ y una instancia de RDS

Una copia de seguridad en una sola zona de disponibilidad o en dos zonas de disponibilidad es una instancia de RDS; una implementación y una copia de seguridad con tres o más instancias es un clúster, de forma similar a los clústeres de Amazon Aurora, Amazon Neptune y Amazon DocumentDB.

El ARN (nombre de recurso de Amazon) se representa de forma diferente en función de si se utiliza la instancia o el clúster:

Un ARN de instancia de RDS: `arn:aws:rds:`*`region`*`: `*`account`*`:db:`*`name`*

Un clúster de varias zonas de disponibilidad de RDS: `arn:aws:rds:`*`region`*`:`*`account`*`:cluster:`*`name`*

Para obtener más información, consulte Implementaciones de clústeres de base de datos Multi-AZ en la Guía del usuario de Amazon RDS.

Para obtener más información, sobre la Creación de una instantánea de un clúster de base de datos Multi-AZ en la Guía del usuario de Amazon RDS.

AWS CloudFormation apile copias de seguridad

Una CloudFormation pila consta de varios recursos con y sin estado de los que puede hacer copias de seguridad como una sola unidad. En otras palabras, puede hacer copias de seguridad y restaurar una aplicación que contenga varios recursos al hacer una copia de seguridad de una pila y restaurar los recursos que contiene. Todos los recursos de una pila se definen por la plantilla de AWS CloudFormation de la pila.

Cuando se hace una copia de seguridad de una CloudFormation pila, se crean puntos de recuperación para la CloudFormation plantilla y para cada recurso adicional compatible con AWS Backup la pila. Estos puntos de recuperación se agrupan dentro de un punto de recuperación global denominado compuesto.

Este punto de recuperación compuesto no se puede restaurar, pero los puntos de recuperación anidados sí se pueden restaurar. Puede restaurar desde una hasta todas las copias de seguridad anidadas dentro de una copia de seguridad compuesta mediante la consola o la AWS CLI.

CloudFormation terminología de pila de aplicaciones

- Punto de recuperación compuesto: un punto de recuperación que se utiliza para agrupar puntos de recuperación anidados, así como otros metadatos.
- Punto de recuperación anidado: punto de recuperación de un recurso que forma parte de una CloudFormation pila y del que se hace una copia de seguridad como parte del punto de recuperación compuesto. Cada punto de recuperación anidado pertenece a la pila de un punto de recuperación compuesto.
- Trabajo compuesto: trabajo de respaldo, copia o restauración de una CloudFormation pila que puede activar otros trabajos de respaldo para los recursos individuales de la pila.
- Trabajo anidado: trabajo de respaldo, copia o restauración de un recurso de una AWS CloudFormation pila.

CloudFormation apilar tareas de copia de seguridad

El proceso de creación de una copia de seguridad se denomina trabajo de copia de seguridad. Un trabajo de backup CloudFormation apilado tiene un estado. Cuando un trabajo de copia de seguridad ha finalizado, tiene el estado `Completed`. Esto significa que se ha creado un AWS CloudFormation punto de recuperación (copia de seguridad).

CloudFormation Se puede hacer una copia de seguridad de las pilas mediante la consola o mediante programación. Para hacer una copia de seguridad de cualquier recurso, incluida una CloudFormation pila, consulta Cómo crear una copia de seguridad en otra parte de esta guía AWS Backup para desarrolladores.

CloudFormation Se puede hacer una copia de seguridad de las pilas mediante el comando `StartBackupJob` de la API. Tenga en cuenta que la documentación y la consola hacen referencia a puntos de recuperación compuestos y anidados; el lenguaje de la API utiliza la terminología “puntos de recuperación principales y secundarios” en la misma relación contextual.

CloudFormation las pilas contienen todos los AWS recursos indicados en tu plantilla. CloudFormation Tenga en cuenta que es posible que la plantilla contenga recursos que aún no son compatibles con AWS Backup. Si la plantilla contiene una combinación de recursos AWS compatibles y recursos no compatibles, AWS Backup seguirá haciendo una copia de seguridad de la plantilla en una pila compuesta, pero Backup solo creará puntos de recuperación de los servicios compatibles con Backup. Todos los tipos de recursos incluidos en la CloudFormation plantilla se incluirán en la copia de seguridad, incluso si no ha optado por un servicio en particular (cambiando un servicio a «Activado» en la configuración de la consola). Las copias de seguridad anidadas (puntos de recuperación) compatibles con AWS Backup se pueden restaurar, pero no es posible respaldar ni restaurar las pilas anidadas.

AWS CloudFormation punto de recuperación

Estado del punto de recuperación

Cuando finaliza el trabajo de copia de seguridad de una pila (el estado del trabajo es `Completed`), se ha creado una copia de seguridad de la pila. Esta copia de seguridad también se conoce como punto de recuperación compuesto. Un punto de recuperación compuesto puede tener uno de los siguientes estados: `Completed`, `Failed` o`Partial`. Tenga en cuenta que un trabajo de copia de seguridad tiene un estado, y un punto de recuperación (también denominado copia de seguridad) también tiene un estado diferente.

Un trabajo de respaldo completado significa que toda su pila y los recursos que contiene están protegidos por AWS Backup. Un estado de error indica que el trabajo de copia de seguridad no se realizó correctamente; debe volver a crear la copia de seguridad una vez que se haya corregido el problema que provocó el error.

Un estado `Partial` significa que no se realizó una copia de seguridad de todos los recursos de la pila. Esto puede ocurrir si la CloudFormation plantilla contiene recursos que actualmente no son

compatibles AWS Backup con ellos o si uno o más de los trabajos de respaldo que pertenecen a los recursos de la pila (recursos anidados) tienen un estado diferente al siguiente. `Completed` Puede crear manualmente una copia de seguridad bajo demanda para volver a ejecutar cualquier recurso cuyo estado no sea `Completed`. Si esperaba que la pila tuviera el estado de `Completed`, pero en su lugar aparece marcado como `Partial`, compruebe cuál de las condiciones anteriores podría aplicarse a su pila.

Cada recurso anidado dentro del punto de recuperación compuesto tiene su propio punto de recuperación individual, cada uno con su propio estado (`Completed` o `Failed`). Es posible restaurar los puntos de recuperación anidados con un estado de `Completed`.

Administración de los puntos de recuperación

Los puntos de recuperación compuestos (copias de seguridad) se pueden copiar; los puntos de recuperación anidados se pueden copiar, eliminar, disociar o restaurar. No se puede eliminar un punto de recuperación compuesto que contenga copias de seguridad anidadas. Una vez eliminados o disociados los puntos de recuperación anidados dentro de un punto de recuperación compuesto, puede eliminar manualmente el punto de recuperación compuesto o dejar que permanezca hasta que se elimine durante el ciclo de vida del plan de copia de seguridad.

Eliminación de un punto de recuperación

Puede eliminar un punto de recuperación mediante la AWS Backup consola o mediante el. AWS CLI

Para eliminar puntos de recuperación mediante la AWS Backup consola,

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Haga clic en Recursos protegidos en el menú de navegación de la izquierda. En el cuadro de texto, escriba `CloudFormation` para que se muestren solo las CloudFormation pilas.
3. Los puntos de recuperación compuestos se mostrarán en el panel Puntos de recuperación. Puede hacer clic en el signo más (+) situado a la izquierda del identificador de cada punto de recuperación para ampliar cada punto de recuperación compuesto y mostrar todos los puntos de recuperación anidados que contiene el compuesto. Puede marcar la casilla situada a la izquierda de cualquier punto de recuperación para incluirlo en la selección de puntos de recuperación que desee eliminar.
4. Haga clic en el botón Eliminar.

Si utiliza la consola para eliminar uno o más puntos de recuperación compuestos, aparecerá un cuadro de advertencia. Este cuadro de advertencia requiere que confirme su intención de eliminar

los puntos de recuperación compuestos, incluidos los puntos de recuperación anidados dentro de las pilas compuestas.

Para eliminar puntos de recuperación mediante la API, use el comando `DeleteRecoveryPoint`.

Si utilizas la API con la, AWS Command Line Interface debes eliminar todos los puntos de recuperación anidados antes de eliminar un punto compuesto. Si envía una solicitud a la API para eliminar una copia de seguridad de pila compuesta (punto de recuperación) que aún contiene puntos de recuperación anidados, la solicitud devolverá un error.

Disociación de un punto de recuperación anidado del punto de recuperación compuesto

Puede disociar un punto de recuperación anidado de un punto de recuperación compuesto (por ejemplo, desea conservar el punto de recuperación anidado pero eliminar el punto de recuperación compuesto). Ambos puntos de recuperación permanecerán, pero dejarán de estar conectados; es decir, las acciones que se realicen en el punto de recuperación compuesto dejarán de aplicarse al punto de recuperación anidado una vez que se haya disociado.

Puede disociar el punto de recuperación mediante la consola o puede llamar a la API `DisassociateRecoveryPointFromParent`. [Tenga en cuenta que las llamadas a la API utilizan el término “principal” para referirse a los puntos de recuperación compuestos].

Copia de un punto de recuperación

Puede copiar un punto de recuperación compuesto o puede copiar un punto de recuperación anidado si el recurso admite la copia entre cuentas y regiones.

Para copiar los puntos de recuperación mediante la consola: AWS Backup

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Haga clic en Recursos protegidos en el menú de navegación de la izquierda. En el cuadro de texto, escriba `CloudFormation` para que se muestren solo las CloudFormation pilas.
3. Los puntos de recuperación compuestos se mostrarán en el panel Puntos de recuperación. Puede hacer clic en el signo más (+) situado a la izquierda del identificador de cada punto de recuperación para ampliar cada punto de recuperación compuesto y mostrar todos los puntos de recuperación anidados que contiene el compuesto. Puede hacer clic en el botón circular de opción situado a la izquierda de cualquier punto de recuperación para copiarlo.
4. Una vez seleccionado, haga clic en el botón Copiar de la esquina superior derecha del panel.

Al copiar un punto de recuperación compuesto, los puntos de recuperación anidados que no admiten la función de copia no se incluirán en la pila copiada. El punto de recuperación compuesto tendrá un estado de `Partial`.

Preguntas frecuentes

1. “¿Qué se incluye como parte de la copia de seguridad de la aplicación?”

   Como parte de cada copia de seguridad de una aplicación definida mediante ella CloudFormation, se hace una copia de seguridad de la plantilla, del valor procesado de cada parámetro de la plantilla y de los recursos anidados AWS Backup compatibles con ella. Se hace una copia de seguridad de un recurso anidado de la misma manera que se hace una copia de seguridad de un recurso individual que no forma parte de una CloudFormation pila. Tenga en cuenta que no se realizará una copia de seguridad de los valores de los parámetros marcados como `no-echo`.

2. «¿Puedo hacer una copia de seguridad de mi AWS CloudFormation pila que tiene pilas anidadas?»

   Sí. Las CloudFormation pilas que contienen pilas anidadas pueden estar en la copia de seguridad.

3. “¿Un estado *`Partial`* significa que se ha producido un error al crear mi copia de seguridad?”

   No. Un estado parcial indica que se realizó una copia de seguridad de algunos puntos de recuperación, pero no de otros. Hay tres condiciones que debe comprobar si esperaba un resultado `Completed` de la copia de seguridad:

   a. ¿Su CloudFormation pila contiene recursos que actualmente no son compatibles? AWS Backup Para ver una lista de los recursos compatibles, consulta los AWS recursos compatibles y las aplicaciones de terceros en nuestra Guía para desarrolladores.

   b. Uno o más de los trabajos de copia de seguridad pertenecientes a recursos de la pila no se ha realizado correctamente y hay que volver a ejecutarlo.

   c. Se eliminó o disoció un punto de recuperación anidado del punto de recuperación compuesto.

4. «¿Cómo excluyo los recursos de la copia de seguridad de mi CloudFormation pila?»

   Al hacer una copia de seguridad de la CloudFormation pila, puede excluir los recursos para que no formen parte de la copia de seguridad. En la consola, durante los procesos de creación de un plan de copia de seguridad y actualización de un plan de copia de seguridad, hay un paso de asignación de recursos. En este paso, hay una sección de Selección de recurso. Si eliges

incluir tipos de recursos específicos y los has incluido CloudFormation como recurso para realizar una copia de seguridad, puedes excluir los ID de recursos específicos de los tipos de recursos seleccionados. También puede utilizar etiquetas para excluir recursos de la pila.

Mediante la CLI, puede utilizar

- `NotResources`en tu plan de respaldo para excluir un recurso específico de tus CloudFormation pilas.
- `StringNotLike` para excluir elementos mediante etiquetas.

5. “¿Qué tipos de copias de seguridad son compatibles con los recursos anidados?”

   Las copias de seguridad de los recursos anidados pueden ser copias de seguridad completas o incrementales, según el tipo de copia de seguridad que admitan AWS Backup estos recursos. Para obtener más información, consulte Funcionamiento de las copias de seguridad incrementales. Sin embargo, tenga en cuenta que los recursos anidados de Amazon S3 y Amazon RDS no admiten PITR (point-in-time restauración).

6. «¿Se hace una copia de seguridad de los conjuntos de cambios que forman parte de la CloudFormation pila?»

   ¡No!. Los conjuntos de cambios no se respaldan como parte de la copia de seguridad de la CloudFormation pila.

7. «¿Cómo afecta el estado de la AWS CloudFormation pila a la copia de seguridad?»

   El estado de la CloudFormation pila puede afectar a la copia de seguridad. Se puede hacer una copia de seguridad de una pila con un estado que incluya `COMPLETE`, como los estados `CREATE_COMPLETE`, `ROLLBACK_COMPLETE`, `UPDATE_COMPLETE`, `UPDATE_ROLLBACK_COMPLETE`, `IMPORT_COMPLETE` o `IMPORT_ROLLBACK_COMPLETE`.

   En caso de que se produzca un error al cargar una plantilla nueva y la pila pase al estado `ROLLBACK_COMPLETE`, se realizará una copia de seguridad de la nueva plantilla, pero las copias de seguridad de los recursos anidados se basarán en los recursos revertidos.

8. “¿En qué se diferencian los ciclos de vida de las pilas de aplicaciones de los ciclos de vida de otros puntos de recuperación?”

   Los ciclos de vida de los puntos de recuperación anidados vienen determinados por el plan de copia de seguridad al que pertenecen. El punto de recuperación compuesto está determinado por

el ciclo de vida más largo de todos los puntos de recuperación anidados. Cuando el último punto de recuperación anidado restante dentro de un punto de recuperación compuesto se elimina o se disocia, también se eliminará el punto de recuperación compuesto.

9. «¿Cómo se CloudFormation copian las etiquetas de un objeto a los puntos de recuperación?»

   Sí. Esas etiquetas se copiarán en cada punto de recuperación anidado respectivo.

10. "¿Hay un orden para eliminar puntos de recuperación compuestos y anidados (copias de seguridad)?"

    Sí. Algunas copias de seguridad deben eliminarse antes de poder eliminar otras. Las copias de seguridad compuestas que contienen puntos de recuperación anidados no se pueden eliminar hasta que se hayan eliminado todos los puntos de recuperación del compuesto. Una vez que un punto de recuperación compuesto ya no contiene puntos de recuperación anidados, puede eliminarlo manualmente. De lo contrario, se eliminará de acuerdo con el ciclo de vida de su plan de copia de seguridad.

Restauración de aplicaciones dentro de una pila

Consulte Cómo restaurar copias de seguridad de pilas de aplicaciones para obtener información sobre la restauración de puntos de recuperación anidados.

Creación de copias de seguridad de Windows VSS

Con AWS Backup, puede realizar copias de seguridad y restaurar aplicaciones Windows habilitadas para VSS (Volume Shadow Copy Service) que se ejecuten en instancias de Amazon EC2. Si la aplicación tiene un grabador VSS registrado en Windows VSS, AWS Backup crea una instantánea que sea coherente con esa aplicación.

Puede realizar restauraciones consistentes y, al mismo tiempo, usar el mismo servicio de respaldo administrado que se usa para proteger otros AWS recursos. Con las copias de seguridad de Windows coherentes con la aplicación en EC2, obtiene la misma configuración de coherencia y conocimiento de la aplicación que las herramientas de copia de seguridad tradicionales.

> **Note**
>
> AWS Backup actualmente, solo admite copias de seguridad consistentes con las aplicaciones de los recursos que se ejecutan en Amazon EC2, específicamente escenarios

de respaldo en los que los datos de la aplicación se pueden restaurar sustituyendo una instancia existente por una nueva creada a partir de la copia de seguridad. No todos los tipos de instancia o aplicaciones son compatibles con las copias de seguridad de Windows VSS.

Para obtener más información, consulte Creación de una instantánea coherente con las aplicaciones de VSS en la Guía del usuario de Amazon EC2.

Para realizar copias de seguridad y restaurar los recursos de Windows habilitados para VSS que ejecutan Amazon EC2, siga estos pasos para completar las tareas previas requeridas. Para obtener instrucciones, consulte Antes de empezar en la Guía del usuario de Amazon EC2 para instancias de Windows.

1. Descargue, instale y configure el agente SSM en. AWS Systems Manager Este paso es necesario. Para obtener instrucciones, consulte Uso del agente SSM en instancias de Amazon EC2 para Windows Server en la Guía del usuario AWS de Systems Manager.
2. Agregue una política de IAM al rol de IAM y asocie el rol a la instancia de Amazon EC2 antes de realizar la copia de seguridad de Windows VSS (Volume Shadow Copy Service). Para obtener instrucciones, consulte Creación de un rol de IAM para instantáneas con VSS en la Guía del usuario de Amazon EC2. Para ver una política de IAM de ejemplo, consulte Políticas gestionadas para AWS Backup.
3. Descargue e instale los componentes de VSS para la instancia de Windows en Amazon EC2.
4. Habilite VSS en: AWS Backup
    1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
    2. En el panel, elija el tipo de copia de seguridad que desea crear, ya sea Crear una copia de seguridad bajo demanda o Administrar planes de Backup. Proporcione la información necesaria para el tipo de copia de seguridad.
    3. Cuando asigne recursos, elija EC2. Actualmente, solo se admiten copias de seguridad de Windows VSS en instancias EC2.
    4. En la sección Configuración avanzada, elija Windows VSS. Esto le permite realizar copias de seguridad de Windows VSS coherentes con la aplicación.
    5. Cree su copia de seguridad.

Un trabajo de copia de seguridad con un estado `Completed` no garantiza que la parte de VSS se realice correctamente; la inclusión de VSS se realiza sobre la base del mejor esfuerzo. Siga

los siguientes pasos para determinar si una copia de seguridad es coherente con la aplicación, coherente ante bloqueos o no ha tenido éxito:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En Mi cuenta, en el menú de navegación de la izquierda, haz clic en Trabajos.
3. Un estado `Completed` indica que el trabajo se ha realizado correctamente y es coherente con la aplicación (VSS).

   Un estado `Completed with issues` indica que la operación de VSS ha tenido errores, por lo que solo se ha realizado correctamente una copia de seguridad coherente ante bloqueos. Este estado también tendrá un mensaje emergente `"Windows VSS Backup Job Error encountered, trying for regular backup"`.

   Si la copia de seguridad no se realizó correctamente, el estado será `Failed`.
4. Para ver detalles adicionales del trabajo de copia de seguridad, haga clic en el trabajo individual. Por ejemplo, los detalles pueden indicar `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`.

Las copias de seguridad habilitadas para VSS con un destino que no sea Windows o que no sea un componente de VSS (Windows) que funcione correctamente serán consistentes en caso de bloqueos sin VSS.

Instancias de Amazon EC2 no compatibles

Los siguientes tipos de instancias de Amazon EC2 no son compatibles con las copias de seguridad de Windows habilitadas para VSS porque son instancias pequeñas y es posible que no realicen la copia de seguridad correctamente.

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Amazon EBS y AWS Backup

El proceso de copia de seguridad de los recursos de Amazon EBS es similar a los pasos que se utilizan para realizar copias de seguridad de otros tipos de recursos:

- Creación de una copia de seguridad bajo demanda
- Creación de una copia de seguridad programada

En las siguientes secciones se indica información específica de recursos.

Nivel de archivo de Amazon EBS para almacenamiento en frío

EBS es uno de los recursos que admiten la transición de copias de seguridad a almacenamiento en frío. Para obtener más información, consulte Ciclo de vida y niveles de almacenamiento.

> **Note**
>
> Esta función no está disponible en las regiones de China (Pekín), China (Ningxia), (EEUU-Este) y AWS GovCloud AWS GovCloud (EEUU-Oeste).

Copias de seguridad de varios volúmenes de Amazon EBS y coherentes ante bloqueos

De forma predeterminada, AWS Backup crea copias de seguridad coherentes con los bloqueos de los volúmenes de Amazon EBS que están conectados a una instancia de Amazon EC2. La coherencia ante bloqueos significa que las instantáneas de cada volumen de Amazon EBS asociado a la misma instancia de Amazon EC2 se toman exactamente en el mismo momento. Ya no tiene que detener sus instancias ni coordinar varios volúmenes de Amazon EBS para garantizar que el estado de su aplicación sea coherente ante bloqueos.

Dado que las instantáneas de varios volúmenes y compatibles con los bloqueos son una AWS Backup funcionalidad predeterminada, no necesita hacer nada diferente para utilizar esta función. Puede hacer copias de seguridad de los volúmenes de Amazon EBS mediante uno de los siguientes procedimientos:

La función utilizada para crear un punto de recuperación de instantáneas de EBS se asociará a esa instantánea. Esta misma función debe usarse para eliminar los puntos de recuperación que haya creado o para hacer la transición de los puntos de recuperación de la misma a un nivel de archivo.

Amazon EBS Snapshot Lock y AWS Backup

AWS Backup Las instantáneas de Amazon EBS gestionadas y las instantáneas asociadas a una AMI de AWS Backup Amazon EC2 gestionada que tengan aplicado el bloqueo de instantáneas de Amazon EBS no se pueden eliminar como parte del ciclo de vida del punto de recuperación si la duración del bloqueo de instantáneas supera el ciclo de vida de la copia de seguridad. Por el contrario, estos puntos de recuperación tendrán el estado de `EXPIRED`. Estos puntos de recuperación se pueden eliminar manualmente si decide eliminar primero el bloqueo de instantáneas de Amazon EBS.

Restauración de recursos de Amazon EBS

Para restaurar los volúmenes de Amazon EBS, siga los pasos que se indican en Restauración de un volumen de Amazon EBS.

Copia de etiquetas en copias de seguridad

En general, AWS Backup copia las etiquetas de los recursos que protege a sus puntos de recuperación. Para obtener más información sobre cómo copiar etiquetas durante una restauración, consulte Copia de etiquetas durante una restauración.

Por ejemplo, cuando hace una copia de seguridad de un volumen de Amazon EC2, AWS Backup copia sus etiquetas de recursos individuales y grupales en la instantánea resultante, de acuerdo con lo siguiente:

- Para obtener una lista de permisos específicos de recursos que son necesarios para guardar etiquetas de metadatos en copias de seguridad, consulte Permisos necesarios para asignar etiquetas a copias de seguridad.
- Las etiquetas que se asociaron originalmente a un recurso y las etiquetas que se asignaron durante la copia de seguridad se asignan a los puntos de recuperación almacenados en una bóveda de respaldo, hasta un máximo de 50 (esta es una AWS limitación). Las etiquetas asignadas durante la copia de seguridad tienen prioridad y ambos conjuntos de etiquetas se copian en orden alfabético.
- DynamoDB no admite la asignación de etiquetas a las copias de seguridad a menos que habilite primero la Copia de seguridad avanzada de DynamoDB.
- Los volúmenes de Amazon EBS que se asocian a las instancias de Amazon EC2 son recursos anidados. Las etiquetas de los volúmenes de Amazon EBS que se adjuntan a las instancias de Amazon EC2 son etiquetas anidadas. AWS Backup hace todo lo posible por copiar las etiquetas

anidadas, pero si no lo consigue, crea una copia de seguridad sin ellas y muestra el estado completado.

- Cuando una copia de seguridad de Amazon EC2 crea un punto de recuperación de imágenes y un conjunto de instantáneas, AWS Backup copia las etiquetas en la AMI resultante. AWS Backup también hace todo lo posible por copiar las etiquetas de los volúmenes asociados a la instancia de Amazon EC2 a las instantáneas resultantes.

Si copia la copia de seguridad en otra Región de AWS, AWS Backup copia todas las etiquetas de la copia de seguridad original en el destino. Región de AWS

Detención de un trabajo de copia de seguridad

Puede detener un trabajo de copia de seguridad una AWS Backup vez iniciado. Al hacerlo, la copia de seguridad no se crea y el registro del trabajo de copia de seguridad se conserva con el estado aborted (anulado).

Para detener un trabajo de copia de seguridad mediante la AWS Backup consola

1. Inicie sesión en la AWS Management Console AWS Backup consola y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación de la izquierda, elija Jobs (Trabajos).
3. Elija el trabajo de copia de seguridad que desea detener.
4. En el panel de detalles del trabajo de copia de seguridad, elija Stop (Detener).

Copia de una copia de seguridad

Para la mayoría de los tipos de recursos, puede copiar las copias de seguridad Regiones de AWS en varias Cuentas de AWS copias de seguridad, a pedido o automáticamente como parte de un plan de copias de seguridad programadas. Para obtener información específica, consultethe section called “Disponibilidad de características por recurso”.

También puede automatizar una secuencia de copias entre cuentas y entre regiones para la mayoría de los recursos compatibles, excepto Amazon RDS y Aurora. Para las instantáneas de Amazon RDS y Aurora, AWS Backup solo admite la automatización de copias entre cuentas o entre regiones debido a la forma en que esos servicios crean sus claves de cifrado (no se admite la copia de una instantánea de un clúster de base de datos Multi-AZ).

Algunos tipos de recursos tienen capacidades de copia de seguridad continua y copia entre regiones y entre cuentas. Cuando se realiza una copia entre regiones o entre cuentas de una copia de seguridad continua, el punto de recuperación copiado (copia de seguridad) se convierte en una copia de seguridad de instantánea (periódica). Según el tipo de recurso, las instantáneas pueden ser una copia incremental o una copia completa. La PITR (restauración en un momento dado) no está disponible para estas copias.

Las copias conservan su configuración de origen, incluidas las fechas de creación y el período de retención. La fecha de creación se refiere al momento en que se creó la fuente, no al momento en que se creó la copia.

NOTA: La configuración del origen tiene prioridad sobre la configuración de vencimiento de la copia, incluso si la copia está configurada para que no venza nunca; una copia que se haya configurado para que no venza nunca conservará la fecha de vencimiento del origen.

Si desea que la nueva copia de seguridad no venza nunca, configure las copias de seguridad de origen para que nunca venzan o especifique que la nueva copia venza 100 años después de su creación.

Contenido

Crear copias de seguridad en Regiones de AWS

Con él AWS Backup, puede copiar copias de seguridad Regiones de AWS en varias copias de seguridad a pedido o automáticamente como parte de un plan de copias de seguridad programado. La replicación entre regiones resulta especialmente útil si hay requisitos de continuidad del negocio o de conformidad que exigen que las copias de seguridad deben almacenarse a una distancia mínima de los datos de producción. Para ver un tutorial de vídeo, consulte Managing cross-Region copies of backups.

Cuando copia una copia de seguridad en una nueva Región de AWS por primera vez, AWS Backup copia la copia de seguridad completa. En general, si un servicio admite copias de seguridad incrementales, las copias posteriores de esa copia de seguridad incluidas en el mismo Región de AWS serán incrementales. AWS Backup volverá a cifrar su copia con la clave gestionada por el cliente de su almacén de destino.

Una excepción es Amazon EBS, que establece que si se cambia el estado de cifrado de una instantánea durante una operación de copia, se obtiene una copia completa (no incremental).

Requisitos

- La mayoría AWS Backup de los recursos compatibles admiten copias de seguridad entre regiones. Para obtener información detallada, consulte Disponibilidad de características por recurso.
- La mayoría de AWS las regiones admiten copias de seguridad entre regiones. Para obtener información detallada, consulte Disponibilidad de las funciones por Región de AWS.
- AWS Backup no admite copias entre regiones para su almacenamiento en capas frías.

Consideraciones sobre la copia entre regiones con recursos específicos

Amazon RDS

No puede copiar un grupo de opciones a otro Región de AWS. Si lo intentas, puede aparecer un error como el siguiente: «La instantánea requiere un grupo de opciones de destino con las siguientes opciones:...»

Debe introducir los mismos grupos de opciones en el destino Región de AWS al crear una nueva copia entre regiones de una instantánea de Amazon RDS.

Realización de copias de seguridad entre regiones bajo demanda

Para replicar una copia de seguridad existente bajo demanda

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Elija Almacenes de Backup.
3. Elija el almacén que contenga el punto de recuperación que desee copiar.
4. En la sección Copias de seguridad, seleccione el punto de recuperación que desee copiar.
5. Con el botón desplegable Acciones, elija Copiar.
6. Escriba los siguientes valores:

   Copiar al destino

   Elija el destino Región de AWS de la copia. Puede agregar una nueva regla a cada copia que se realice en un nuevo destino.

Almacén de copias de seguridad de destino

Elija el almacén de copia de seguridad de destino de la copia.

Transferir al almacenamiento en frío

Elija cuándo realizar la transferencia de una copia de la copia de seguridad al almacenamiento en frío. Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Este valor no se puede modificar una vez que la copia se ha migrado al almacenamiento en frío.

Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla Disponibilidad de características por recurso. La expresión de almacenamiento en frío se omite para otros recursos.

Periodo de retención

Especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío. El periodo de retención Siempre conserva la copia indefinidamente.

Rol de IAM

Elija la función de IAM que AWS Backup se utilizará al crear la copia. El rol también debe AWS Backup figurar como entidad de confianza, lo que AWS Backup permite asumirlo. Si selecciona Predeterminado y el rol AWS Backup predeterminado no está presente en su cuenta, se le creará uno con los permisos correctos.

7. Elija Copiar.

Programación de la copia de seguridad entre regiones

Puede utilizar un plan de copia de seguridad programadas para copiar las copias de seguridad en Regiones de AWS.

Para copiar una copia de seguridad mediante un plan de copia de seguridad programadas

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En Mi cuenta, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.
3. En la página Crear plan de copia de seguridad, elija Crear un nuevo plan.

4. En Nombre del plan de copia de seguridad, introduzca un nombre para su plan de copia de seguridad.
5. En la sección Configuración de regla de copia de seguridad, agregue una regla de copia de seguridad que defina una programación de copia de seguridad, un intervalo de copia de seguridad y reglas de ciclo de vida. Puede agregar más reglas de copia de seguridad más adelante.

   a. En Nombre, ingrese un nombre para la regla.

   b. Para Almacén de copia de seguridad, elija un almacén de la lista. Los puntos de recuperación de esta copia de seguridad se guardarán en este almacén. También puede crear un almacén de copias de seguridad nuevo.

   c. En Frecuencia de copia de seguridad, elija la frecuencia con la que desea realizar copias de seguridad.

   d. Para los servicios compatibles con el PITR, si desea utilizar esta función, seleccione Habilitar las copias de seguridad continuas para la point-in-time recuperación (PITR). Para ver una lista de los servicios que admiten la PITR, consulta esa sección de la tabla Disponibilidad de características por recurso.

   e. En Intervalo de copia de seguridad, elija Usar valores predeterminados de intervalo de copia de seguridad (recomendado). Puede personalizar el intervalo de copia de seguridad.

   f. En Copiar en el destino, elija la Región de AWS de destino de la copia de la copia de seguridad. La copia de seguridad se copiará en esta región. Puede agregar una nueva regla a cada copia que se realice en un nuevo destino. A continuación, ingrese los siguientes valores:

      Copiar en el almacén de otra cuenta

      No active esta opción. Para obtener más información sobre la copia multicuenta, consulta Cómo crear copias de seguridad en varias cuentas Cuentas de AWS

      Almacén de copias de seguridad de destino

      Elija el almacén de copias de seguridad de la región de destino donde se AWS Backup copiará la copia de seguridad.

      Si desea crear un nuevo almacén de copias de seguridad para realizar copias entre regiones, elija Crear nuevo almacén de copia de seguridad. Ingrese la información en el asistente. A continuación, elija Crear almacén de copia de seguridad.

6. Elija Crear plan.

Crear copias de seguridad en todas partes Cuentas de AWS

Con él AWS Backup, puede realizar copias de seguridad de hasta varias Cuentas de AWS copias a pedido o automáticamente como parte de un plan de copias de seguridad programado. Utilice una copia de seguridad multicuenta si desea copiar sus copias de seguridad de forma segura a una o más personas Cuentas de AWS de su organización por motivos operativos o de seguridad. Si la copia de seguridad original se elimina accidentalmente, puede copiar la copia de seguridad de su cuenta de destino a su cuenta de origen y, a continuación, iniciar la restauración. Para poder hacerlo, debe tener dos cuentas que pertenezcan a la misma organización en el servicio AWS Organizations . Para obtener más información, consulte Tutorial: Creación y configuración de una organización en la Guía del usuario de Organizations.

En su cuenta de destino, debe crear un almacén de copias de seguridad. A continuación, debe asignar una clave gestionada por el cliente para cifrar las copias de seguridad en la cuenta de destino y una política de acceso basada en los recursos para permitir el acceso AWS Backup a los recursos que desee copiar. En la cuenta de origen, si sus recursos están cifrados con una clave administrada por el cliente, debe compartir esta clave con la cuenta de destino. A continuación, puede crear un plan de copia de seguridad y elegir una cuenta de destino que forme parte de su unidad organizativa en AWS Organizations.

Al copiar una copia de seguridad en varias cuentas por primera vez, la AWS Backup copia de seguridad completa. En general, si un servicio admite copias de seguridad incrementales, las copias posteriores de esa copia de seguridad en la misma cuenta son incrementales. AWS Backup vuelve a cifrar la copia con la clave gestionada por el cliente de la bóveda de destino.

Requisitos

- Antes de administrar los recursos Cuentas de AWS en varias entradas AWS Backup, sus cuentas deben pertenecer a la misma organización del AWS Organizations servicio.
- La mayoría de los recursos compatibles AWS Backup admiten la copia de seguridad entre cuentas. Para obtener información detallada, consulte Disponibilidad de características por recurso.
- La mayoría de AWS las regiones admiten la copia de seguridad entre cuentas. Para obtener información detallada, consulte Disponibilidad de las funciones por Región de AWS.
- AWS Backup no admite copias multicuenta para su almacenamiento en niveles inactivos.

Configuración de la copia de seguridad entre cuentas

¿Qué necesita para crear copias de seguridad entre cuentas?

- Una cuenta de origen

  La cuenta de origen es la cuenta en la que residen AWS los recursos de producción y las copias de seguridad principales.

  El usuario de la cuenta de origen inicia la operación de copia de seguridad entre cuentas. El usuario o rol de la cuenta de origen debe tener los permisos de API adecuados para iniciar la operación. Los permisos adecuados pueden ser la política AWS gestionada`AWSBackupFullAccess`, que permite el acceso total a AWS Backup las operaciones, o una política gestionada por el cliente que permite realizar acciones como`ec2:ModifySnapshotAttribute`: Para obtener más información sobre los tipos de políticas, consulte Políticas administradas por AWS Backup.
- Una cuenta de destino

  La cuenta de destino es la cuenta en la que desea guardar una copia de su copia de seguridad. Puede elegir más de una cuenta de destino. La cuenta de destino debe estar en la misma organización que la cuenta de origen en AWS Organizations.

  Debe “permitir” la política de acceso `backup:CopyIntoBackupVault` para su almacén de copias de seguridad de destino. La ausencia de esta política impedirá los intentos de copia en la cuenta de destino.
- Una cuenta de administración en AWS Organizations

  La cuenta de administración es la cuenta principal de su organización, tal como la define AWS Organizations, que se utiliza para administrar las copias de seguridad entre cuentas entre sus Cuentas de AWS. Para utilizar la copia de seguridad entre cuentas, también debe habilitar la confianza en el servicio. Tras habilitar la confianza en el servicio, puede usar cualquier cuenta de la organización como cuenta de destino. Desde la cuenta de destino, puede elegir qué almacenes va a usar para realizar copias de seguridad entre cuentas.
- Habilite la copia de seguridad entre cuentas en la consola de AWS Backup

Para obtener información acerca de la seguridad, consulte Consideraciones de seguridad para la copia de seguridad entre cuentas.

Para utilizar la copia de seguridad entre cuentas, debe habilitar la característica de copia de seguridad entre cuentas. A continuación, debe “permitir” la política de acceso `backup:CopyIntoBackupVault` a su almacén de copias de seguridad de destino.

Habilite la copia de seguridad entre cuentas

1. Inicie sesión con las credenciales AWS Organizations de su cuenta de administración. La copia de seguridad entre cuentas solo se puede habilitar o deshabilitar con estas credenciales.
2. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
3. En Mi cuenta, elija Configuración.
4. Para Copia de seguridad entre cuentas, elija Habilitar.
5. En Almacenes de copia de seguridad, elija su almacén de destino.

   En el caso de las copias multicuentas, la bóveda de origen y la bóveda de destino se encuentran en cuentas diferentes. Cambie a la cuenta propietaria de la cuenta de destino, según sea necesario.
6. En la sección Política de acceso, seleccione “Permitir” `backup:CopyIntoBackupVault`. Por ejemplo, elija Agregar permisos y, a continuación, Permitir el acceso a un almacén de copias de seguridad desde la organización. Se rechazará cualquier acción entre cuentas que no `backup:CopyIntoBackupVault` sea la realizada.
7. Ahora, cualquier cuenta de su organización puede compartir el contenido de su almacén de copias de seguridad con cualquier otra cuenta de su organización. Para obtener más información, consulte Intercambio de un almacén de copias de seguridad con una cuenta de AWS diferente. Para limitar las cuentas que pueden recibir el contenido de los almacenes de copias de seguridad de otras cuentas, consulte Configuración de la cuenta como cuenta de destino.

Programación de copias de seguridad entre cuentas

Puede utilizar un plan de copia de seguridad programadas para copiar las copias de seguridad en Cuentas de AWS.

Para copiar una copia de seguridad mediante un plan de copia de seguridad programadas

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En Mi cuenta, elija Planes de copia de seguridad y, a continuación, elija Crear plan de copia de seguridad.

3. En la página Crear plan de copia de seguridad, elija Crear un nuevo plan.
4. En Nombre del plan de copia de seguridad, introduzca un nombre para su plan de copia de seguridad.
5. En la sección Configuración de regla de copia de seguridad, agregue una regla de copia de seguridad que defina una programación de copia de seguridad, un intervalo de copia de seguridad y reglas de ciclo de vida. Puede agregar más reglas de copia de seguridad más adelante.

   En Nombre de la regla, ingrese un nombre para la regla.
6. En la sección Programar, en Frecuencia, elija con qué frecuencia quiere que se realice la copia de seguridad.
7. En Intervalo de copia de seguridad, elija Usar valores predeterminados de intervalo de copia de seguridad (recomendado). Puede personalizar el intervalo de copia de seguridad.
8. Para Almacén de copia de seguridad, elija un almacén de la lista. Los puntos de recuperación de esta copia de seguridad se guardarán en este almacén. También puede crear un almacén de copias de seguridad nuevo.
9. En la sección Generar copia (opcional), ingrese los siguientes valores:

   Región de destino

   Elija el destino Región de AWS de la copia de seguridad. La copia de seguridad se copiará en esta región. Puede agregar una nueva regla a cada copia que se realice en un nuevo destino.

   Copiar en el almacén de otra cuenta

   Mueva el conmutador para elegir esta opción. La opción aparece en color azul cuando se selecciona. Aparecerá la opción ARN del almacén externo.

   ARN del almacén externo

   Ingrese el nombre de recurso de Amazon (ARN) de la cuenta de destino. El ARN es una cadena que contiene el ID de la cuenta y su. Región de AWS AWS Backup copiará la copia de seguridad a la bóveda de la cuenta de destino. La lista Región de destino se actualiza automáticamente a la región del ARN del almacén externo.

   En Permitir el acceso al almacén de copias de seguridad, elija Permitir. A continuación, elija Permitir en el asistente que se abre.

AWS Backup necesita permisos para acceder a la cuenta externa y copiar la copia de seguridad al valor especificado. El asistente muestra el siguiente ejemplo de política que proporciona este acceso.

```
{
  "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"
      }
    }
  ]
}
```

Transferir al almacenamiento en frío

Elija cuándo desea transferir la réplica de la copia de seguridad al almacenamiento en frío y cuándo va a caducar (se va a eliminar). Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Este valor no se puede modificar una vez que la copia se ha migrado al almacenamiento en frío.

Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla Disponibilidad de características por recurso. La expresión de almacenamiento en frío se omite para otros recursos.

Vencimiento especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío.

> **Note**
>
> Cuando las copias de seguridad caduquen y estén marcadas para su eliminación como parte de su política de ciclo de vida, las AWS Backup eliminará en un momento

elegido al azar durante las 8 horas siguientes. Este intervalo ayuda a garantizar un rendimiento uniforme.

10. Elija Etiquetas agregadas a puntos de recuperación para agregar etiquetas a sus puntos de recuperación.
11. Para la Configuración avanzada de copia de seguridad, elija Windows VSS para habilitar las instantáneas compatibles con la aplicación para el software de terceros seleccionado que se ejecuta en EC2.
12. Elija Crear plan.

Realización de copias de seguridad entre cuentas bajo demanda

Si lo desea, puede copiar una copia de seguridad a una copia Cuenta de AWS de seguridad diferente.

Para copiar una copia de seguridad bajo demanda

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En Mi cuenta, elija Almacén de copia de seguridad para ver todos tus almacenes de copias de seguridad en la lista. Puede filtrar por nombre o etiqueta del almacén de copias de seguridad.
3. Elija el ID de punto de recuperación de la copia de seguridad que desee copiar.
4. Elija Copiar.
5. Amplíe Detalles de la copia de seguridad para ver información sobre el punto de recuperación que está copiando.
6. En la sección Copiar configuración, elija una opción de la lista Región de destino.
7. Elija Copiar en el almacén de otra cuenta. La opción aparece en color azul cuando se selecciona.
8. Ingrese el nombre de recurso de Amazon (ARN) de la cuenta de destino. El ARN es una cadena que contiene el ID de la cuenta y su. Región de AWS AWS Backup copiará la copia de seguridad a la bóveda de la cuenta de destino. La lista Región de destino se actualiza automáticamente a la región del ARN del almacén externo.
9. En Permitir el acceso al almacén de copias de seguridad, elija Permitir. A continuación, elija Permitir en el asistente que se abre.

Para crear la copia, AWS Backup necesita permisos para acceder a la cuenta de origen. El asistente muestra un ejemplo de política que proporciona este acceso. Esta política se muestra a continuación:

```
{
  "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. En Transferir al almacenamiento en frío, elija cuándo desea transferir la copia de la copia de seguridad al almacenamiento en frío y cuándo va a vencer (se va a eliminar) la copia. Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Este valor no se puede modificar una vez que la copia se ha migrado al almacenamiento en frío.

    Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla Disponibilidad de características por recurso. La expresión de almacenamiento en frío se omite para otros recursos.

    Vencimiento especifica el número de días que deben transcurrir desde la creación hasta que se elimina la copia. Este valor debe ser 90 días superior al valor de Transferir al almacenamiento en frío.

11. Para el rol de IAM, especifique el rol de IAM (por ejemplo, el rol predeterminado) que tiene los permisos necesarios para que la copia de seguridad esté disponible para su copia. El acto de copiar lo realiza el rol vinculado al servicio de la cuenta de destino.

12. Elija Copiar. Según el tamaño del recurso que está copiando, este proceso puede tardar varias horas en completarse. Cuando se complete el trabajo de copia, verá la copia en la pestaña Trabajos de copia del menú Trabajos.

Claves de cifrado y copias multicuenta

La clave de cifrado de copias multicuenta depende del tipo de recurso. Los recursos que lo tienen AWS Backup Administración completa utilizan la clave de cifrado de la bóveda de respaldo de origen. Las claves KMS administradas por el cliente se pueden usar para el cifrado de copias entre cuentas de estos tipos de recursos.

Los tipos de recursos que no se administran por completo AWS Backup tienen la misma clave KMS de origen y la misma clave KMS de recurso. No se admite la copia multicuenta con claves de KMS AWS administradas para estos tipos de recursos que no estén completamente administrados por AWS Backup.

Si necesitas ayuda adicional para solucionar errores de copia entre cuentas, consulta el Centro de AWS conocimiento.

Al realizar una copia multicuenta, la política de claves de KMS de la cuenta de origen debe incluir la cuenta de destino en la política de claves de KMS.

Restaurar una copia de seguridad de una Cuenta de AWS a otra

AWS Backup no admite la recuperación de recursos de uno Cuenta de AWS a otro. Sin embargo, puede copiar una copia de seguridad desde una cuenta a otra diferente y, a continuación, restaurarla en esa cuenta. Por ejemplo, no puede restaurar una copia de seguridad de la cuenta A a la cuenta B, pero puede copiar una copia de seguridad de la cuenta A a la cuenta B y, a continuación, restaurarla en la cuenta B.

La restauración de una copia de seguridad de una cuenta a otra es un proceso de dos pasos.

Para restaurar una copia de seguridad de una cuenta a otra

1. Copie la copia de seguridad del origen Cuenta de AWS a la cuenta en la que desee restaurarla. Para obtener instrucciones, consulte Configuración de la copia de seguridad entre cuentas.
2. Utilice las instrucciones correspondientes a su recurso para restaurar la copia de seguridad.

Intercambio de un almacén de copias de seguridad con una cuenta de AWS diferente

AWS Backup le permite compartir un almacén de copias de seguridad con una o varias cuentas, o con toda su organización AWS Organizations. Puede compartir un almacén de copias de seguridad de destino con una cuenta de AWS , un usuario o un rol de IAM de origen.

Para compartir un almacén de copias de seguridad de destino

1. Elija y AWS Backup y, a continuación, elija Almacenes de copia de seguridad.
2. Elija el nombre del almacén de copias de seguridad que desea compartir.
3. En el panel Política de acceso, elija el menú desplegable Agregar permisos.
4. Elija Permitir el acceso de nivel de cuenta a un almacén de copias de seguridad. O bien, puede optar por permitir el acceso a nivel de organización o de rol.
5. Ingrese el AccountID de la cuenta que quiere compartir con este almacén de copias de seguridad de destino.
6. Elija Guardar política.

Puede utilizar las políticas de IAM para compartir su almacén de copias de seguridad.

Compartir un almacén de copias de seguridad de destino con una Cuenta de AWS o rol de IAM

La siguiente política comparte un almacén de copias de seguridad con el número de cuenta `4444555566666` y el rol de IAM `SomeRole` en el número de cuenta `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":"*"
    }
  ]
}
```

Comparte una bóveda de respaldo de destino en la que se encuentre una unidad organizativa AWS Organizations

La siguiente política comparte un almacén de copias de seguridad con las unidades organizativas que utilizan su `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/*"
          ]
        }
      }
    }
  ]
}
```

Comparta una bóveda de respaldo de destino con una organización en AWS Organizations

La siguiente política comparte un almacén de copias de seguridad con la organización con un `PrincipalOrgID` de “o-a1b2c3d4e5”.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
```

```
}
```

Configuración de la cuenta como cuenta de destino

La primera vez que habilita las copias de seguridad multicuenta con su cuenta de AWS Organizations administración, cualquier usuario de una cuenta de miembro puede configurar su cuenta para que sea una cuenta de destino. Se recomienda configurar una o más de las siguientes políticas de control de servicios (SCP) en AWS Organizations para limitar tus cuentas de destino. Para obtener más información sobre cómo adjuntar políticas de control de servicios a AWS Organizations los nodos, consulte Adjuntar y separar políticas de control de servicios.

Limitar las cuentas de destino mediante etiquetas

Cuando se vincula a una cuenta AWS Organizations raíz, OU o individual, esta política limita las copias de los destinos de esa raíz, unidad organizativa o cuenta a solo aquellas cuentas con bóvedas de respaldo que hayas etiquetado. `DestinationBackupVault` El permiso `"backup:CopyIntoBackupVault"` controla el comportamiento del almacén de copias de seguridad y, en este caso, qué almacenes de copias de seguridad de destino son válidos. Utilice esta política, junto con la etiqueta correspondiente que se aplica a los almacenes de destino aprobados, para controlar el destino de las copias entre cuentas únicamente a las cuentas y almacenes de copia de seguridad aprobados.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

Limitar las cuentas de destino mediante números de cuenta y nombres de almacén

Cuando se vincula a una cuenta AWS Organizations raíz, OU o cuenta individual, esta política limita las copias que se originen en esa raíz, unidad organizativa o cuenta a solo dos cuentas de destino. El permiso `"backup:CopyFromBackupVault"` controla el comportamiento de un punto de recuperación del almacén de copias de seguridad y, en este caso, los destinos a los que se puede copiar ese punto de recuperación. El almacén de origen solo permitirá realizar copias en la primera cuenta de destino (112233445566) si uno o varios nombres del almacén de copias de seguridad de destino comienzan por `cab-`. El almacén de origen solo permitirá realizar copias en la segunda cuenta de destino (123456789012) si el destino es un almacén de copias de seguridad único llamado `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"
          ]
        }
      }
    }
  ]
}
```

Limite las cuentas de destino mediante unidades organizativas en AWS Organizations

Cuando se adjuntan a una unidad organizativa o AWS Organizations raíz que contenga la cuenta de origen, o cuando se adjunten a la cuenta de origen, la siguiente política limita las cuentas de destino a las cuentas incluidas en las dos unidades organizativas especificadas.

```
{
  "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/*"
          ]
        }
      }
    }
  ]
}
```

Consideraciones de seguridad para la copia de seguridad entre cuentas

Tenga en cuenta lo siguiente cuando realice copias de seguridad entre cuentas en AWS Backup:

- El almacén de destino no puede ser el almacén predeterminado. Esto se debe a que el almacén predeterminado está cifrado con una clave que no se puede compartir con otras cuentas.
- Es posible que las copias de seguridad entre cuentas sigan ejecutándose durante 15 minutos después de que deshabilite la copia de seguridad entre cuentas. Esto se debe a la coherencia futura y puede provocar que algunos trabajos entre cuentas se inicien o finalicen incluso después de deshabilitar la copia de seguridad entre cuentas.
- Si la cuenta de destino abandona la organización más adelante, esa cuenta retendrá las copias de seguridad. Para evitar una posible filtración de datos, incluya un permiso de denegación en el permiso `organizations:LeaveOrganization` en una política de control de servicio (SCP) asociada a la cuenta de destino. Para obtener información detallada sobre las SCP, consulte Eliminación de una cuenta miembro de la organización en la Guía del usuario de Organizations.
- Si eliminas una función de trabajo de copia durante una copia multicuenta, no AWS Backup podrás dejar de compartir las instantáneas de la cuenta de origen cuando se complete la tarea de copia. En este caso, el trabajo de copia de seguridad finaliza, pero el estado del trabajo de copia aparece como Failed to unshare snapshot.

Eliminación de copias de seguridad

Le recomendamos que utilice AWS Backup para eliminar automáticamente las copias de seguridad que ya no necesite configurando su ciclo de vida al crear su plan de copias de seguridad. Por ejemplo, si configuras el ciclo de vida de tu plan de copias de seguridad para conservar los puntos

de recuperación durante un año, se AWS Backup eliminarán automáticamente el 1 de enero de 2022 los puntos de recuperación que haya creado el 1 de enero de 2021 o en un plazo de varias horas. (distribuye sus eliminaciones de AWS Backup forma aleatoria dentro de las 8 horas siguientes a la expiración del punto de recuperación para mantener el rendimiento). Para obtener más información sobre cómo configurar su política de retención del ciclo de vida, consulte Creación de un plan de copia de seguridad.

Sin embargo, es posible que desee eliminar manualmente uno o más puntos de recuperación. Por ejemplo:

- Tiene puntos de recuperación `EXPIRED`. Estos puntos de recuperación no AWS Backup se pudieron eliminar automáticamente porque eliminaste o modificaste la política de IAM original que utilizaste para crear tu plan de respaldo. Cuando AWS Backup intentó eliminarlos, no tenía permiso para hacerlo.

  También se pueden crear puntos de recuperación caducados si un punto de recuperación AWS gestionado de Amazon EBS o Amazon EC2 tiene aplicado un bloqueo de instantáneas de Amazon EBS AWS Backup y no puede completar el proceso de ciclo de vida que normalmente provocaría la eliminación del punto de recuperación. Tenga en cuenta que estos puntos de recuperación vencidos se pueden restaurar desde la consola y la API de Amazon EC2 o desde la consola y la API de Amazon EBS.

  > **Warning**
  >
  > Seguirá almacenando los puntos de recuperación vencidos en su cuenta. Esto podría aumentar los costos de almacenamiento.

  Después del 6 de agosto de 2021, AWS Backup mostrará el punto de recuperación objetivo como Expirado en su bóveda de respaldo. Si coloca el ratón sobre el estado rojo Vencido, aparecerá un mensaje de estado emergente en el que se explica por qué no se ha podido eliminar la copia de seguridad. También puede elegir Actualizar para obtener la información más reciente.
- Ya no desea que un plan de copia de seguridad funcione de la forma en que lo configuró. La actualización del plan de copia de seguridad afecta a los puntos de recuperación futuros que creará, pero no afecta al punto de recuperación que ya haya creado. Para obtener más información, consulte Actualización de un plan de copia de seguridad.
- Tiene que depurar después de terminar una prueba o un tutorial.

Eliminación de las copias de seguridad manualmente

Para eliminar manualmente los puntos de recuperación

1. En la AWS Backup consola, en el panel de navegación, seleccione Backup Vaults.
2. En la página Backup vaults (Almacenes de copias de seguridad), elija el almacén de copias de seguridad donde almacenó las copias de seguridad.
3. Elija un punto de recuperación, elija el menú desplegable Acciones y, a continuación, elija Eliminar.
4. 1. Si la lista contiene una copia de seguridad continua, elija una de las siguientes opciones. Cada copia de seguridad continua tiene un único punto de recuperación.
      - Eliminar permanentemente mis datos de copia de seguridad o Eliminar punto de recuperación. Al seleccionar una de estas opciones, detendrá las copias de seguridad continuas futuras y también eliminará los datos de las copias de seguridad continuas existentes.

        > **Note**
        >
        > Consulte Copias de seguridad y point-in-time restauración continuas (PITR) las consideraciones sobre el respaldo continuo de Amazon S3, Amazon RDS y Aurora.

      - Conserve mis datos de respaldo continuos o desasocie el punto de recuperación. Al seleccionar una de estas opciones, detendrá las copias de seguridad continuas futuras, pero rentendrá los datos de copia de seguridad continua existentes hasta que venzan, según lo definido por su periodo de retención.

        Un punto de recuperación continua (copia de seguridad) de Amazon S3 disociado permanecerá en su almacén de copias de seguridad, pero su estado pasará a `STOPPED`.
   2. Para eliminar todos los puntos de recuperación de la lista, escriba delete y, a continuación, elija Eliminar punto de recuperación.
   3. AWS Backup comienza a enviar sus puntos de recuperación para su eliminación y muestra una barra de progreso. Mantenga abierta la pestaña del navegador y no salga de esta página durante el proceso de envío.
   4. Al final del proceso de envío, AWS Backup aparece un estado en el banner. El estado puede ser:

- Enviado correctamente. Puede elegir Ver el progreso del estado de eliminación de cada punto de recuperación.
- Obtiene un error de envío. Puede elegir Ver el progreso del estado de eliminación de cada punto de recuperación o Volver a intentar el envío.
- Un resultado mixto, en el que algunos puntos de recuperación se enviaron correctamente y otros no.

5. Si elige Ver el progreso, puede revisar el Estado de eliminación de cada copia de seguridad. Si el estado de eliminación es Error o Vencido, puede hacer clic en ese estado para ver el motivo. También puede optar por Volver a intentar las eliminaciones con errores.

Solución de problemas de eliminaciones manuales

En raras ocasiones, es AWS Backup posible que no se complete la solicitud de eliminación. AWS Backup usa la función vinculada al servicio `AWSServiceRoleForBackup` para realizar eliminaciones.

Si la solicitud de eliminación tiene como resultado un error, compruebe que su rol de IAM tenga permiso para crear roles vinculados a servicios. En concreto, compruebe que su rol de IAM tenga la acción `iam:CreateServiceLinkedRole`. Si no la tiene, agregue este permiso al rol utilizado para crear una copia de seguridad. Al añadir este permiso, se pueden AWS Backup realizar eliminaciones manuales.

Si, tras confirmar que su rol de IAM incluye la acción `iam:CreateServiceLinkedRole`, los puntos de recuperación siguen estancados en el estado `DELETING`, es probable que estemos investigando el problema. Complete la eliminación de forma manual con los siguientes pasos:

1. Configure un recordatorio para regresar en 2 o 3 días.
2. Transcurridos 2 o 3 días, compruebe si hay puntos de eliminación `EXPIRED` recientes que hayan sido el resultado de su primera operación de eliminación manual.
3. Elimine manualmente esos puntos de recuperación `EXPIRED`.

Para obtener más información sobre roles, consulte Uso de roles vinculados a servicios y Adición y eliminación de permisos de identidad de IAM.

Edición de una copia de seguridad

Después de crear una copia de seguridad mediante AWS Backup, puede cambiar el ciclo de vida o las etiquetas de la copia de seguridad. El ciclo de vida define el momento en que se migra una copia de seguridad al almacenamiento en frío y cuándo dicho recurso vence. AWS Backup migra y da por vencidas automáticamente las copias de seguridad en función del ciclo de vida que se defina.

Para ver la lista de recursos que puede transferir al almacenamiento en frío, consulte la sección “Ciclo de vida al almacenamiento en frío” de la tabla Disponibilidad de características por recurso. La expresión de almacenamiento en frío se omite para otros recursos.

> **Note**
>
> La edición de las etiquetas de una copia de seguridad mediante la AWS Backup consola solo se admite para las copias de seguridad de los sistemas de archivos Amazon Elastic File System (Amazon EFS) y Amazon DynamoDB avanzado.
> Las etiquetas que se agregaron al punto de recuperación al crear otros recursos seguirán apareciendo, pero aparecerán atenuadas y no se podrán editar. Aunque estas etiquetas no se pueden editar en la AWS Backup consola, puede editar las etiquetas de las copias de seguridad de estos otros servicios mediante la consola o la API del servicio.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. Al actualizar la configuración de “transition to cold after days” (número de días tras los cuales migrará a almacenamiento en frío), el valor debe tener como mínimo la edad de la copia de seguridad más un día. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

A continuación se muestra un ejemplo de cómo actualizar el ciclo de vida de una copia de seguridad.

Para editar el ciclo de vida de una copia de seguridad

1. Inicie sesión en la AWS Backup consola AWS Management Console y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).

3. En la sección Backups (Copias de seguridad), elija una copia de seguridad.
4. En la página de detalles de copia de seguridad, elija Edit (Editar).
5. Configure los ajustes del ciclo de vida y, a continuación, seleccione Save (Guardar).

Restauración de una copia de seguridad

Cómo restaurar

Para obtener instrucciones de restauración de la consola y enlaces a la documentación AWS Backup de cada tipo de recurso compatible, consulte los enlaces al final de esta página.

Para restaurar una copia de seguridad mediante programación, utilice la operación de API StartRestoreJob.

Los valores de configuración (“restaurar metadatos”) que necesita para restaurar el recurso varían en función del recurso que desee restaurar. Para obtener los metadatos de configuración con los que se creó la copia de seguridad, puede llamar a GetRecoveryPointRestoreMetadata. También hay ejemplos de restauración de metadatos en los enlaces al final de esta página.

La restauración desde el almacenamiento en frío suele tardar 4 horas más que la restauración desde el almacenamiento en caliente.

Para cada restauración, se crea un trabajo de restauración con un identificador de trabajo único, por ejemplo, `1323657E-2AA4-1D94-2C48-5D7A423E7394`.

> **Note**
>
> AWS Backup no proporciona ningún acuerdo de nivel de servicio (SLA) durante un período de restauración. Los tiempos de restauración pueden variar en función de la carga y la capacidad del sistema, incluso en el caso de restauraciones que contengan los mismos recursos.

Restauraciones no destructivas

Cuando se utiliza AWS Backup para restaurar una copia de seguridad, se crea un nuevo recurso con la copia de seguridad que se está restaurando. Esto sirve para evitar que la actividad de restauración destruya los recursos existentes.

Pruebas de restauración

Puede realizar pruebas en sus recursos para simular una experiencia de restauración. De este modo podrá determinar si cumple el objetivo de tiempo de restauración (RTO) de su organización y prepararse para futuras necesidades de restauración.

Para obtener más información, consulte Pruebas de restauración.

Copia de etiquetas durante una restauración

> **Note**
>
> Las restauraciones de Amazon DynamoDB, Amazon S3, SAP HANA en instancias de Amazon EC2, máquinas virtuales y recursos de Amazon Timestream actualmente no disponen de esta característica.

Introducción

Puede copiar etiquetas a medida que restaura un recurso si las etiquetas pertenecían al recurso protegido en el momento de la copia de seguridad. Las etiquetas, que son etiquetas que contienen un par de clave-valor, pueden ayudarle a identificar y buscar recursos. Al iniciar un trabajo de restauración, las etiquetas que pertenecían a los recursos originales de los que se hizo una copia de seguridad se pueden agregar al recurso que restaura.

Si decide incluir etiquetas durante un trabajo de restauración, este paso puede reemplazar la sobrecarga y el trabajo que supone aplicar etiquetas manualmente a los recursos una vez finalizado el trabajo de restauración. Tenga en cuenta que esto es distinto de agregar etiquetas nuevas a los recursos restaurados.

Al restaurar una copia de seguridad en el flujo de la consola, las etiquetas de origen se copian de forma predeterminada. En la consola, quite la marca de la casilla si quiere dejar de copiar las etiquetas a un recurso restaurado.

En la operación de la API `StartRestoreJob`, el parámetro `CopySourceTagsToRestoredResource` está configurado en `false` de forma predeterminada, lo que excluirá las etiquetas originales del recurso que está restaurando. Si desea incluir las etiquetas originales, configúrelo en`True`.

Consideraciones

- Un recurso puede tener hasta 50 etiquetas, incluidos los recursos restaurados. Consulte Cómo etiquetar sus AWS recursos para obtener más información sobre los límites de etiquetas.
- Asegúrese de que el rol utilizado para restaurar o copiar etiquetas tenga los permisos correctos. El rol predeterminado para las restauraciones contiene los permisos necesarios. Un rol personalizado debe incluir permisos adicionales para etiquetar los recursos.
- Los siguientes recursos no son compatibles actualmente para la inclusión de etiquetas de restauración: VMware Cloud™ on AWS, VMware Cloud™ on AWS Outposts, sistemas locales, SAP HANA en instancias Amazon EC2, Timestream, DynamoDB, Advanced DynamoDB y Amazon S3.
- En el caso de las copias de seguridad continuas, se copiarán en el recurso restaurado las etiquetas del recurso original, a partir de la copia de seguridad más reciente.
- Las etiquetas no se copiarán en las restauraciones a nivel de elemento.
- Las etiquetas que se agregaron a una copia de seguridad después de que se completase el trabajo de copia de seguridad, pero que no estaban presentes en el recurso original antes de la copia de seguridad, no se copiarán en el recurso restaurado. Solo las copias de seguridad creadas después del 22 de mayo de 2023 son elegibles para la copia de etiquetas en la restauración.

Interacción de las etiquetas con recursos específicos

- Amazon EC2
  - Las etiquetas aplicadas a las instancias de Amazon EC2 restauradas también se aplican a los volúmenes de Amazon EBS restaurados adjuntos.
  - Las etiquetas aplicadas a los volúmenes de EBS adjuntos a las instancias de origen no se copian en los volúmenes adjuntos a las instancias restauradas. Si tiene políticas de IAM que permiten o deniegan a los usuarios el acceso a los volúmenes de EBS en función de sus etiquetas, debe reasignar manualmente las etiquetas necesarias a los volúmenes restaurados para garantizar que sus políticas sigan vigentes.
- Al restaurar un recurso de Amazon EFS, debe copiarlo en un nuevo sistema de archivos. Las etiquetas no se pueden copiar en las restauraciones en un sistema de archivos existente.
- Amazon RDS
  - Si el clúster de RDS del que se hizo la copia de seguridad sigue activo, se copiarán las etiquetas de este clúster.

  - Si el clúster original ya no está activo, en su lugar, se copiarán las etiquetas de la instantánea del clúster.
  - Las etiquetas que estaban presentes en el recurso en el momento de la copia de seguridad se copiarán durante la restauración, independientemente de si el parámetro booleano para `CopySourceTagsToRestoredResource` está establecido en `True` o `False`. Sin embargo, si la instantánea no contiene etiquetas, se utilizará la configuración booleana anterior.
- De forma predeterminada, los clústeres de Amazon Redshift siempre incluyen etiquetas durante un trabajo de restauración.

Copia de etiquetas mediante la consola

1. Abra la consola de AWS Backup.
2. En el panel de navegación, elija Recursos protegidos y seleccione el ID del recurso de Amazon S3 que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID del recurso seleccionado. Para restaurar un recurso:
   a. En el panel Copia de seguridad, elija el ID del punto de recuperación del recurso.
   b. En la esquina superior derecha del panel, elija Restaurar (también puede ir al almacén de copias de seguridad, buscar el punto de recuperación, hacer clic en Acciones y, a continuación, hacer clic en Restaurar).
4. En la página Restaurar copia de seguridad, localice el panel denominado Restaurar con etiquetas. Para incluir todas las etiquetas del recurso original, mantenga marcada la casilla de verificación (tenga en cuenta que en la consola esta casilla está marcada de forma predeterminada).
5. Haga clic en Restaurar copia de seguridad una vez que haya seleccionado todos los ajustes y roles que prefiera.

Para incluir etiquetas mediante programación

Use la operación de la API `StartRestoreJob`. Asegúrese de que el siguiente parámetro booleano esté establecido en `True`.

```
CopySourceTagsToRestoredResource = true
```

Si el parámetro booleano es `CopySourceTagsToRestoredResource =True`, el trabajo de restauración copiará las etiquetas de los recursos originales al material restaurado.

> **Important**
>
> El trabajo de restauración fallará si se incluye este parámetro para un recurso no compatible (VMware, sistemas locales AWS Outposts, SAP HANA en instancias EC2, Timestream, DynamoDB, Advanced DynamoDB y 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
}
```

Solución de problemas de restauración de etiquetas

ERROR: permisos insuficientes

SOLUCIÓN: asegúrese de tener los permisos necesarios en su rol de restauración para poder incluir etiquetas en el recurso restaurado. La política de funciones de servicio AWS gestionado predeterminada para las restauraciones contiene los permisos necesarios para esta tarea AWSBackupServiceRolePolicyForRestores.

Si decide usar un rol personalizado, asegúrese de que estén presentes los siguientes permisos:

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

Para obtener más información, consulte Permisos de API.

Estados de los trabajos de restauración

Puede ver el estado de un trabajo de restauración en la página Trabajos de la consola de AWS Backup . Los estados de los trabajos de restauración incluyen pendiente, en ejecución, anulado, completado y error.

Temas

- Restauración de datos de S3
- Restauración de una máquina virtual mediante AWS Backup
- Restauración de un sistema de archivos de FSx
- Restauración de un volumen de Amazon EBS
- Restauración de un sistema de archivos de Amazon EFS
- Restauración de una tabla de Amazon DynamoDB
- Restauración de una base de datos de RDS
- Restauración de un clúster de Amazon Aurora
- Restauración de una instancia de Amazon EC2
- Restauración de un volumen de Storage Gateway
- Restauración de una tabla de Amazon Timestream
- Restauración de un clúster de Amazon Redshift
- Restauración de una base de datos de SAP HANA en una instancia de Amazon EC2
- Restauración de un clúster de DocumentDB
- Restauración de un clúster de Neptune
- Restaure las copias CloudFormation de seguridad

Restauración de datos de S3

Puede restaurar los datos de S3 de los que realizó una copia de AWS Backup seguridad en la clase de almacenamiento S3 Standard. Puede restaurar todos los objetos de un bucket u objetos específicos. Puede restaurarlos en un bucket existente o nuevo.

Permisos de restauración de Amazon S3

Antes de empezar a restaurar los recursos, asegúrate de que el rol que estás utilizando tenga permisos suficientes.

Para obtener más información, consulta las siguientes entradas sobre políticas:

1. `AWSBackupServiceRolePolicyForS3Restore`
2. `AWSBackupServiceRolePolicyForRestores`
3. Políticas gestionadas para AWS Backup

Consideraciones sobre la restauración de Amazon S3

- AWS Backup crea una copia de seguridad de todas las versiones de S3, pero restaura solo la versión más reciente de la pila de versiones en cualquier momento.
- Las listas de control de acceso (ACL) deben estar habilitadas en el bucket de destino o, de lo contrario, el trabajo dará como resultado un error. Para habilitar las ACL, siga las instrucciones de la página Configuración de la ACL.
- Las restauraciones de objetos se omiten si el bucket de origen tiene un objeto con el mismo nombre o ID de versión.
- Si restaura objetos específicos, puede restaurar la versión actual de un objeto.
- Al restaurar el depósito de S3 original,
  - AWS Backup no realiza una restauración destructiva, lo que significa que no AWS Backup colocará un objeto en un depósito en lugar de un objeto que ya existe, independientemente de la versión.
  - En la versión actual, un marcador de borrado se considera que el objeto no existe, por lo que se puede realizar una restauración.
  - AWS Backup no elimina objetos (sin eliminar marcadores) de un depósito durante una restauración (por ejemplo: las claves que se encuentran actualmente en el depósito y que no estaban presentes durante la copia de seguridad permanecerán).

- Restauración de copias entre regiones
  - Si bien las copias de seguridad de S3 se pueden copiar entre regiones, los trabajos de restauración solo se realizan en la misma región en la que se encuentra la copia de seguridad o copia original.

    Example

    Ejemplo: un bucket de S3 creado en la región EE.UU. Este (Virginia del Norte) se puede copiar en la región Canadá (Central). El trabajo de restauración puede iniciarse mediante el bucket original de la región Este de EE. UU. (Norte de Virginia) y restaurarse a esa región, o bien puede iniciarse con la copia en la región de Canadá (centro) y restaurarse en esa región.
  - El método de cifrado original no se puede utilizar para restaurar un punto de recuperación (copia de seguridad) copiado de otra región. El AWS KMS cifrado de copias entre regiones no está disponible para los recursos de Amazon S3; en su lugar, utilice un tipo de cifrado diferente para un trabajo de restauración.

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon S3

Para restaurar los datos de Amazon S3 mediante la AWS Backup consola:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y seleccione el ID del recurso de Amazon S3 que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID del recurso seleccionado. Para restaurar un recurso:

   a. En el panel Copias de seguridad, elija el ID del punto de recuperación del recurso.

   b. En la esquina superior derecha del panel, elija Restaurar.

      (También puede ir al almacén de copias de seguridad, buscar el punto de recuperación, hacer clic en Acciones y, a continuación, hacer clic en Restaurar).
4. Si va a restaurar una copia de seguridad continua, en el panel Tiempo de restauración, seleccione una de las siguientes opciones:

   a. Acepte el valor predeterminado para restaurar a la Última hora restaurable.

   b. Especifique la fecha y la hora de la restauración.

5. En el panel Configuración, especifique si desea Restaurar todo el bucket o realizar una Restauración a nivel de elemento.

   a. Si elige la restauración a nivel de elemento, restaurará hasta 5 elementos (objetos o carpetas en un depósito) por trabajo de restauración especificando el URI de S3 de cada elemento que identifica de forma única ese objeto.

      (Para obtener más información acerca de los URI de los buckets de S3, consulte Métodos para acceder a un bucket en la Guía del usuario de Amazon Simple Storage Service).

   b. Elija Agregar elemento para especificar otro elemento para restaurarlo.

6. Elige el Destino de restauración. Puede Restaurar al bucket fuente, Usar bucket existente o Crear nuevo bucket.

   > **Note**
   >
   > El depósito de destino de la restauración debe tener activado el control de versiones. AWS Backup le notifica si el depósito que ha seleccionado no cumple este requisito.

   a. Si eliges Usar un depósito existente, selecciona el depósito S3 de destino en el menú desplegable, que muestra todos los depósitos existentes en tu región actual. AWS

   b. Si elige Crear nuevo bucket, escriba el Nuevo nombre de bucket. El nuevo bucket tiene activado el control de versiones de S3 de forma predeterminada. La configuración Bloquear acceso público (BPA) estará desactivada de forma predeterminada. Puede modificar estos ajustes después de crear el bucket en S3.

7. Para el cifrado de los objetos de su depósito de S3, puede elegir el cifrado de objetos restaurado. Utilice las claves de cifrado originales (de forma predeterminada), una clave de Amazon S3 (SSE-S3) o una clave de AWS Key Management Service (SSE-KMS).

   Esta configuración solo se aplica al cifrado de los objetos del bucket de S3. Esto no afecta al cifrado del propio depósito.

   a. Utilizar claves de cifrado originales (opción predeterminada) restaura los objetos con las mismas claves de cifrado utilizadas por el objeto de origen. Si un objeto de origen no estaba cifrado, este método restaura el objeto sin cifrar.

      Esta opción de restauración le permite elegir opcionalmente una clave de cifrado sustituta para cifrar los objetos de restauración si la clave original no está disponible.

b. Si elige la clave de Amazon S3 (SSE-S3), no es necesario que especifique ninguna otra opción.

c. Si elige la AWS Key Management Service clave (SSE-KMS), puede realizar las siguientes elecciones: Clave administrada de AWS (aws/s3), elegir una de AWS KMS las claves o introducir el ARN de la clave. AWS KMS

   i. Si elige la Clave administrada de AWS (aws/s3), no es necesario que especifique ninguna otra opción.

   ii. Si eliges una de tus AWS KMS claves, selecciona una AWS KMS clave en el menú desplegable. Como alternativa, elija Crear clave.

   iii. Si introduce un AWS KMS ARN clave, escriba el ARN en el cuadro de texto. Como alternativa, elija Crear clave.

8. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.

9. Seleccione Restaurar copia de seguridad. Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon S3

Utilice `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de 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
```

Estado del punto de recuperación

Los puntos de recuperación tendrán un estado que indica su estado.

`PARTIAL`el estado indica que no se AWS Backup pudo crear el punto de recuperación antes de que se cerrara la ventana de respaldo. Para aumentar el plazo de su plan de respaldo mediante la API, consulte UpdateBackupPlan. También puede seleccionar y editar el plan de copia de seguridad mediante la consola para aumentar el periodo del plan de copia de seguridad.

`EXPIRED`el estado indica que el punto de recuperación ha superado su período de retención, pero AWS Backup carece de permiso o no puede eliminarlo por algún motivo. Para eliminar estos puntos de recuperación manualmente, consulte el Paso 3: elimine los puntos de recuperación en la sección Depuración de recursos de la Introducción.

El estado `STOPPED` se produce en una copia de seguridad continua cuando un usuario ha realizado alguna acción que provoca la desactivación de la copia de seguridad continua. Esto puede deberse a la eliminación de permisos, la desactivación del control de versiones, la desactivación de los eventos que se envían a Amazon EventBridge o la desactivación de EventBridge las reglas establecidas por. AWS Backup

Para resolver el estado `STOPPED`, asegúrese de que todos los permisos solicitados estén en vigor y de que el control de versiones esté activado en el bucket de S3. Una vez que se cumplan estas condiciones, la siguiente instancia de una regla de copia de seguridad que se ejecute provocará la creación de un nuevo punto de recuperación continuo. No es necesario eliminar los puntos de recuperación con el estado STOPPED.

Restauración de una máquina virtual mediante AWS Backup

Puede restaurar una máquina virtual en VMware, VMware Cloud on AWS, VMware Cloud on AWS Outposts, un volumen de Amazon EBS o una instancia de Amazon EC2. Para restaurar (o migrar) una máquina virtual a EC2 se necesita una licencia. De forma predeterminada, AWS incluirá una licencia (de pago). Para obtener más información, consulte Opciones de licencia en la Guía del usuario de VM Import/Export.

Puede restaurar una máquina virtual VMware mediante la AWS Backup consola o a través del. AWS CLI Cuando se restaura una máquina virtual, no se incluye la carpeta VMware Tools. Consulte la documentación de VMware para volver a instalar VMware Tools.

AWS Backup Las restauraciones de máquinas virtuales no son destructivas, es decir, AWS Backup no sobrescriben las máquinas virtuales existentes durante una restauración. En su lugar, el trabajo de restauración implementa una nueva máquina virtual.

Tareas

- Consideraciones a la hora de restaurar una máquina virtual en una instancia de Amazon EC2
- Utilice la AWS Backup consola para restaurar los puntos de recuperación de la máquina virtual
- Se usa AWS CLI para restaurar los puntos de recuperación de máquinas virtuales

Consideraciones a la hora de restaurar una máquina virtual en una instancia de Amazon EC2

- Para restaurar (o migrar) una máquina virtual a EC2 se necesita una licencia. De forma predeterminada, AWS incluirá una licencia (se aplican cargos). Para obtener más información, consulte Opciones de licencia en la Guía del usuario de VM Import/Export.
- Hay un límite máximo de 5 TB (terabytes) para cada disco de máquina virtual.
- No puede especificar un key pair al restaurar la máquina virtual en una instancia. Puede añadir un par de claves `authorized_keys` durante el lanzamiento (a través de los datos de usuario de la instancia) o después del lanzamiento (tal y como se describe en esta sección de solución de problemas de la Guía del usuario de Amazon EC2).
- Confirme que su sistema operativo es compatible con la importación y exportación desde Amazon EC2 en la Guía del usuario de VM Import/Export.
- Consulte las limitaciones relacionadas con la importación de máquinas virtuales a Amazon EC2 en la Guía del usuario de VM Import/Export.
- Cuando restaure en una instancia de Amazon EC2 mediante AWS CLI, debe especificar. `"RestoreTo":"EC2Instance"` Todos los demás atributos tienen valores predeterminados.

Utilice la AWS Backup consola para restaurar los puntos de recuperación de la máquina virtual

Puede restaurar una máquina virtual desde varias ubicaciones en el panel de navegación izquierdo de la AWS Backup consola:

- Elija Hipervisores para ver los puntos de recuperación de las máquinas virtuales administradas por un hipervisor que esté conectado a AWS Backup.

- Elija Máquinas virtuales para ver los puntos de recuperación de las máquinas virtuales en todos los hipervisores que estén conectados a AWS Backup.
- Seleccione Backup Vaults para ver los puntos de recuperación almacenados en un almacén específico AWS Backup .
- Elija Recursos protegidos para ver los puntos de recuperación de todos sus recursos AWS Backup protegidos.

Si tiene que restaurar una máquina virtual que ya no tiene conexión con la puerta de enlace de copia de seguridad, elija Almacenes de copia de seguridad o Recursos protegidos para localizar el punto de recuperación.

Opciones

- Restaure a VMware
- Restaurar en un volumen de Amazon EBS
- Restauración en una instancia de Amazon EC2

Para restaurar una máquina virtual en VMware, VMware Cloud on AWS y VMware Cloud on AWS Outposts

1. En las vistas Hipervisores o Máquinas virtuales, elija el Nombre de máquina virtual que desea restaurar. En la vista Recursos protegidos, elija el ID de recurso de la máquina virtual que desea restaurar.
2. Elija el botón de opción situado junto al ID de punto de recuperación que se va a restaurar.
3. Elija Restore (Restaurar).
4. Elija el Tipo de restauración.
    a. La Restauración completa restaura todos los discos de la máquina virtual.
    b. La Restauración a nivel de disco restaura una selección de uno o más discos definida por el usuario. Utilice el menú desplegable para seleccionar los discos que desea restaurar.
5. Elija la Ubicación de la restauración. Las opciones son VMware, VMware Cloud on AWS y VMware Cloud on AWS Outposts.
6. Si va a realizar una restauración en su totalidad, vaya al paso siguiente. Si va a realizar una restauración a nivel de disco, aparecerá un menú desplegable en Discos de máquina virtual. Elija uno o más volúmenes de arranque para restaurarlos.

7. Seleccione un Hipervisor en el menú desplegable para administrar la máquina virtual restaurada
8. Para la máquina virtual restaurada, utilice las prácticas recomendadas de su organización para especificar:

    a. Nombre
    b. Ruta (como `/datacenter/vm`)
    c. Nombre del recurso de computación (como VMHost o clúster)

        Si un host forma parte de un clúster, no puede restaurarlo en el host, sino solo en el clúster en cuestión.
    d. Almacén de datos
9. En Rol de restauración, seleccione el Rol predeterminado (recomendado) o Elegir un rol de IAM en el menú desplegable.
10. Seleccione Restaurar copia de seguridad.
11. Opcional: compruebe si su trabajo de restauración tiene el estado `Completed`. En el panel de navegación izquierdo, elija Trabajos.

Para restaurar una máquina virtual en un volumen de Amazon EBS

1. En las vistas Hipervisores o Máquinas virtuales, elija el Nombre de máquina virtual que desea restaurar. En la vista Recursos protegidos, elija el ID de recurso de la máquina virtual que desea restaurar.
2. Elija el botón de opción situado junto al ID de punto de recuperación que se va a restaurar.
3. Elija Restore (Restaurar).
4. Elija el Tipo de restauración.

    - La Restauración de disco restaura una selección de uno o más discos definida por el usuario. Utilice el menú desplegable para seleccionar el disco que desea restaurar.
5. Elija la Ubicación de la restauración como Amazon EBS.
6. En el menú desplegable Disco de máquina virtual, elija el volumen de arranque que desea restaurar.
7. En Tipo de volumen de EBS, elija el tipo de volumen.
8. Elige la zona de disponibilidad.
9. Cifrado (opcional). Marque la casilla si elige cifrar el volumen de EBS.

10. Seleccione su clave KMS en el menú.
11. En Restaurar el rol, selecciona el rol predeterminado (recomendado) o Elige un rol de IAM.
12. Seleccione Restaurar copia de seguridad.
13. Opcional: compruebe si su trabajo de restauración tiene el estado `Completed`. En el panel de navegación izquierdo, elija Trabajos.
14. Opcional: visite How do I create an LVM logical volume on an entire Amazon EBS volume? para obtener más información sobre cómo montar los volúmenes administrados y acceder a los datos del volumen de Amazon EBS restaurado.

Para restaurar una máquina virtual en una instancia de Amazon EC2

1. En las vistas Hipervisores o Máquinas virtuales, elija el Nombre de máquina virtual que desea restaurar. En la vista Recursos protegidos, elija el ID de recurso de la máquina virtual que desea restaurar.
2. Elija el botón de opción situado junto al ID de punto de recuperación que se va a restaurar.
3. Elija Restore (Restaurar).
4. Elija el Tipo de restauración.
   - La Restauración completa restaura el sistema de archivos por completo, incluida la carpeta y los archivos del nivel raíz.
5. Elija la Ubicación de la restauración como Amazon EC2.
6. En el tipo de instancia, elija la combinación de cómputo y memoria necesaria para ejecutar la aplicación en la nueva instancia.

   > **Tip**
   >
   > Elija un tipo de instancia que coincida o supere las especificaciones de la máquina virtual original. Para obtener más información, consulte la Guía de tipos de instancia de Amazon EC2.

7. Para Virtual Private Cloud (VPC), elige una nube privada virtual (VPC), que defina el entorno de red de la instancia.
8. En Subnet, elija una de las subredes de la VPC. La instancia recibe una dirección IP privada del rango de direcciones de la subred.

9. En el caso de los grupos de seguridad, elige un grupo de seguridad que sirva de firewall para el tráfico a tu instancia.
10. En Restaurar el rol, selecciona el rol predeterminado (recomendado) o Elige un rol de IAM.
11. Opcional: para ejecutar un script en la instancia en el momento del lanzamiento, expanda la configuración avanzada e introduzca el script en Datos de usuario.
12. Seleccione Restaurar copia de seguridad.
13. Opcional: compruebe si su trabajo de restauración tiene el estado `Completed`. En el panel de navegación izquierdo, elija Trabajos.

Se usa AWS CLI para restaurar los puntos de recuperación de máquinas virtuales

Utilice `StartRestoreJob`.

Puede especificar los siguientes metadatos para restaurar una máquina virtual en Amazon EC2 y Amazon EBS:

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

Puede especificar los siguientes metadatos para la restauración de una máquina virtual en VMware, VMware Cloud on AWS y VMware cloud on AWS Outpost:

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

En este ejemplo se muestra cómo realizar una restauración completo en 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"}'
```

Restauración de un sistema de archivos de FSx

Las opciones de restauración que están disponibles cuando se restauran los sistemas de archivos de Amazon FSx son las mismas que cuando se utiliza la copia de seguridad nativa de Amazon FSx. AWS Backup Puede utilizar el punto de recuperación de una copia de seguridad para crear un nuevo sistema de archivos y restaurar una point-in-time instantánea de otro sistema de archivos.

Al restaurar los sistemas de archivos de Amazon FSx, AWS Backup crea un nuevo sistema de archivos y lo rellena con los datos (Amazon FSx para NetApp ONTAP permite restaurar un volumen en un sistema de archivos existente). Esto es similar a la forma en que Amazon FSx nativo realiza copias de seguridad y restaura los sistemas de archivos. La restauración de una copia de seguridad en un nuevo sistema de archivos lleva el mismo tiempo que la creación de un nuevo sistema de archivos. Los datos restaurados a partir de la copia de seguridad se cargan de forma diferida en el sistema de archivos. Por lo tanto, es posible que observe una latencia ligeramente mayor durante el proceso.

> **Note**
>
> No puede restaurar en un sistema de archivos de Amazon FSx existente ni puede restaurar archivos o carpetas individuales.

FSx para ONTAP no es compatible con copias de seguridad de determinados tipos de volúmenes, incluidos los volúmenes de DP (protección de datos), los volúmenes de LS (carga compartida), los volúmenes completos o los volúmenes de sistemas de archivos que están llenos. Para obtener más información, consulte FSx for ONTAP Working with backups. AWS Backup Las bóvedas que contienen puntos de recuperación de los sistemas de archivos de Amazon FSx están visibles desde fuera. AWS Backup Puede restaurar los puntos de recuperación con Amazon FSx, pero no puede eliminarlos.

Puede ver las copias de seguridad creadas por la funcionalidad de copia de seguridad automática integrada de Amazon FSx desde la AWS Backup consola. También puede recuperar estas copias de seguridad utilizando AWS Backup. Sin embargo, no puede eliminar estas copias de seguridad ni cambiar las programaciones de copias de seguridad automáticas de sus sistemas de archivos Amazon FSx mediante. AWS Backup

Puede restaurar las copias de seguridad creadas AWS Backup mediante la AWS Backup consola, la API o AWS CLI. En esta sección se muestra cómo utilizar la AWS Backup consola para restaurar los sistemas de archivos de Amazon FSx.

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon FSx

Restauración de un sistema de archivos de FSx para Windows File Server

Para restaurar un sistema de archivos de FSx para Windows File Server

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y elija el ID del recurso de Amazon FSx que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar copia de seguridad.
5. En la sección Detalles del sistema de archivos, el ID de la copia de seguridad se muestra en ID de copia de seguridad y el tipo de sistema de archivos se muestra en Tipo de sistema de archivos. Puede restaurar sistemas de archivos de FSx para Windows File Server y FSx para Lustre.

6. Acepte el valor predeterminado para Tipo de implementación. No puede cambiar el tipo de implementación de un sistema de archivos durante la restauración.
7. Elija el Tipo de almacenamiento que va a usar. Si la capacidad de almacenamiento del sistema de archivos es inferior a 2000 GiB, no puede utilizar el tipo de almacenamiento HDD.
8. Para la capacidad de rendimiento, elija Capacidad de rendimiento recomendada para utilizar la velocidad recomendada de 16 MB por segundo (MBps) o elija Especificar la capacidad de rendimiento e ingrese una nueva velocidad.
9. En la sección Red y seguridad, proporcione la información requerida.
10. Si va a restaurar un sistema de archivos de FSx para Windows File Server, proporcione la información de autenticación de Windows utilizada para acceder al sistema de archivos, o puede crear una nueva.

    > **Note**
    >
    > Al restaurar una copia de seguridad, no puede cambiar el tipo de Active Directory del sistema de archivos.

    Para obtener más información sobre Microsoft Active Directory, consulte Working with Active Directory in Amazon FSx for Windows File Server en la Guía del usuario de Amazon FSx para Windows File Server.
11. De forma opcional, en la sección Copia de seguridad y mantenimiento, proporcione la información para configurar sus preferencias de copia de seguridad.
12. En la sección Rol de restauración, elija el rol de IAM que AWS Backup utilizará para crear y administrar las copias de seguridad en su nombre. Se recomienda elegir el Rol predeterminado. Si no hay un rol predeterminado, se creará uno automáticamente con los permisos adecuados. También puede proporcionar su propio rol de IAM.
13. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Restauración de un sistema de archivos de Amazon FSx para Lustre

AWS Backup es compatible con los sistemas de archivos Amazon FSx for Lustre que tienen un tipo de implementación de almacenamiento persistente y no están vinculados a un repositorio de datos como Amazon S3.

Para restaurar un sistema de archivos de Amazon FSx para Lustre

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y elija el ID del recurso de Amazon FSx que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar copia de seguridad al nuevo sistema de archivos.
5. En la sección Configuración, el ID de la copia de seguridad se muestra en ID de copia de seguridad y el tipo de sistema de archivos se muestra en Tipo de sistema de archivos. El Tipo de sistema de archivos debe ser Lustre.
6. De forma opcional, puede ingresar un nombre para el sistema de archivos.
7. Elija un tipo de despliegue. AWS Backup solo admite el tipo de despliegue persistente. No puede cambiar el tipo de implementación de un sistema de archivos durante la restauración.

   El tipo de implementación persistente es para el almacenamiento a largo plazo. Para obtener información detallada sobre las opciones de implementación de FSx para Lustre, consulte Using Available Deployment Options for Amazon FSx for Lustre File Systems en la Guía del usuario de Amazon FSx para Lustre.
8. Elija el Rendimiento por unidad de almacenamiento que desee utilizar.
9. Especifique la Capacidad de almacenamiento que se va a utilizar. Introduzca una capacidad entre 32 GiB y 64 436 GiB.
10. En la sección Red y seguridad, proporcione la información requerida.
11. De forma opcional, en la sección Copia de seguridad y mantenimiento, proporcione la información para configurar sus preferencias de copia de seguridad.
12. En la sección Rol de restauración, elija el rol de IAM que AWS Backup utilizará para crear y administrar las copias de seguridad en su nombre. Se recomienda elegir el Rol predeterminado. Si no hay un rol predeterminado, se creará uno automáticamente con los permisos adecuados. También puede proporcionar su rol de IAM.
13. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Restauración de volúmenes de Amazon FSx para NetApp ONTAP

Para restaurar los volúmenes de Amazon FSx para NetApp ONTAP:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y elija el ID del recurso de Amazon FSx que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar.

   La primera sección, Detalles del sistema de archivos, muestra el ID del punto de recuperación, el ID del sistema de archivos y el tipo de sistema de archivos.
5. En Opciones de restauración, hay varias posibilidades. En primer lugar, elija el Sistema de archivos del menú desplegable.
6. A continuación, elija la Máquina virtual de almacenamiento preferida del menú desplegable.
7. Escriba un nombre para su volumen.
8. Especifique la Ruta de unión, que es la ubicación dentro del sistema de archivos donde se montará el volumen.
9. Especifique en megabytes (MB) el Tamaño del volumen que va a crear.
10. De forma opcional, puede marcar la casilla para Habilitar la eficiencia de almacenamiento. Esto permitirá la deduplicación, la compresión y la compactación.
11. En el menú desplegable Política de clasificación por niveles de los grupos de capacidad, seleccione la preferencia de nivel.
12. En los permisos de restauración, elija la función de IAM que AWS Backup se utilizará para restaurar las copias de seguridad.
13. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Restauración de un sistema de archivos de Amazon FSx para OpenZFS

Para restaurar un sistema de archivos de FSx para OpenZFS

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y elija el ID del recurso de Amazon FSx que desee restaurar.

3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Elija el ID del punto de recuperación del recurso.
4. En la esquina superior derecha del panel, elija Restaurar para abrir la página Restaurar copia de seguridad.

   En la sección Detalles del sistema de archivos, el ID de la copia de seguridad se muestra en ID de copia de seguridad y el tipo de sistema de archivos se muestra en Tipo de sistema de archivos. El tipo de sistema de archivos debe ser FSx para OpenZFS.
5. En Opciones de restauración, puede seleccionar Restauración rápida o Restauración estándar. La restauración rápida utilizará la configuración predeterminada del sistema de archivos de origen. Si realiza una restauración rápida, vaya al paso 7.

   Si elige la restauración estándar, especifique las siguientes configuraciones adicionales:

   a. IOPS de SSD provisionadas: puede elegir el botón de opción Automático o puede elegir la opción Aprovisionado por el usuario, si está disponible.
   b. Capacidad de rendimiento: puede elegir la Capacidad de rendimiento recomendada de 64 MB/seg o Especificar la capacidad de rendimiento.
   c. (Opcional) Grupos de seguridad de VPC: puede especificar grupos de seguridad de VPC para asociarlos a la interfaz de red del sistema de archivos.
   d. Clave de cifrado: especifique la AWS Key Management Service clave para proteger los datos del sistema de archivos restaurados en reposo.
   e. (Opcional) Configuración del volumen raíz: esta configuración está comprimida de forma predeterminada. Para ampliarla, haga clic en el quilate (flecha) que apunta hacia abajo. Al crear un sistema de archivos a partir de una copia de seguridad, se creará un nuevo sistema de archivos; los volúmenes y las instantáneas retendrán sus configuraciones de origen.
   f. (Opcional) Copia de seguridad y mantenimiento: para configurar una copia de seguridad programada, haga clic en el quilate (flecha) que apunta hacia abajo para ampliar la sección. Puede elegir el intervalo de copia de seguridad, la hora y el minuto, el periodo de retención y el intervalo de mantenimiento semanal.
6. (Opcional) Puede introducir un nombre para el volumen.
7. La Capacidad de almacenamiento de SSD mostrará la capacidad de almacenamiento del sistema de archivos.
8. Elija la Nube privada virtual (VPC) desde la que se puede acceder a su sistema de archivos.

9. En el menú desplegable Subred, elija la subred en la que reside la interfaz de red del sistema de archivos.
10. En la sección Función de restauración, elija la función de IAM que AWS Backup utilizará para crear y gestionar las copias de seguridad en su nombre. Se recomienda elegir el Rol predeterminado. Si no hay un rol predeterminado, se creará uno automáticamente con los permisos adecuados. También puede elegir un rol de IAM.
11. Compruebe todas las entradas y elija Restaurar copia de seguridad.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon FSx

Para restaurar Amazon FSx mediante la API o la CLI, utilice `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de Amazon FSx:

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

Metadatos de restauración de FSx para Windows File Server

Puede especificar los siguientes metadatos durante una restauración de FSx para Windows File Server:

- ThroughputCapacity
- PreferredSubnetId

- ActiveDirectoryId

Metadatos de restauración de FSx para Lustre

Puede especificar los siguientes `PerUnitStorageThroughput` y `DriveCacheType` durante una restauración de FSx para Lustre.

Metadatos de restauración de FSx para ONTAP

Puede especificar los siguientes metadatos durante las restauraciones de FSx para ONTAP:

- Name #nombre del volumen que se va a crear
- OntapConfiguration: # configuración ontap
- `junctionPath`
- `sizeInMegabytes`
- `storageEfficiencyEnabled`
- `storageVirtualMachineId`
- `tieringPolicy`

Restauración de metadatos de FSx para OpenZFS

Puede especificar los siguientes metadatos durante las restauraciones de FSx para OpenZFS:

- `ThroughputCapacity`
- `DesklopsConfiguration`
- Si se especifican Iops, debe incluir un valor entre 0 y 160 000, pero no incluir Mode.

Ejemplo de comando de restauración de la CLI:

```
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\"}"'
```

Ejemplo de restauración de metadatos:

```
"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\\\"]\"}"
```

Restauración de un volumen de Amazon EBS

Al restaurar una instantánea de Amazon Elastic Block Store (Amazon EBS) AWS Backup , crea un nuevo volumen de Amazon EBS que puede adjuntar a su instancia de Amazon EC2.

Puede elegir restaurar una instantánea como un volumen de EBS o como un volumen de AWS Storage Gateway .

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon EBS

Para restaurar un volumen de Amazon EBS

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de EBS que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. Especifique los parámetros de restauración del recurso. Los parámetros de restauración establecidos son específicos del tipo de recurso seleccionado.

   En Tipo de recurso, elija el AWS recurso que se va a crear al restaurar esta copia de seguridad.
5. Si elige EBS volume (Volumen de EBS), proporcione los valores de Volume type (Tipo de volumen) y Size (GiB) (Tamaño [GiB]) y seleccione una zona de disponibilidad.

   - Después del Rendimiento, aparecerá una casilla de verificación opcional para Cifrar este volumen. Esta opción permanecerá activa si el punto de recuperación de EBS está cifrado.

     Puede especificar una clave KMS o puede crear una AWS KMS clave.

Si elige Volumen de Storage Gateway, elija una Puerta de enlace en un estado accesible. Elija también el Nombre de destino iSCSI.

- Para las puertas de enlace del Volumen almacenado, elija un ID de disco.
- Para las puertas de enlace del Volumen en caché, elija una capacidad que sea al menos tan grande como el recurso protegido.

6. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración.

> **Note**
>
> Si la función AWS Backup predeterminada no está presente en su cuenta, se creará una función predeterminada para usted con los permisos correctos. Puede eliminar este rol predeterminado o inutilizarlo.

7. Seleccione Restaurar copia de seguridad.

   Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

La restauración de una instantánea de EBS archivada la mueve temporalmente de almacenamiento en frío a almacenamiento en caliente para crear un nuevo volumen de EBS. Este tipo de restauración conlleva un cargo de recuperación único. Los costos de almacenamiento tanto en caliente como en frío se facturan durante este periodo de restauración. Los volúmenes de EBS almacenados en frío no se pueden restaurar en un volumen de Backup Gateway.

Puede restaurar una instantánea de EBS archivada en almacenamiento en frío mediante la consola de AWS Backup o la línea de comandos. Una restauración desde almacenamiento en frío puede tardar hasta 72 horas. Para obtener más información, consulte Archivar instantáneas de Amazon EBS en la Guía del usuario de Amazon EBS.

Console

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Vaya a Almacenes de copia de seguridad > *Almacén* > Restaurar instantánea de EBS archivada.

3. En la sección Configuración, introduzca un valor de 0 a 180, ambos inclusive, que especifique el número de días para restaurar temporalmente una instantánea archivada.
4. Introduzca otros ajustes: tipo de volumen, tamaño, IOPS, zona de disponibilidad, rendimiento y cifrado.
5. Elija su rol de restauración.
6. Seleccione Restaurar copia de seguridad. En la ventana emergente de confirmación, confirme las instantáneas y el tipo de restauración. A continuación, seleccione Restaurar instantánea.

AWS CLI

1. Utilizar `start-restore-job`
2. Incluya los parámetros.
3.
4.
5.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon EBS

Para restaurar Amazon EBS mediante la API o la CLI, utilice `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de 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
```

Ejemplo:

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

Restauración de un sistema de archivos de Amazon EFS

Si va a restaurar una instancia de Amazon Elastic File System (Amazon EFS), puede realizar una restauración completa o una restauración a nivel de elemento.

Restauración completa

Cuando se realiza una restauración completa, se restaura todo el sistema de archivos.

AWS Backup no admite restauraciones destructivas con Amazon EFS. Una restauración destructiva se produce cuando un sistema de archivos restaurado elimina o sobrescribe el sistema de archivos de origen o existente. En cambio, AWS Backup restaura el sistema de archivos en un directorio de recuperación fuera del directorio raíz.

Restauración a nivel de elemento

Al realizar una restauración a nivel de elemento, AWS Backup restaura un archivo o directorio específico. Debe especificar la ruta relativa a la raíz del sistema de archivos. Por ejemplo, si el sistema de archivos está montado en `/user/home/myname/efs` y la ruta de archivo es `user/home/myname/efs/file1`, escriba **`/file1`**. Las etiquetas distinguen entre mayúsculas y minúsculas. No se admiten caracteres comodín ni cadenas de expresiones regulares. La ruta puede ser diferente de la del host si el sistema de archivos se monta mediante un punto de acceso.

Puede seleccionar hasta 10 elementos si utiliza la consola para realizar una restauración de EFS. No hay límite de elementos cuando se utiliza la CLI para realizar restauraciones; sin embargo, hay un límite de 200 KB en la longitud de los metadatos de restauración que se pueden transferir.

Puede restaurar esos elementos en un sistema de archivos nuevo o existente. En cualquier caso, AWS Backup crea un nuevo directorio de Amazon EFS (`aws-backup-restore_`*`datetime`*) a partir del directorio raíz para contener los elementos. La jerarquía completa de los elementos especificados se conserva en el directorio de recuperación. Por ejemplo, si el directorio A contiene los subdirectorios B, C y D, AWS Backup mantiene la misma estructura jerárquica cuando se recuperan A, B, C y D. Independientemente de si realiza una restauración de nivel de elemento de Amazon EFS en un sistema de archivos existente o en un sistema de archivos nuevo, cada intento de restauración creará un nuevo directorio de recuperación fuera del directorio raíz que contendrá los archivos restaurados. Si intenta realizar varias restauraciones de la misma ruta, es posible que existan varios directorios que contengan los elementos restaurados.

> **Note**
>
> Si solo mantiene una copia de seguridad semanal, solo podrá restaurar el estado del sistema de archivos al momento en que realizó la copia de seguridad. No podrá restaurar copias de seguridad incrementales anteriores.

Utilice la AWS Backup consola para restaurar un punto de recuperación de Amazon EFS

Para restaurar un sistema de archivos de Amazon EFS

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Su almacén de copias de seguridad de EFS recibe la política de acceso `Deny backup:StartRestoreJob` al crearse. Si es la primera vez que va a restaurar el almacén de copias de seguridad, debe cambiar la política de acceso como se indica a continuación.
   a. Elija Almacenes de Backup.
   b. Elija el almacén de copias de seguridad que contenga el punto de recuperación que desea restaurar.
   c. Elija la Política de acceso al almacén.
   d. Si está presente, elimine `backup:StartRestoreJob` de `Statement`. Para ello, elija Editar, elimine `backup:StartRestoreJob` y, a continuación, elija Guardar política.
3. En el panel de navegación, elija Recursos protegidos y el ID del sistema de archivos de EFS que desee restaurar.
4. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID del sistema de archivos seleccionado. Para restaurar un sistema de archivos, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del sistema de archivos. En la esquina superior derecha del panel, elija Restaurar.
5. Especifique los parámetros de restauración del sistema de archivos. Los parámetros de restauración establecidos son específicos del tipo de recurso seleccionado.

   Puede realizar una restauración completa, que restaura todo el sistema de archivos. También puede restaurar archivos y directorios específicos mediante una restauración de nivel de elemento.

- Elija la opción Restauración completa para restaurar el sistema de archivos en su totalidad, incluidas todas las carpetas y archivos del nivel raíz.
- Elija la opción Restaurar a nivel de elemento para restaurar un archivo o directorio específico. Puede seleccionar y restaurar hasta cinco elementos en su Amazon EFS.

  Para restaurar un archivo o directorio concretos, debe especificar la ruta relativa relacionada con el punto de montaje. Por ejemplo, si el sistema de archivos está montado en `/user/home/myname/efs` y la ruta de archivo es `user/home/myname/efs/file1`, escriba **`/file1`**. Las rutas distinguen entre mayúsculas y minúsculas y no pueden contener caracteres especiales, caracteres comodín ni cadenas de expresiones regulares.

  1. En el cuadro de texto Ruta de elemento, escriba la ruta de acceso del archivo o la carpeta.
  2. Elija Agregar elemento para agregar otros archivos o directorios. Puede seleccionar y restaurar hasta cinco elementos en su sistema de archivos de EFS.

6. En Restore location (Ubicación de la restauración)

   - Elija Restaurar a un directorio del sistema de archivos de origen si desea restaurar al sistema de archivos de origen.
   - Elija Restaurar a un sistema de archivos nuevo si desea restaurar a otro sistema de archivos.

7. El Tipo de sistema de archivos.

   - (Recomendado) Elija Regional si desea restaurar el sistema de archivos en varias zonas de AWS disponibilidad.
   - Elija Una zona si desea restaurar el sistema de archivos en una única zona de disponibilidad. A continuación, en el menú desplegable de Zona de disponibilidad, elija el destino de la restauración.

   Para obtener más información, consulte Managing Amazon EFS storage classes en la Guía del usuario de Amazon EFS.

8. Para el Rendimiento

   - Si opta por realizar una restauración Regional, elija entre Uso general (recomendado) o Máximo de E/S.
   - Si opta por realizar una restauración de Una zona, tiene que elegir Uso general (recomendado). Las restauraciones de Una zona no admiten Máximo de E/S.

9. Para Habilitar el cifrado

- Elija Habilitar el cifrado si desea cifrar el sistema de archivos. Los identificadores de clave y los alias de KMS aparecen en la lista una vez creados con la consola AWS Key Management Service (AWS KMS).
- En el cuadro de texto Clave de KMS, elija la clave que desee utilizar de la lista.

10. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración.

> **Note**
>
> Si la función AWS Backup predeterminada no está presente en su cuenta, se creará una función predeterminada para usted con los permisos correctos. Puede eliminar este rol predeterminado o inutilizarlo.

11. Seleccione Restaurar copia de seguridad.

    Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

> **Note**
>
> Si solo mantiene una copia de seguridad semanal, solo podrá restaurar el estado del sistema de archivos al momento en que realizó la copia de seguridad. No podrá restaurar copias de seguridad incrementales anteriores.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon EFS

Utilice `StartRestoreJob`. Cuando restaure una instancia de Amazon EFS, puede restaurar un sistema de archivos completo o archivos y directorios específicos. Para restaurar recursos de Amazon EFS, necesita la siguiente información:

- `file-system-id`— El ID del sistema de archivos Amazon EFS del que se hace la copia de seguridad AWS Backup. Devuelta por `GetRecoveryPointRestoreMetadata`. Esto no es obligatorio cuando se restaura un nuevo sistema de archivos (este valor se ignora si el parámetro `newFileSystem` es`True`).

- `Encrypted`: un valor booleano que, si es verdadero, especifica que el sistema de archivos está cifrado. Si se especifica `KmsKeyId`, `Encrypted` se debe configurar en `true`.
- `KmsKeyId`— Especifica la AWS KMS clave que se utiliza para cifrar el sistema de archivos restaurado.
- `PerformanceMode`: especifica el modo de rendimiento del sistema de archivos.
- `CreationToken`: un valor proporcionado por el usuario que garantiza la exclusividad (idempotencia) de la solicitud.
- `newFileSystem`: un valor booleano que, si es verdadero, especifica que el punto de recuperación se restaura en un nuevo sistema de archivos de Amazon EFS.
- `ItemsToRestore` : una matriz de hasta cinco cadenas en la que cada cadena es una ruta de archivo. Utilice `ItemsToRestore` para restaurar archivos o directorios específicos en lugar de restaurar todo el sistema de archivos. Este parámetro es opcional.

También puede incluir `aws:backup:request-id`.

Las restauraciones de One Zone se pueden realizar mediante la inclusión de los siguientes parámetros:

```
"singleAzFilesystem": "true"
"availabilityZoneName": "ap-northeast-3"
```

Para obtener más información sobre los valores de configuración de Amazon EFS, consulte create-file-system.

Deshabilitación de las copias de seguridad automáticas en Amazon EFS

De forma predeterminada, Amazon EFS crea copias de seguridad de los datos automáticamente. Estas copias de seguridad se representan como puntos de recuperación en AWS Backup. Si se intenta eliminar el punto de recuperación, aparecerá un mensaje de error que indica que no hay suficientes privilegios para realizar la acción.

Se recomienda mantener activa esta opción de copia de seguridad automática. Especialmente en el caso de una eliminación accidental de datos, la copia de seguridad permite restaurar el contenido del sistema de archivos a la fecha del último punto de recuperación creado.

En el improbable caso de que desee desactivarlas, la política de acceso debe cambiarse de `"Effect": "Deny"` a `"Effect": "Allow"`. Consulte la Guía del usuario de Amazon EFS para obtener más información sobre cómo activar o desactivar las copias de seguridad automáticas.

Restauración de una tabla de Amazon DynamoDB

Utilice la AWS Backup consola para restaurar los puntos de recuperación de DynamoDB

Para restaurar una tabla de DynamoDB

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de DynamoDB que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. En Settings (Configuración), en el campo de texto New table name (Nuevo nombre de tabla), escriba un nuevo nombre de tabla.
5. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración.
6. Para Configuración de cifrado:

   a. Si DynamoDB administra la copia de seguridad (su ARN comienza por) AWS Backup , cifra la tabla restaurada `arn:aws:dynamodb` con una clave propia. AWS

      Para elegir una clave diferente para cifrar la tabla restaurada, puede utilizar la AWS Backup StartRestoreJoboperación o realizar la restauración desde la consola de DynamoDB.

   b. Si la copia de seguridad admite la AWS Backup administración completa (su ARN comienza por`arn:aws:backup`), puede elegir cualquiera de las siguientes opciones de cifrado para proteger la tabla restaurada:

      - (Predeterminada) Clave de KMS propiedad de DynamoDB (sin cargo adicional por el cifrado)
      - Clave de KMS administrada por DynamoDB (se aplican cargos de KMS)
      - Clave de KMS administrada por el cliente (se aplican cargos de KMS)

      Las claves “propiedad de DynamoDB” y “administradas por DynamoDB” son las mismas que las claves “propiedad de AWS” y “administradas por AWS”, respectivamente. Para

obtener más información, consulte Cifrado en reposo: cómo funciona en la Guía para desarrolladores de Amazon DynamoDB.

Para obtener más información sobre la AWS Backup administración completa, consulteCopia de seguridad avanzada de DynamoDB.

> **Note**
>
> La siguiente guía solo se aplica si restaura una copia de seguridad y desea cifrar la tabla restaurada con la misma clave que utilizó para cifrar la tabla original.
> Al restaurar una copia de seguridad entre regiones, para cifrar la tabla restaurada con la misma clave que utilizó para cifrar la tabla original, la clave debe ser multirregional. AWS-las claves propias y AWS administradas no son claves multirregionales. Para obtener más información, consulte Multi-Region keys en la Guía para desarrolladores de AWS Key Management Service .
> Al restaurar una copia de seguridad multicuenta, para cifrar la tabla restaurada con la misma clave que utilizaste para cifrar la tabla original, debes compartir la clave de la cuenta de origen con la de destino. AWS-las claves propias y AWS administradas no se pueden compartir entre cuentas. Para obtener más información, consulte Allowing users in other accounts to use a KMS key en la Guía para desarrolladores de AWS Key Management Service .

7. Seleccione Restaurar copia de seguridad.

   Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de DynamoDB

Utilice `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de DynamoDB: Los metadatos no distinguen entre mayúsculas y minúsculas.

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

A continuación, se muestra un ejemplo del argumento `restoreMetadata` de una operación `StartRestoreJob` en la CLI:

```
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
```

En el ejemplo anterior, se cifra la tabla restaurada con una AWS clave propia. La parte de los metadatos de restauración que especifica el cifrado mediante la clave AWS propiedad es:. `\"encryptionType\":\"Default\","kmsMasterKeyArn\":\"Not Applicable\"`

Para cifrar la tabla restaurada con una clave AWS administrada, especifique los siguientes metadatos de restauración:. `"encryptionType\":\"KMS\",\"kmsMasterKeyArn\":\"Not Applicable\"`

Para cifrar la tabla restaurada con una clave administrada por el cliente, especifique los siguientes metadatos de restauración: `"encryptionType \":\"KMS\",\"kmsMasterKeyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`.

Restauración de una base de datos de RDS

Para restaurar una base de datos de Amazon RDS, se han de especificar varias opciones de restauración. Para obtener más información acerca de estas opciones, consulte Copia de seguridad y restauración de una instancia de base de datos de Amazon RDS en la Guía del usuario de Amazon RDS.

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon RDS

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Amazon RDS que desee restaurar.

3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. En el panel Instance specifications (Especificaciones de la instancia), acepte los valores predeterminados o especifique las opciones de configuración de DB engine (Motor de base de datos), License Model (Modelo de licencias), DB instance class (Clase de instancia de base de datos), Multi-AZ y Storage type (Tipo de almacenamiento). Por ejemplo, si desea una instancia de base de datos en espera, especifique Multi-AZ.
5. En el panel de configuración, especifique un nombre que sea único para todas las instancias de bases de datos y los clústeres de su propiedad Cuenta de AWS en la región actual. El identificador de instancias de bases de datos no distingue entre mayúsculas y minúsculas, pero se almacena con todas las letras en minúsculas (como en "`mydbinstance`"). Este campo es obligatorio.
6. En el panel Red y seguridad, acepte los valores predeterminados o especifique las opciones para la configuración de la Nube Privada Virtual (VPC), el grupo de subredes, la accesibilidad pública (normalmente Sí) y la zona de disponibilidad.
7. En el panel Database options (Opciones de base de datos), acepte los valores predeterminados o especifique las opciones de configuración de Database port (Puerto de base de datos), DB parameter group (Grupo de parámetros de base de datos), Option Group (Grupo de opciones), Copy tags to snapshots (Copiar etiquetas en instantáneas) e IAM DB Authentication Enabled (Autenticación de base de datos de IAM habilitada).
8. En Cifrado, use la configuración predeterminada. Si la instancia de base de datos de origen de la instantánea se cifró, la instancia de base de datos restaurada también se cifrará. Este cifrado no se puede eliminar.
9. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
10. En el panel Maintenance (Mantenimiento), acepte el valor predeterminado o especifique la opción de Auto minor version upgrade (Actualización automática de versiones secundarias).
11. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.
12. Una vez que se hayan especificado todos los ajustes, elija Restore backup (Restaurar copia de seguridad).

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon RDS

Utilice `StartRestoreJob`. Para obtener información sobre los metadatos y los valores aceptados, consulte `RestoreDBInstanceFromDBSnapshot` en la Referencia de la API de Amazon RDS. Además, AWS Backup acepta los siguientes atributos únicamente informativos. Sin embargo, su inclusión no afectará a la restauración:

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

Restauración de un clúster de Amazon Aurora

Usa la AWS Backup consola para restaurar los puntos de recuperación de Aurora

AWS Backup restaura su clúster de Aurora; no crea ni adjunta una instancia de Amazon RDS a su clúster. En los siguientes pasos, creará y asociará una instancia de Amazon RDS al clúster de Aurora restaurado mediante la CLI.

La restauración de un clúster de Aurora requiere que especifique varias opciones de restauración. Para obtener información acerca de estas opciones, consulte Información general de copias de seguridad y restauración de un clúster de base de datos Aurora en la Guía del usuario de Amazon Aurora. Las especificaciones de las opciones de restauración se encuentran en la guía de la API de `RestoreDBClusterFromSnapshot`.

Para restaurar un clúster de Amazon Aurora

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Aurora que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el

botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.

4. En el panel Instance specifications (Especificaciones de la instancia), acepte los valores predeterminados o especifique las opciones de configuración de DB engine (Motor de base de datos), DB engine version (Versión del motor de base de datos) y Capacity type (Tipo de capacidad).

   > **Note**
   >
   > Si se selecciona el tipo de capacidad Serverless (Sin servidor), aparecerá el panel Capacity settings (Ajustes de capacidad). Especifique las opciones de configuración de Minimum Aurora capacity unit (Unidad mínima de capacidad de Aurora) y Maximum Aurora capacity unit (Unidad máxima de capacidad de Aurora) o elija diferentes opciones en la sección Additional scaling configuration (Configuración de escalado adicional).

5. En el panel de configuración, especifique un nombre que sea único para todas las instancias de clústeres de bases de datos que le Cuenta de AWS pertenezcan en la región actual.
6. En el panel Red y seguridad, acepte los valores predeterminados o especifique las opciones de configuración de Nube privada virtual (VPC), Grupo de subredes y Zona de disponibilidad.
7. En el panel Database options (Opciones de base de datos), acepte los valores predeterminados o especifique las opciones de configuración de Database port (Puerto de base de datos), DB cluster parameter group (Grupo de parámetros de clúster de base de datos) e IAM DB Authentication Enabled (Autenticación de base de datos de IAM habilitada).
8. En el panel Backup (Copia de seguridad), acepte el valor predeterminado o especifique la opción de configuración de Copy tags to snapshots (Copiar etiquetas en instantáneas).
9. En el panel Backtrack (Rastreo), acepte el valor predeterminado o especifique las opciones de configuración de Enable Backtrack (Habilitar rastreo) o Disable Backtrack (Deshabilitar rastreo).
10. En el panel Encryption (Cifrado), acepte el valor predeterminado o especifique las opciones de configuración de Enable encryption (Habilitar cifrado) o Disable encryption (Deshabilitar cifrado).
11. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
12. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.
13. Después de especificar todos los ajustes, elija Restore backup (Restaurar copia de seguridad).

Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

14. Una vez finalizada la restauración, asocie el clúster de Aurora restaurado a una instancia de Amazon RDS.

    Uso de la AWS CLI:

    - Para Linux, macOS o 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
    ```

    - Para 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
    ```

Consulte las copias de seguridad y point-in-time restauración continuas (PITR) para obtener información sobre las copias de seguridad continuas y la restauración en un momento determinado.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Aurora

Utilice `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de 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;
```

Ejemplo:

```
"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\":\"[]\"}"
```

Restauración de una instancia de Amazon EC2

Al restaurar una instancia EC2, AWS Backup crea una imagen de máquina de Amazon (AMI), una instancia, el volumen raíz de Amazon EBS, los volúmenes de datos de Amazon EBS (si el recurso protegido tenía volúmenes de datos) y las instantáneas de Amazon EBS. Puede personalizar algunos ajustes de la instancia mediante la AWS Backup consola o un mayor número de ajustes mediante el SDK o un SDK. AWS CLI AWS

Las siguientes consideraciones se aplican a la restauración de instancias de EC2:

- AWS Backup configura la instancia restaurada para que use el mismo par de claves que el recurso protegido usó originalmente. No puedes especificar un par de claves diferente para la instancia restaurada durante el proceso de restauración.
- AWS Backup no realiza copias de seguridad ni restaura los datos de usuario que se utilizan al lanzar una instancia de Amazon EC2.
- Al configurar la instancia restaurada, puede elegir entre utilizar el mismo perfil de instancia que el recurso protegido utilizó originalmente o lanzarla sin un perfil de instancia. Esto es para evitar la posibilidad de que se produzcan escalamientos de privilegios. Puede actualizar el perfil de la instancia restaurada mediante la consola Amazon EC2.

Si usa el perfil de instancia original, debe conceder AWS Backup los siguientes permisos, donde el ARN del recurso es el ARN del rol de IAM asociado al perfil de instancia.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

- Durante una restauración, se aplican todas las restricciones de configuración y cuotas de Amazon EC2.
- Si el almacén que contiene los puntos de recuperación de Amazon EC2 tiene un candado, consulte Consideraciones adicionales de seguridad para obtener más información.

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon EC2

puede restaurar una instancia Amazon EC2 completa desde un único punto de recuperación, incluidos el volumen raíz, los volúmenes de datos y algunos ajustes de configuración de la instancia, como el tipo de instancia y el key pair.

Para restaurar los recursos de Amazon EC2 mediante la consola AWS Backup

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y, a continuación, elija el ID del recurso de Amazon EC2 para abrir la página de detalles del recurso.
3. En el panel Puntos de recuperación, seleccione el botón de radio situado junto al ID del punto de recuperación que desee restaurar. En la esquina superior derecha del panel, elija Restaurar.
4. En el panel Configuración de red, utilizamos la configuración de la instancia protegida para seleccionar los valores predeterminados para el tipo de instancia, la VPC, la subred, el grupo de seguridad y el rol de IAM de la instancia. Puedes usar estos valores predeterminados o cambiarlos según sea necesario.
5. En el panel Restaurar funciones, utilice la función predeterminada o elija una función de IAM para especificar una función de IAM que conceda AWS Backup permiso para restaurar la copia de seguridad.

6. En el panel Etiquetas de recursos protegidos, seleccionamos Copiar etiquetas del recurso protegido al recurso restaurado de forma predeterminada. Si no desea copiar estas etiquetas, desactive la casilla de verificación.
7. En el panel de configuración avanzada, acepte los valores predeterminados de la configuración de la instancia o cámbielos según sea necesario. Para obtener información sobre estos ajustes, selecciona Información para que el ajuste abra su panel de ayuda.
8. Cuando termine de configurar la instancia, seleccione Restaurar copia de seguridad.

Restaure Amazon EC2 con AWS CLI

En la interfaz de línea de comandos, `start-restore-job`permite restaurar con un máximo de 32 parámetros (incluidos algunos parámetros que no se pueden personalizar a través de la AWS Backup consola).

La lista siguiente son los metadatos aceptados que puede transferir para restaurar un punto de recuperación de 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 acepta los siguientes atributos únicamente informativos. Sin embargo, su inclusión no afectará a la restauración:

```
vpcId
```

También puede restaurar instancias de Amazon EC2 sin incluir parámetros almacenados. Esta opción está disponible en la pestaña Recurso protegido de la consola de AWS Backup .

Restauración de un volumen de Storage Gateway

Si va a restaurar una instantánea de AWS Storage Gateway volumen, puede elegir restaurarla como un volumen de Storage Gateway o como un volumen de Amazon EBS. Esto se debe a que AWS Backup se integra con ambos servicios y cualquier instantánea de Storage Gateway se puede restaurar en un volumen de Storage Gateway o en un volumen de Amazon EBS.

Restaure Storage Gateway a través de la AWS Backup consola

Para restaurar un volumen de Storage Gateway

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Storage Gateway que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. Especifique los parámetros de restauración del recurso. Los parámetros de restauración establecidos son específicos del tipo de recurso seleccionado.

   En Tipo de recurso, elija el AWS recurso que se va a crear al restaurar esta copia de seguridad.
5. Si elige Volumen de Storage Gateway, elija una Puerta de enlace en un estado accesible. Elija también el Nombre de destino iSCSI.

   1. Para las puertas de enlace del “Volumen almacenado”, elija un ID de disco.

2. Para las puertas de enlace del “Volumen en caché”, elija una capacidad que sea al menos tan grande como el recurso protegido.

   Si elige EBS volume (Volumen de EBS), proporcione los valores de Volume type (Tipo de volumen) y Size (GiB) (Tamaño [GiB]) y seleccione una zona de disponibilidad.

6. En la función de restauración, elija la función de IAM que AWS Backup asumirá para esta restauración.

   > **Note**
   >
   > Si la función AWS Backup predeterminada no está presente en su cuenta, se creará una función predeterminada para usted con los permisos correctos. Puede eliminar este rol predeterminado o inutilizarlo.

7. Seleccione Restaurar copia de seguridad.

   Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.

Restaure Storage Gateway con AWS CLI

En la interfaz de línea de comandos, `start-restore-job` permite restaurar un volumen de Storage Gateway.

La siguiente lista contiene los metadatos aceptados.

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and Región de AWS.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

Restauración de una tabla de Amazon Timestream

Al restaurar una tabla de Amazon Timestream, hay varias opciones que configurar, como el nombre de la nueva tabla, la base de datos de destino, las preferencias de asignación de almacenamiento

(memoria y almacenamiento magnético) y el rol que utilizará para completar el trabajo de restauración. También puede elegir un bucket de Amazon S3 para almacenar los registros de errores. Las escrituras en el almacenamiento magnético son asíncronas, por lo que se recomienda registrar los errores.

El almacenamiento de datos de Timestream tiene dos niveles: un almacén en memoria y un almacén magnético. Se requiere un almacén en memoria, pero tiene la opción de transferir la tabla restaurada a un almacenamiento magnético una vez transcurrido el tiempo de memoria especificado. El almacén de memoria está optimizado para escrituras de datos de alto rendimiento y point-in-time consultas rápidas. El almacén magnético está optimizado para permitir escrituras de datos tardías con menor rendimiento, almacenamiento de datos a largo plazo y consultas analíticas rápidas.

Cuando restaura una tabla de Timestream, determina cuánto tiempo desea que la tabla permanezca en cada nivel de almacenamiento. Con la consola o la API, puede configurar el tiempo de almacenamiento de ambos. Tenga en cuenta que el almacenamiento es lineal y secuencial. Timestream almacenará primero la tabla restaurada en el almacenamiento en memoria y, a continuación, la transferirá automáticamente al almacenamiento magnético cuando se alcance el tiempo de almacenamiento en memoria.

> **Note**
>
> El periodo de retención del almacenamiento magnético debe ser igual o superior al periodo de retención original (que se muestra en la parte superior derecha de la consola) o se perderán datos.

Ejemplo: configura la asignación del almacén en memoria para que almacene los datos durante una semana y configura la asignación del almacenamiento magnético para que almacene los mismos datos durante un año. Cuando los datos del almacén en memoria cumplen una semana, se mueven automáticamente al almacén magnético. A continuación, se conservan en el almacén magnético durante un año. Al final de ese plazo, se eliminan de Timestream y de AWS Backup.

Para restaurar una tabla de Amazon Timestream mediante la consola AWS Backup

Puede restaurar las tablas de Timestream en la AWS Backup consola que fueron creadas por. AWS Backup

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.

2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Amazon Timestream que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. Especifique los ajustes de configuración de la nueva tabla, que incluyen:

   a. Nombre de tabla nueva, compuesto de 2 a 256 caracteres (letras, números, guiones, puntos y guiones bajos).

   b. Base de datos de destino, elegida en el menú desplegable.
5. Asignación de almacenamiento: establezca la cantidad de tiempo que la tabla restaurada residirá primero en el almacenamiento en memoria y, a continuación, la cantidad de tiempo que la tabla restaurada permanecerá en el almacenamiento magnético. El almacenamiento en memoria puede establecerse en horas, días, semanas o meses. El almacenamiento magnético puede establecerse en días, semanas, meses o años.
6. (Opcional) Habilitar escrituras de almacenamiento magnético: tiene la opción de permitir las escrituras en el almacenamiento magnético. Si esta opción está marcada, los datos que lleguen tarde, es decir, los datos con una marca temporal fuera del periodo de retención de memoria, se escribirán directamente en el almacén magnético.
7. (Opcional) Ubicación de los registros de errores de Amazon S3: puede especificar una ubicación de S3 en la que se almacenarán los registros de errores. Examine sus archivos de S3 o copie y pegue la ruta del archivo de S3.

   > **Note**
   >
   > Si decide especificar una ubicación para el registro de errores de S3, el rol que utilice para esta restauración debe tener permiso para escribir en un bucket de S3 o debe contener una política con ese permiso.
8. Elija el rol de IAM que desee transferir para realizar las restauraciones. Puede usar el rol de IAM predeterminado o especificar uno diferente.
9. Haga clic en Restaurar copia de seguridad.

Sus trabajos de restauración serán visibles en Recursos protegidos. Para ver el estado actual de su trabajo de restauración, haga clic en el botón de actualización o en CTRL-R.

Para restaurar una tabla de Amazon Timestream mediante la API, la CLI o el SDK

Utilice `StartRestoreJob` para restaurar una tabla de Timestream mediante la API.

Para restaurar un Timestream mediante AWS CLI, utilice la operación `start-restore-job.` y especifique los siguientes metadatos:

```
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
```

A continuación, se muestra una plantilla de ejemplo:

```
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
```

También puede utilizar `DescribeRestoreJob` para obtener información de la restauración.

En AWS CLI, utilice la operación `describe-restore-job` y utilice los siguientes metadatos:

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

A continuación, se muestra una plantilla de ejemplo:

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

Restauración de un clúster de Amazon Redshift

Puede restaurar instantáneas automáticas y manuales en la AWS Backup consola o mediante CLI.

Al restaurar un clúster de Amazon Redshift, la configuración original del clúster se introduce en la consola de forma predeterminada. Puede especificar diferentes ajustes para las siguientes configuraciones. Cuando restaure una tabla, tiene que especificar las bases de datos de origen y destino. Para obtener más información sobre estas configuraciones, consulte Restauración de un clúster desde una instantánea en la Guía de administración de Amazon Redshift.

- Una sola tabla o clúster: puede elegir entre restaurar un clúster completo o una sola tabla. Si decide restaurar una sola tabla, necesitará la base de datos de origen, el esquema de origen y el nombre de la tabla de origen, así como el clúster de destino, el esquema y el nombre de la nueva tabla.
- Tipo de nodo: cada clúster de Amazon Redshift consta de un nodo principal y al menos un nodo de computación. Al restaurar un clúster, tiene que especificar el tipo de nodo que cumpla con sus requisitos de CPU, RAM, capacidad de almacenamiento y tipo de unidad.
- Número de nodos: al restaurar un clúster, tiene que especificar el número de nodos necesarios.
- Resumen de la configuración
- Permisos de clúster

Para restaurar un clúster o una tabla de Amazon Redshift mediante la consola AWS Backup

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso deAmazon Redshift que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Puntos de recuperación, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.

4. Opciones de restauración

    a. Restaure el clúster de una instantána, o

    b. Restaure una sola tabla de una instantánea en un nuevo clúster. Si elige estas opciones, tiene que configurar lo siguiente:

        i. Activar o desactivar los nombres que distinguen entre mayúsculas y minúsculas.

        ii. Introducir los valores de la tabla de origen, incluida la base de datos, el esquema y la tabla. La información de la tabla de origen se encuentra en la consola de Amazon Redshift.

        iii. Introducir los valores de la tabla de destino, incluida la base de datos, el esquema y el nombre de la nueva tabla.

5. Especifique los ajustes de configuración del nuevo clúster.

    a. Para restaurar el clúster: elija el identificador del clúster, el tipo de nodo y el número de nodos.

    b. Especifique la zona de disponibilidad y los intervalos de mantenimiento.

    c. Para asociar roles adicionales, haga clic en Asociar roles de IAM.

6. Opcional: configuraciones adicionales:

    a. La opción Usar valores predeterminados está activada de forma predeterminada.

    b. Use los menús desplegables para seleccionar la configuración de redes y seguridad, grupos de seguridad de VPC, grupo de subredes del clúster y zona de disponibilidad.

    c. Active o desactive el Enrutamiento de VPC mejorado.

    d. Determine si quiere que el punto de conexión de su clúster sea accesible públicamente. Si es así, las instancias y los dispositivos fuera de la VPC pueden conectarse a la base de datos a través del punto de conexión del clúster. Si está activado, introduzca la dirección IP elástica.

7. Opcional: configuración de la base de datos. Puede optar por introducir lo siguiente

    a. Puerto de la base de datos (escriba en el campo de texto)

    b. Grupos de parámetros

8. Mantenimiento: puede elegir lo siguiente

    a. Periodo de mantenimiento

   b. Pista de mantenimiento, entre actual, de seguimiento o vista previa. Esto controla qué versión del clúster se aplica durante un intervalo de mantenimiento.

9. La instantánea automática está configurada de forma predeterminada.

   a. Periodo de retención de instantáneas automatizadas. El periodo de retención debe ser de 0 a 35 días. Elija 0 para no crear instantáneas automatizadas.

   b. El periodo de retención manual de las instantáneas es de 1 a 3653 días.

   c. Existe una casilla de verificación opcional para la reubicar el clúster. Si está marcada, permite reubicar el clúster en otra zona de disponibilidad. Una vez que haya habilitado la reubicación, puede usar el punto de conexión de VPC.

10. Supervisión: después de restaurar un clúster, puede configurar la supervisión a través CloudWatch de Amazon Redshift.

11. Elija el rol de IAM que desee transferir para realizar las restauraciones. Puede usar el rol predeterminado o especificar uno diferente.

Los trabajos de restauración sarán visibles en Trabajos. Para ver el estado actual de su trabajo de restauración, haga clic en el botón de actualización o en CTRL-R.

Restaurar un clúster de Amazon Redshift mediante la API, la CLI o el SDK

Utilice `StartRestoreJob` para restaurar un clúster de Amazon Redshift.

Para restaurar un Amazon Redshift mediante el AWS CLI, utilice el comando `start-restore-job` y especifique los siguientes metadatos:

```
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
```

Para obtener más información, consulte RestoreFromClusterSnapshot en la Referencia de la API de Amazon Redshift y restore-from-cluster-snapshot en la Guía de AWS CLI .

A continuación, se muestra una plantilla de ejemplo:

```
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 Región de AWS
-\-endpoint-url URL
```

A continuación se muestra un ejemplo:

```
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 \
```

También puede utilizar `DescribeRestoreJob` para obtener información de la restauración.

En AWS CLI, utilice la operación `describe-restore-job` y utilice los siguientes metadatos:

```
Region
```

A continuación, se muestra una plantilla de ejemplo:

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region Región de AWS
```

A continuación se muestra un ejemplo:

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

Restauración de una base de datos de SAP HANA en una instancia de Amazon EC2

Las bases de datos de SAP HANA en las instancias EC2 se pueden restaurar mediante la AWS Backup consola, mediante la API o mediante AWS CLI.

Temas

- Restaure una base de datos de instancias de SAP HANA en Amazon EC2 mediante la consola AWS Backup
- StartRestoreJob API para SAP HANA en EC2
- CLI para SAP HANA en EC2
- Resolución de problemas

Restaure una base de datos de instancias de SAP HANA en Amazon EC2 mediante la consola AWS Backup

Tenga en cuenta que los trabajos de copia de seguridad y restauración que involucren la misma base de datos no pueden realizarse simultáneamente. Cuando se realiza un trabajo de restauración

de una base de datos de SAP HANA, es probable que al intentar hacer una copia de seguridad de la misma base de datos se produzca un error: "Database cannot be backed up while it is stopped".

1. Acceda a la AWS Backup consola con las credenciales de los requisitos previos.
2. En el menú desplegable Ubicación de restauración de destino, elija una base de datos para sobrescribirla con el punto de recuperación que va a utilizar para la restauración (tenga en cuenta que la instancia que aloja la base de datos de destino de la restauración también debe tener los permisos establecidos en los requisitos previos).

   > **Important**
   >
   > Las restauraciones de bases de datos de SAP HANA son destructivas. La restauración de una base de datos sobrescribirá la base de datos en la ubicación de restauración de destino especificada.

3. Complete este paso solo si va a realizar una restauración de copia del sistema; de lo contrario, vaya al paso 4.

   Las restauraciones de copia del sistema son trabajos de restauración que restauran en una base de datos de destino diferente de la base de datos de origen que generó el punto de recuperación. Para las restauraciones de copia del sistema, observe el comando `aws ssm-sap put-resource-permission` que aparece en la consola. Este comando debe copiarse, pegarse y ejecutarse en la máquina que haya cumplido los requisitos previos. Al ejecutar el comando, utilice las credenciales del rol en el requisito previo en el que se configuran los permisos necesarios para registrar aplicaciones.

   ```
   // 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. Una vez que elija la ubicación de restauración, podrá ver el ID de recurso de la base de datos de destino, el Nombre de la aplicación, el Tipo de base de datos y la Instancia EC2.
5. Si lo desea, puede abrir la Configuración avanzada de restauración para cambiar la opción de restauración del catálogo. La selección predeterminada es restaurar el catálogo más reciente de AWS Backup.

6. Haga clic en Restaurar copia de seguridad.
7. La ubicación de destino se sobrescribirá durante la restauración (“restauración destructiva”), por lo que debe confirmar que lo permite en el siguiente cuadro de diálogo emergente.
   a. Para continuar, debe comprender que la base de datos existente se sobrescribirá con la que está restaurando.
   b. Una vez entendido esto, debe reconocer que los datos existentes se sobrescribirán. Para confirmarlo y continuar, escriba overwrite en el campo de entrada de texto.
8. Haga clic en Restaurar copia de seguridad.

Si el procedimiento tiene éxito, aparecerá un banner azul en la parte superior de la consola. Esto significa que el trabajo de restauración está en curso. Se le redirigirá automáticamente a la página de trabajos, donde su trabajo de restauración aparecerá en la lista de trabajos de restauración. Este trabajo más reciente tendrá un estado `Pending`. Puede buscar el ID del trabajo de restauración y, a continuación, hacer clic en él para ver los detalles de cada trabajo de restauración. Para actualizar la lista de trabajos de restauración, haga clic en el botón de actualización para ver los cambios en el estado del trabajo de restauración.

StartRestoreJob API para SAP HANA en EC2

Esta acción recupera el recurso guardado identificado por un nombre de recurso de Amazon (ARN).

Sintaxis de la solicitud

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parámetros de solicitud de URI: la solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud: la solicitud admite los siguientes datos en formato JSON:

IdempotencyTokenUna cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a las que, de otro modo, serían idénticas. `StartRestoreJob` Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Metadatos

Un conjunto de pares clave-valor de metadatos. Contiene información, como el nombre del recurso, necesaria para restaurar un punto de recuperación. Para obtener los metadatos de configuración de un recurso en el momento en que se realizó la copia de seguridad, solo tiene que llamar a `GetRecoveryPointRestoreMetadata`. Sin embargo, es posible que para restaurar un recurso se necesiten valores adicionales a los proporcionados por el recurso `GetRecoveryPointRestoreMetadata`. Por ejemplo, puede que tenga que proporcionar un nombre de recurso nuevo si el original ya existe.

Tiene que incluir metadatos específicos para restaurar SAP HANA en una instancia de Amazon EC2. Consulte los StartRestoreJob metadatos para ver los elementos específicos de SAP HANA.

Para recuperar los metadatos pertinentes, puede utilizar la llamada `GetRecoveryPointRestoreMetadata`.

Ejemplo de un punto de recuperación estándar de base de datos SAP HANA:

```
"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"
```

```
    }
```

Ejemplo de un punto de recuperación continuo de base de datos SAP HANA:

```
"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"
    }
```

CLI para SAP HANA en EC2

El comando `start-restore-job` recupera el recurso guardado identificado con un nombre de recurso de Amazon (ARN). La CLI seguirá la directriz de API anterior.

Sinopsis:

```
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]
```

Opciones

`--recovery-point-arn` (cadena) es una cadena en forma de número de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`.

`--metadata` (mapa): un conjunto de pares clave-valor de metadatos. Contiene información, como el nombre del recurso, necesaria para restaurar un punto de recuperación. Para obtener los metadatos de configuración de un recurso en el momento en que se realizó la copia de seguridad, solo tiene que llamar a `GetRecoveryPointRestoreMetadata`. Sin embargo, es posible que para restaurar un recurso se necesiten valores adicionales a los proporcionados por el recurso `GetRecoveryPointRestoreMetadata`. Tiene que especificar metadatos concretos para restaurar SAP HANA en una instancia de Amazon EC2:

- `aws:backup:request-id`: se trata de cualquier cadena de UUID utilizada para la idempotencia. No altera en modo alguno su experiencia de restauración.
- `aws:backup:TargetDatabaseArn`: especifique la base de datos en la que desee restaurar. Este es el ARN de la base de datos de SAP HANA en Amazon EC2.
- `CatalogRestoreOption`: especifique dónde restaurar el catálogo. Uno de `NO_CATALOG`, `LATEST_CATALOG_FROM_AWS_BACKUP`, `CATALOG_FROM_LOCAL_PATH`.
- `LocalCatalogPath`: Si el valor de CatalogRestoreOption los metadatos es`CATALOG_FROM_LOCAL_PATH`, especifique la ruta al catálogo local de la instancia EC2. Debe ser una ruta de archivo válida en la instancia de EC2.
- `RecoveryType`: actualmente se admiten los tipos de recuperación, `FULL_DATA_BACKUP_RECOVERY`, `POINT_IN_TIME_RECOVERY` y `MOST_RECENT_TIME_RECOVERY`.

clave = (cadena); valor = (cadena). Sintaxis abreviada:

```
KeyName1=string,KeyName2=string
```

Sintaxis de JSON:

```
{"string": "string"
  ...}
```

`--idempotency-token` es una cadena elegida por el usuario que puede utilizar para distinguir entre llamadas a `StartRestoreJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

`--resource-type` es una cadena que inicia un trabajo para restaurar un punto de recuperación para uno de los siguientes recursos: `SAP HANA on Amazon EC2` para SAP HANA en Amazon EC2. Opcionalmente, los recursos de SAP HANA se pueden etiquetar mediante el comando `aws ssm-sap tag-resource`.

Resultado: `RestoreJobId` es una cadena que identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Resolución de problemas

Si se produce alguno de los siguientes errores al intentar realizar una operación de copia de seguridad, consulte la resolución correspondiente.

- Error: error en el registro de copias de seguridad continuas

  Para mantener los puntos de recuperación para las copias de seguridad continuas, SAP HANA crea registros de todos los cambios. Si los registros no están disponibles, el estado de cada uno de estos puntos de recuperación continua es `STOPPED`. El último punto de recuperación viable que se puede utilizar para restaurar es uno que tenga el estado `AVAILABLE`. Si faltan datos de registro durante el tiempo transcurrido entre los puntos de recuperación con un estado `STOPPED` y los puntos con un estado `AVAILABLE`, no se puede garantizar que la restauración se realice correctamente en esos momentos. Si introduce una fecha y una hora dentro de este intervalo, AWS Backup intentará realizar la copia de seguridad, pero utilizará la hora de restauración más cercana disponible. Este error se muestra en el mensaje `“Encountered an issue with log backups. Please check SAP HANA for details."`

Solución: en la consola, se muestra la hora de restauración más reciente, con base en los registros. Puede introducir una hora más reciente que la que se muestra. Sin embargo, si los datos de este momento no están disponibles en los registros, AWS Backup utilizará la hora de restauración más reciente.

- Error: `Internal error`

  Solución: crea un caso de soporte desde la consola o ponte en contacto AWS Support con ellos con los detalles de la restauración, como el identificador del trabajo de restauración.

- Error: `The provided role arn:aws:iam::ACCOUNT_ID:role/ServiceLinkedRole cannot be assumed by AWS Backup`

  Solución: asegúrese de que el rol asumido al realizar la restauración tenga los permisos necesarios para crear roles vinculados a servicios.

- Error: `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:...`

  Solución: asegúrese de introducir correctamente el rol que se asume al solicitar los permisos de restauración descritos en los requisitos previos.

- Error: `b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n`

  Solución: asegúrese de que el agente Backint esté instalado correctamente. Compruebe todos los requisitos previos, especialmente el de instalar el AWS BackInt agente y el AWS Systems Manager de SAP en su servidor de aplicaciones SAP y, a continuación, vuelva a intentar instalar el BackInt agente.

- Error: `IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED`

  Solución: el flujo de trabajo del servicio canceló el trabajo de restauración. Vuelva a intentar el trabajo de restauración.

- Error: `RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"`

Solución: se está produciendo una inestabilidad de red transitoria en la instancia. Vuelva a intentar la restauración. Si este problema se produce de forma constante, intente agregar `ForceRetry: "true"` al archivo de configuración del agente en `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml`.

Para cualquier otro problema relacionado con el agente de AWS Backint, consulte Solución de problemas del AWS agente de Backint para SAP HANA.

Restauración de un clúster de DocumentDB

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon DocumentDB

La restauración de un clúster de Amazon DocumentDB requiere que especifique varias opciones de restauración. Para obtener información sobre estas opciones, consulte Restoring from a Cluster Snapshot en la Guía para desarrolladores de Amazon DocumentDB.

Para restaurar un clúster de Amazon DocumentDB

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Amazon DocumentDB que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. En el panel Configuración, acepte los valores predeterminados o especifique las opciones para Identificador del clúster, Versión del motor, Clase de instancia y Número de instancias.
   - NOTA: Si no hay una VPC predeterminada durante la restauración, debe especificar una subred en otra VPC.
5. En el panel Red y seguridad, aparecerá “Sin preferencias”.
6. En el ncryption-at-rest panel E, acepte el valor predeterminado o especifique las opciones para los ajustes Activar el cifrado o Desactivar el cifrado.
7. En el panel de Opciones de clúster, escriba el Puerto y elija el Grupo de parámetros de clúster.

8. En el panel Backup, seleccione backup continuo para point-in-time recuperación (PITR), backups de instantáneas programados o ambos.
9. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
10. En el panel Mantenimiento, especifique un intervalo de mantenimiento o elija Sin preferencias.
11. En el panel Etiquetas, elija Agregar etiqueta.
12. En el panel Protección contra eliminación, marque la casilla de verificación Habilitar la protección contra eliminación.
13. Después de especificar todos los ajustes, elija Restore backup (Restaurar copia de seguridad).

    Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.
14. Una vez finalizada la restauración, asocie el clúster de Amazon DocumentDB restaurado a una instancia de Amazon RDS.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Amazon DocumentDB

En primer lugar, restaure el clúster. Utilice `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de 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
```

A continuación, asocie el clúster de Amazon DocumentDB restaurado a una instancia de Amazon RDS mediante `create-db-instance`.

- Para Linux, macOS o Unix:

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- Para Windows:

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

Restauración de un clúster de Neptune

Utilice la AWS Backup consola para restaurar los puntos de recuperación de Amazon Neptune

Para restaurar una base de datos de Amazon Neptune, se han de especificar varias opciones de restauración. Para obtener información sobre estas opciones, consulte Restoring from a DB Cluster Snapshot en la Guía del usuario de Neptune.

Para restaurar una base de datos de Neptune

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Recursos protegidos y el ID del recurso de Neptune que desee restaurar.
3. En la página Detalles del recurso, se muestra una lista de puntos de recuperación para el ID de recurso seleccionado. Para restaurar un recurso, en el panel Copias de seguridad, active el botón de opción situado junto al ID del punto de recuperación del recurso. En la esquina superior derecha del panel, elija Restaurar.
4. En el panel Especificaciones de instancias, acepte los valores predeterminados o especifique el Motor de base de datos y la Versión.

5. En el panel de configuración, especifique un nombre que sea único para todas las instancias de clústeres de bases de datos que le Cuenta de AWS pertenezcan en la región actual. El identificador de clúster de bases de datos no distingue entre mayúsculas y minúsculas, pero se almacena con todas las letras en minúsculas (como en "`mydbclusterinstance`"). Este campo es obligatorio.
6. En el panel Opciones de base de datos, acepte los valores predeterminados o especifique las opciones de configuración de Puerto de base de datos, Grupo de parámetros de clúster de bases de datos y Autenticación de bases de datos de IAM habilitada.
7. En el panel Encryption (Cifrado), acepte el valor predeterminado o especifique las opciones de configuración de Enable encryption (Habilitar cifrado) o Disable encryption (Deshabilitar cifrado).
8. En el panel Exportaciones de registros, elija los tipos de registro que desee publicar en Amazon CloudWatch Logs. El rol de IAM ya se ha definido.
9. En el panel Restore role (Restaurar rol), elija el rol de IAM que AWS Backup asumirá para esta restauración.
10. Después de especificar todos los ajustes, elija Restore backup (Restaurar copia de seguridad).

    Aparecerá el panel Trabajos de restauración. En la parte superior de la página, aparecerá un mensaje con información sobre el trabajo de restauración.
11. Una vez finalizada la restauración, asocie el clúster de Neptune restaurado a una instancia de Amazon RDS.

Utilice la AWS Backup API, la CLI o el SDK para restaurar los puntos de recuperación de Neptune

En primer lugar, restaure el clúster. Utilice `StartRestoreJob`. Puede especificar los siguientes metadatos durante las restauraciones de 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
```

A continuación, asocie el clúster de Neptune restaurado a una instancia de Amazon RDS mediante `create-db-instance`.

- Para Linux, macOS o 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
```

- Para 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
```

Para obtener más información, consulte `RestoreDBClusterFromSnapshot` en la Referencia de la API de administración de Neptune y `restore-db-cluster-from-snapshot` en la Guía de la CLI de Neptune.

Restaure las copias CloudFormation de seguridad

Una copia de seguridad CloudFormation compuesta es una combinación de una CloudFormation plantilla y todos los puntos de recuperación anidados asociados. Se puede restaurar cualquier número de puntos de recuperación anidados, pero el punto de recuperación compuesto (que es el punto de recuperación de nivel superior) no se puede restaurar.

Al restaurar un punto de recuperación de una CloudFormation plantilla, se crea una pila nueva con un conjunto de cambios que representa la copia de seguridad.

Restaure CloudFormation con la AWS Backup consola;

Desde la CloudFormation consola puedes ver la nueva pila y el conjunto de cambios. Para obtener más información sobre los conjuntos de cambios, consulte Updating stacks using change sets en la Guía del usuario de AWS CloudFormation .

Determina los puntos de recuperación anidados desde los que deseas realizar la restauración con tu CloudFormation pila y, a continuación, restaúralos mediante la AWS Backup consola.

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Vaya a Almacenes de copia de seguridad, seleccione el almacén de copias de seguridad que contenga el punto de recuperación deseado y, a continuación, haga clic en Puntos de recuperación.
3. Restaure el punto AWS CloudFormation de recuperación de la plantilla.
    a. Haga clic en el punto de recuperación compuesto que contiene los puntos de recuperación anidados que desea restaurar para que aparezca la página de detalles del punto de recuperación compuesto.
    b. En Puntos de recuperación anidados, se mostrarán los puntos de recuperación anidados. Cada punto de recuperación tendrá un identificador de punto de recuperación, un estado, un identificador de recurso, un tipo de recurso, un tipo de copia de seguridad y la hora en que se creó el punto de recuperación. Haga clic en el botón de radio situado junto al punto AWS CloudFormation de recuperación y, a continuación, en Restaurar. Asegúrese de seleccionar el punto de recuperación que tenga el tipo de recurso: AWS CloudFormation y el tipo de copia de seguridad: copia de seguridad.
4. Cuando se complete el trabajo de restauración de la CloudFormation plantilla, la AWS CloudFormation plantilla restaurada estará visible en la AWS CloudFormation consola, en Stacks.
5. En Nombres de pilas, encontrará la plantilla restaurada con el estado `REVIEW_IN_PROGRESS`.
6. Haga clic en el nombre de la pila para ver los detalles de la pila.
7. Hay pestañas debajo del nombre de la pila. Haga clic en Conjuntos de cambios.
8. Ejecute el conjunto de cambios.
9. Tras este proceso, los recursos de la pila original se volverán a crear en la nueva pila. Los recursos con estado se volverán a crear vacíos. Para recuperar los recursos activos, vuelve a la lista de puntos de recuperación de la AWS Backup consola, selecciona el punto de recuperación que necesitas e inicia una restauración.

Restaure CloudFormation con AWS CLI

En la interfaz de línea de comandos, `start-restore-job`permite restaurar una CloudFormation pila.

La siguiente lista contiene los metadatos aceptados para restaurar un CloudFormation recurso.

```
// 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
```

Pruebas de restauración

Temas

Información general

Las pruebas de restauración, una función ofrecida por AWS Backup, proporcionan una evaluación automática y periódica de la viabilidad de la restauración, así como la capacidad de monitorear los tiempos de duración de las tareas de restauración.

En primer lugar se crea un plan de prueba de restauración en el que se indica un nombre para el plan, la frecuencia de las pruebas de restauración y la hora de inicio objetivo. A continuación, asigne los recursos que desea incluir en el plan. Luego, elige incluir puntos de recuperación específicos o aleatorios en la prueba. AWS Backup la copia de seguridad deduce de forma inteligente los metadatos que se necesitarán para que el trabajo de restauración se realice correctamente.

Cuando llegue la hora programada de su plan, AWS Backup inicia las tareas de restauración según su plan y supervisa el tiempo que se tarda en completar la restauración.

Cuando el plan de prueba de restauración termina de ejecutarse, puede utilizar los resultados para demostrar conformidad con los requisitos de la organización o de gobernanza, por ejemplo, la ejecución correcta de escenarios de prueba de restauración o la hora de finalización del trabajo de restauración.

Si lo desea, puede usarlo Restablecer la validación de las pruebas para confirmar los resultados de la prueba de restauración.

Una vez que se complete la validación opcional o se cierre la ventana de validación, AWS Backup elimina los recursos involucrados en la prueba de restauración y los recursos se eliminarán de acuerdo con los SLA del servicio.

Al final del proceso de prueba puede ver los resultados y la hora de finalización de las pruebas.

Pruebas de restauración comparadas con el proceso de restauración

Las pruebas de restauración ejecutan las tareas de restauración del mismo modo que las restauraciones bajo demanda y utilizan los mismos puntos de recuperación (copias de seguridad) que la restauración bajo demanda. Verá las llamadas CloudTrail (si ha optado por `StartRestoreJob` participar) para cada trabajo iniciado mediante las pruebas de restauración

Sin embargo, hay algunas diferencias entre la operación de una prueba de restauración programada y una operación de restauración bajo demanda:

	Pruebas de restauración	Restaurar
Cuenta	La práctica recomendada es designar una cuenta para utilizarla en las pruebas de restauración	Puede restaurar los recursos desde una cuenta
AWS Backup Audit Manager	Puede activar un control para confirmar si una prueba de restauración cumple los objetivos de restauración especificados	
Cadencia	Periódicamente como parte de un plan programado.	Bajo demanda
Regionalidad	Disponible en todas las regiones comerciales en las que AWS Backup opera, excepto en Israel (Tel Aviv) No disponible AWS GovCloud (EE. UU. Este), AWS GovCloud (EE. UU. Oeste), China (Pekín) y China (Ningxia).	Disponible en todas las regiones comerciales en las que opera AWS Backup
Recursos	Los tipos de recursos que puede asignar a su plan de prueba son: Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, Amazon FSx (Lustre, ONTAP, OpenZFS, Windows), Amazon Neptune, Amazon RDS y Amazon S3.	Pueden restaurarse todos los recursos.

	Pruebas de restauración	Restaurar
Resultados	Una vez que se completa el trabajo de prueba de restauración, el recurso restaurado se elimina una vez que finaliza la Restablecer la validación de las pruebas ventana.	Cuando finaliza el trabajo de restauración permanece la versión restaurada del recurso.
Etiquetas	En el caso de los tipos de recursos que admiten etiquetas en la restauración, las pruebas aplican etiquetas en la restauración.	Las etiquetas son opcionales para los recursos compatibles.

Restaurar la gestión de pruebas

Puede crear, ver, actualizar o eliminar un plan de prueba de restauración en la consola de AWS Backup.

Puede utilizar AWS CLI para realizar operaciones mediante programación en planes de prueba de restauración. Cada CLI es específica del AWS servicio en el que se origina. Los comandos deben ir precedidos de `aws backup`.

Eliminación de datos

Cuando finaliza una prueba de restauración, AWS Backup comienza a eliminar los recursos involucrados en la prueba. Esta eliminación no se realiza al instante. Cada recurso tiene una configuración subyacente que determina cómo se almacenan esos recursos y cómo se realiza su ciclo de vida. Por ejemplo, si los buckets de Amazon S3 forman parte de la prueba de restauración, se agregan al bucket reglas del ciclo de vida. La ejecución de las reglas y la eliminación completa del bucket y sus objetos pueden tardar varios días, pero solo se cobrará por estos recursos hasta el día en que se inicie la regla de ciclo de vida (de forma predeterminada, es 1 día). La velocidad de eliminación dependerá del tipo de recurso.

Los recursos que forman parte de un plan de prueba de restauración contienen una etiqueta llamada `awsbackup-restore-test`. Si un usuario elimina esta etiqueta, AWS Backup no podrá eliminar el recurso al final del período de prueba y, en su lugar, tendrá que eliminarlo manualmente.

Para comprobar por qué es posible que los recursos no se hayan eliminado como se esperaba, puede buscar en la consola los trabajos con error o utilizar la interfaz de línea de comandos para llamar a la solicitud de la API `DescribeRestoreJob` para recuperar los mensajes de estado de eliminación.

Los planes de Backup (planes de pruebas que no son de restauración) ignoran los recursos creados por las pruebas de restauración (aquellos `awsbackup-restore-test` cuya etiqueta o nombre comience por`awsbackup-restore-test`).

Control de costos

Las pruebas de restauración tienen un costo por prueba. Según los recursos incluidos en el plan de prueba de restauración, los trabajos de restauración que forman parte del plan también pueden tener un costo. Para obtener más información, consulte Precios de AWS Backup.

Al configurar un plan de prueba de restauración por primera vez, puede resultarle beneficioso incluir un número mínimo de tipos de recursos y recursos protegidos para familiarizarse con la característica, el proceso y los costos medios involucrados. Puede actualizar un plan después de su creación para añadir más tipos de recursos y recursos protegidos.

Creación de un plan de prueba de restauración

Un plan de prueba de restauración consta de dos partes: creación del plan y asignación de recursos.

Cuando se utiliza la consola, estas partes son secuenciales. En la primera parte se establecen el nombre, la frecuencia y las horas de inicio. En la segunda parte se asignan recursos al plan de prueba.

Cuando utilices una AWS CLI API, `create-restore-testing-plan`utilízala primero. Una vez que reciba una respuesta correcta y se haya creado el plan, utilice `create-restore-testing-selection` para cada tipo de recurso que desee incluir en el plan.

Console

Parte I: Crear un plan de prueba de restauración mediante la consola

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el menú de navegación de la izquierda, seleccione Prueba de restauración.
3. Elija Crear un plan de prueba de restauración.

4. General

    a. Nombre: escriba un nombre para el nuevo plan de prueba de restauración. El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos.

    b. Frecuencia de prueba: elija la frecuencia con la que se ejecutarán las pruebas de restauración.

    c. Hora de inicio: establezca la hora (en horas y minutos) a la que desea que comience la prueba. También puede configurar la zona horaria local en la que desea que se desarrolle el plan de prueba de restauración.

    d. Comenzar dentro: este valor (en horas) es el período de tiempo en el que está previsto que comience la prueba de restauración. AWS Backup hace todo lo posible por iniciar todas las tareas de restauración designadas durante el inicio dentro de un plazo determinado y distribuye aleatoriamente las horas de inicio dentro de este período.

5. Selección de puntos de recuperación: aquí puede configurar los almacenes de origen, el rango de puntos de recuperación y los criterios de selección para los puntos de recuperación (copias de seguridad) que desea incluir en el plan.

    a. Almacenes de origen: elija si desea incluir todos los almacenes disponibles o solo almacenes específicos para ayudar a filtrar los puntos de recuperación que pueden incluirse en el plan. Si elige almacenes específicos, seleccione en el menú desplegable los almacenes que desea incluir.

    b. Puntos de recuperación aptos: especifique el periodo de tiempo del que se seleccionarán puntos de recuperación. Puede seleccionar de 1 a 365 días, de 1 a 52 semanas, de 1 a 12 meses o 1 año.

    c. Criterios de selección: una vez especificado el rango de fechas de los puntos de recuperación, puede elegir si desea incluir el último o uno aleatorio en el plan. Puede resultar conveniente elegir uno aleatorio para evaluar el estado general de los puntos de recuperación con mayor frecuencia en el caso de que en algún momento esté justificado restaurar a una versión anterior.

    d. P puntos de oint-in-time recuperación: si su plan incluye recursos con puntos de respaldo continuo (point-in-time-restore/PITR), puede marcar esta casilla para que su plan de pruebas incluya los respaldos continuos como puntos de recuperación elegibles (consulte Disponibilidad de funciones por recurso para ver qué tipos de recursos tienen esta función).

6. (opcional) Etiquetas agregada al plan de prueba de restauración: puede agregar hasta 50 etiquetas al plan de prueba de restauración. Cada etiqueta debe agregarse por separado. Para agregar una etiqueta, elija Agregar nueva etiqueta.

Parte II: Asignar recursos al plan mediante la consola

En esta sección, elija los recursos de los que ha hecho una copia de seguridad para incluirlos en el plan de prueba de restauración. Elija el nombre de la asignación de recursos, el rol utilizado para la prueba de restauración y el periodo de retención antes de la limpieza. A continuación, seleccione el tipo de recurso, seleccione el ámbito y, si lo desea, ajuste la selección con etiquetas.

> **Tip**
>
> Para volver al plan de prueba de restauración al que desea agregar recursos, puede ir a la consola de AWS Backup, seleccionar Prueba de restauración y, a continuación, buscar el plan de prueba que prefiera y seleccionarlo.

1. General

   a. Nombre de asignación de recursos: introduzca un nombre para esta asignación de recursos mediante una cadena de caracteres alfanuméricos y guiones bajos, sin espacios en blanco.

   b. Restaurar el rol de IAM: la prueba debe utilizar el rol de IAM (Identity and Access Management) que designe. Puede elegir el rol AWS Backup predeterminado o uno diferente. Si el AWS Backup predeterminado aún no existe al finalizar este proceso, lo AWS Backup creará automáticamente con los permisos necesarios. El rol de IAM que elija para las pruebas de restauración debe contener los permisos que se encuentran en AWSBackupServicePolicyForRestores.

   c. Periodo de retención antes de la limpieza: durante una prueba de restauración, los datos de copia de seguridad se restauran temporalmente. De forma predeterminada, estos datos se eliminan una vez finalizada la prueba. Tiene la opción de demorar la eliminación de estos datos si desea ejecutar la validación de la restauración.

      Si planea ejecutar la validación, seleccione Retener durante un número específico de horas e introduzca un valor de 1 a 168 horas, ambos incluidos. Tenga en cuenta que la

validación se puede ejecutar mediante programación, pero no desde la consola de AWS Backup .

2. Recursos protegidos:

   a. Seleccionar el tipo de recurso: seleccione los tipos de recursos y el ámbito de las copias de seguridad de esos tipos que desea incluir en el plan de prueba de recursos. Cada plan puede contener varios tipos de recursos, pero cada tipo de recurso debe asignarse al plan de forma individual.

   b. Alcance de la selección de recursos: una vez elegido el tipo, seleccione si desea incluir todos los recursos protegidos disponibles de ese tipo o si desea incluir únicamente recursos protegidos específicos.

   c. (opcional) Refinar selección de recursos mediante etiquetas: si sus copias de seguridad tienen etiquetas, puedes filtrarlas por etiquetas para seleccionar recursos protegidos específicos. Introduzca la clave de la etiqueta, la condición para que esta clave se incluya o no y el valor de la clave. A continuación, seleccione el botón Añadir etiquetas.

      Las etiquetas de los recursos protegidos se evalúan comprobando las etiquetas del último punto de recuperación del almacén de copia de seguridad que contiene el recurso protegido.

3. Parámetros de restauración: algunos recursos requieren la especificación de parámetros para preparar un trabajo de restauración. En la mayoría de los casos, AWS Backup deducirá los valores en función de la copia de seguridad almacenada.

   En la mayoría de los casos, se recomienda mantener estos parámetros; sin embargo, puede cambiar los valores realizando una selección diferente en el menú desplegable. Algunos ejemplos en los que el cambio de los valores puede ser óptimo son: anulación de claves de cifrado, ajustes de Amazon FSx cuando no se puedan inferir datos y creación de subredes.

   Por ejemplo, si una base de datos de RDS es uno de los tipos de recursos que asigna a su plan de prueba de restauración, parámetros como zona de disponibilidad, nombre de la base de datos, clase de instancia de base de datos y grupo de seguridad de VPC aparecerán con valores inferidos que puede cambiar si lo desea.

AWS CLI

El comando de la CLI `CreateRestoreTestingPlan` sirve para crear un plan de prueba de restauración.

El plan de prueba debe contener:

- `RestoreTestingPlan`, que debe contener un `RestoreTestingPlanName` único
- Expresión cron `ScheduleExpression`
- `RecoveryPointSelection`

  Aunque se llama de manera similar, NO es lo mismo `RestoreTestingSelection` que.

  `RecoveryPointSelection`tiene cinco parámetros (tres obligatorios y dos opcionales). Los valores que especifique determinan qué punto de recuperación se incluye en la prueba de restauración. Debe indicar `Algorithm` si desea incluir el último punto de recuperación dentro del suyo `SelectionWindowDays` o si desea un punto de recuperación aleatorio, y debe indicar a través `IncludeVaults` de qué bóvedas se pueden elegir los puntos de recuperación.

Una selección puede tener uno o varios ARN de recursos protegidos o una o varias condiciones, pero no ambos.

También puede incluir:

- `ScheduleExpressionTimezone`
- `Tags`
- `CreatorRequestId`
- `StartWindowHours`

Utilice el comando de la CLI `create-restore-testing-plan.`

Una vez que el plan se haya creado correctamente, debe asignarle recursos utilizando `create-restore-testing-selection`.

Consta de `RestoreTestingSelectionName`, `ProtectedResourceType` y uno de los siguientes elementos:

- `ProtectedResourceArns`

- `ProtectedResourceConditions`

Cada tipo de recurso protegido puede tener un único valor. Una selección de pruebas de restauración puede incluir un valor comodín ("*") como `ProtectedResourceArns` junto con `ProtectedResourceConditions`. También puede incluir hasta 30 ARN de recursos protegidos específicos en `ProtectedResourceArns`.

Determinación del punto de recuperación

Cada vez que se ejecuta un plan de pruebas (según la frecuencia y la hora de inicio especificadas), la prueba de restauración restaura un punto de recuperación apto por cada recurso protegido seleccionado. Si ningún punto de recuperación de un recurso cumple los criterios de selección de puntos de recuperación, ese recurso no se incluirá en la prueba.

Un punto de recuperación para un recurso protegido seleccionado en una prueba es elegible si cumple los criterios del período de tiempo especificado e incluye almacenes en el plan de pruebas de restauración.

Se selecciona un recurso protegido si la selección de recursos para la prueba incluye el tipo de recurso y si se cumple alguna de las siguientes condiciones:

- El ARN del recurso se especifica en esa selección; o
- Las condiciones de etiqueta de esa selección coinciden con las etiquetas del último punto de recuperación del recurso

Actualizar un plan de prueba de restauración

Puede actualizar partes de su plan de prueba de restauración y las selecciones de recursos que contiene a través de la consola o de AWS CLI.

Console

Actualizar planes y selecciones de prueba de restauración en la consola

Cuando ve la página de detalles del plan de prueba de restauración en la consola, puede editar (actualizar) muchos de los ajustes del plan. Para ello,

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el menú de navegación de la izquierda, seleccione Prueba de restauración.
3. Seleccione el botón Editar.

4. Ajuste la frecuencia, la hora de inicio y la hora en que comenzará la prueba después de la hora de inicio elegida.
5. Guarde los cambios.

AWS CLI

Actualice los planes y selecciones de pruebas de restauración mediante AWS CLI

Solicita UpdateRestoreTestingPlany se UpdateRestoreTestingSelectionpuede utilizar para enviar actualizaciones parciales a un plan o selección específicos. Los nombres no se pueden cambiar, pero puede actualizar otros parámetros. Incluya solo los parámetros que desee cambiar en cada solicitud.

Antes de enviar una solicitud de actualización, utilice GetRestoreTestingPlany GetRestoreTestingSelectionpara determinar si la suya RestoreTestingSelection contiene ARN específicos o si utiliza el comodín y las condiciones.

Si la selección de las pruebas de restauración ha especificado ARN (en lugar de un comodín) y desea cambiarlos por un comodín con condiciones, la solicitud de actualización debe incluir tanto el comodín del ARN como las condiciones. Una selección puede tener ARN de recursos protegidos o utilizar el comodín con condiciones, pero no puede tener ambos.

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`
- `update-restore-testing-selection`

Visualización de planes de prueba de restauración existentes

Console

Vea los detalles sobre un plan de prueba de restauración existente y los recursos asignados en la consola

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.

2. En el menú de navegación de la izquierda, seleccione Prueba de restauración. La pantalla muestra sus planes de prueba de restauración. Los planes se muestran de forma predeterminada por último tiempo de ejecución.
3. Seleccione el enlace de un plan para ver sus detalles, incluido un resumen del plan, su nombre, frecuencia, hora de inicio y valor de inicio.

También puede ver los recursos protegidos de este plan, los trabajos de pruebas de restauración de los últimos 30 días incluidos en este plan y cualquier etiqueta que haya creado para formar parte de este plan de prueba.

AWS CLI

Obtenga detalles sobre un plan de prueba de restauración existente y la selección de pruebas mediante la línea de comandos

- `list-restore-testing-plan`
- `list-restore-testing-selections`
- `get-restore-testing-plan`
- `get-restore-testing-selection`

Visualización de los trabajos de prueba de restauración

Console

Visualización de trabajos de prueba de restauración existentes en la consola

Los trabajos de prueba de restauración se incluyen en la página de trabajos de restauración.

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Navegue a la página Trabajos.

   Como alternativa, puede seleccionar Prueba de restauración y, a continuación, seleccionar un plan de prueba de restauración para ver sus detalles y los trabajos asociados al plan.
3. Seleccione la pestaña Trabajos de restauración.

   En esta página puede ver el estado, la hora de restauración, el tipo de restauración, el identificador del recurso, el tipo de recurso, el plan de prueba de restauración al que

pertenece el trabajo, la hora de creación y el identificador del punto de recuperación del trabajo de restauración.

Los trabajos incluidos en un plan de prueba de restauración tienen el tipo de restauración Prueba.

Los trabajos de prueba de restauración tienen varias categorías de estado:

- El tipo de estado que requiere atención aparece subrayado; pase el ratón sobre el estado para ver detalles adicionales, si están disponibles.
- Si se Restablecer la validación de las pruebas ha iniciado la prueba, aparecerá un estado de validación (no disponible en la consola).
- El estado de eliminación indica el estado de los datos generados por la prueba de restauración. Hay tres estados de eliminación posibles: Correcto, Eliminando y Error.

  Si se produce un error al eliminar un trabajo de prueba de restauración, tendrá que eliminar el recurso manualmente, ya que el flujo de la prueba de restauración no ha podido completarlo automáticamente. A menudo, si se quita la etiqueta `awsbackup-restore-test` del recurso, se desencadena un error de eliminación.

AWS CLI

Visualización de trabajos de prueba de restauración existentes en la línea de comandos

- `list-restore-jobs-by-protected-resource`

Eliminación de un plan de prueba de restauración

Console

Eliminación del plan de prueba de restauración en la consola

1. Vaya a Visualización de planes de prueba de restauración existentes para ver sus planes de prueba de restauración actuales.
2. En la página de detalles del plan de prueba de restauración, elimine un plan seleccionando Eliminar.

3. Después de seleccionar Eliminar, aparecerá una pantalla emergente para confirmar de que desea eliminar el plan. En esta pantalla, el nombre del plan de prueba de restauración específico aparecerá en negrita. Para continuar, escriba el nombre exacto del plan de prueba, distinguiendo mayúsculas y minúsculas, incluidos guiones bajos, guiones y puntos.

   Si no se puede seleccionar la opción Eliminar el plan de prueba de restauración, vuelva a introducir el nombre hasta que coincida con el nombre mostrado. Cuando coincida exactamente, se podrá seleccionar la opción de eliminar el plan de prueba de restauración.

AWS CLI

Eliminación del plan de prueba de restauración mediante la línea de comandos

El comando CLI se DeleteRestoreTestingSelectionpuede usar para eliminar una selección de pruebas de restauración. Incluya `RestoreTestingPlanName` y `RestoreTestingSelectionName` en la solicitud.

Todas las selecciones de pruebas asociadas a un plan de prueba deben eliminarse antes de eliminar el plan de prueba. Una vez eliminadas todas las selecciones de prueba, puedes usar la solicitud de API DeleteRestoreTestingPlanpara eliminar un plan de pruebas de restauración. Debe incluir `RestoreTestingPlanName`.

- `delete-restore-testing-selection`
- `delete-restore-testing-plan`

Auditoría de pruebas de restauración

Restaure las integraciones de las pruebas con AWS Backup Audit Manager para ayudarlo a evaluar si un recurso restaurado se completó dentro del tiempo de restauración previsto.

Para obtener más información, consulte el control Tiempo de restauración para que los recursos cumplan el objetivo en Controles y corrección de AWS Backup Audit Manager.

Restauración de cuotas y parámetros de prueba

- 100 planes de prueba de restauración
- Se pueden agregar 50 etiquetas a cada plan de prueba de restauración
- 30 selecciones por plan

- 30 ARN de recursos protegidos por selección
- 30 condiciones de recursos protegidos por selección (incluidas las que se encuentran en `StringEquals` y `StringNotEquals`)
- 30 selectores de almacén por selección
- Días del periodo máximo de selección: 365 días
- Horas del periodo de inicio: mínimo: 1 hora; máximo: 168 horas (7 días)
- Longitud máxima del nombre del plan: 50 caracteres
- Longitud máxima del nombre de la selección: 50 caracteres

Puede consultar información adicional sobre los límites en AWS Backup cuotas.

Restaure la solución de problemas de errores

Si tiene trabajos de pruebas de restauración con un estado de restauración de`Failed`, los siguientes motivos pueden ayudarle a determinar la causa y la solución.

Los mensajes de error se pueden ver en la AWS Backup consola, en la página de detalles del estado del trabajo o mediante los comandos CLI `list-restore-jobs-by-protected-resource` o`list-restore-jobs`.

1. Error: *`No default VPC for this user. GroupName is only supported for EC2-Classic and default VPC.`*

   Solución 1: actualice la selección de pruebas de restauración y anule el parámetro`SubnetId`. La AWS Backup consola muestra este parámetro como «Subred».

   Solución 2: vuelva a crear la VPC predeterminada.

   Tipos de recursos afectados: Amazon EC2

2. Error: *`No subnets found for the default VPC [vpc]. Please specify a subnet.`*

   Solución 1: actualice la selección de pruebas de restauración y anule el parámetro de `SubnetId` restauración. La AWS Backup consola muestra este parámetro como «Subred».

   Solución 2: cree una subred predeterminada en la VPC predeterminada.

   Tipos de recursos afectados: Amazon EC2

3. Error: *No default subnet detected in VPC. Please contact AWS Support to recreate default Subnets.*

   Solución 1: actualice la selección de pruebas de restauración y anule el parámetro de `DBSubnetGroupName` restauración. La AWS Backup consola muestra este parámetro como grupo de subredes.

   Solución 2: cree una subred predeterminada en la VPC predeterminada.

   Tipos de recursos afectados: Amazon Aurora, Amazon DocumentDB, Amazon RDS, Neptune

4. Error:. *IAM Role cannot be assumed by AWS Backup*

   Solución: la función de restauración debe ser asumible por AWS Backup. Actualice la política de confianza del rol en IAM para permitir que lo asuma `"backup.amazonaws.com"` o actualice su selección de pruebas de restauración para utilizar un rol que pueda asumir. AWS Backup

   Tipos de recursos afectados: todos

5. Error: *Access denied to KMS key.* o *The specified AWS KMS key* ARN *does not exist, is not enabled or you do not have permissions to access it.*

   Solución: compruebe lo siguiente:

   a. La función de restauración tiene acceso a la AWS KMS clave utilizada para cifrar las copias de seguridad y, si corresponde, a la clave de KMS utilizada para cifrar el recurso restaurado.
   b. Las políticas de recursos de las claves de KMS anteriores permiten que la función de restauración acceda a ellas.

   Si aún no se cumplen las condiciones anteriores, configure la función de restauración y las políticas de recursos para el acceso adecuado. A continuación, vuelva a ejecutar el trabajo de prueba de restauración.

   Tipos de recursos afectados: todos

6. Errores: *User ARN is not authorized to perform action on resource because no identity based policy allows the action.* o*Access denied performing s3:CreateBucket on awsbackup-restore-test-xxxxxx*.

Solución: la función de restauración no tiene los permisos adecuados. Actualice los permisos en IAM para la función de restauración.

Tipos de recursos afectados: todos

7. Errores: *User ARN is not authorized to perform action on resource because no resource-based policy allows the action.* o *User ARN is not authorized to perform action on resource with an explicit deny in a resource based policy.*

   Solución: la función de restauración no tiene un acceso adecuado al recurso especificado en el mensaje. Actualice la política de recursos del recurso mencionado.

   Tipos de recursos afectados: todos

Restauración de metadatos inferidos de las pruebas

La restauración de un punto de recuperación requiere la restauración de los metadatos. Para realizar pruebas de restauración, AWS Backup infiere automáticamente metadatos que pueden permitir una restauración satisfactoria. El comando se `get-restore-testing-inferred-metadata` puede utilizar para previsualizar lo que AWS Backup se deduce. El comando `get-restore-job-metadata` devuelve el conjunto de metadatos inferido por. AWS Backup Tenga en cuenta que, para algunos tipos de recursos (Amazon FSx), no AWS Backup es capaz de deducir un conjunto completo de metadatos.

Los metadatos de restauración inferidos se determinan durante el proceso de prueba de restauración. Puede anular determinadas claves de metadatos de restauración incluyendo el parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Algunas anulaciones de metadatos no están disponibles en la consola. AWS Backup

Cada recurso compatible tiene claves y valores de metadatos de restauración inferidos y claves de metadatos de restauración anulables. Solo es necesario incluir los pares de valores de clave o los pares de valores de clave anidados de `RestoreMetadataOverrides` marcados como *obligatorios para restauración correcta*; los demás son opcionales. Tenga en cuenta que los valores de clave no distinguen entre mayúsculas y minúsculas.

> **Important**
>
> AWS Backup puede deducir que un recurso debe restaurarse a la configuración predeterminada, como una instancia de Amazon EC2 o un clúster de Amazon RDS restaurado a la VPC predeterminada. Sin embargo, si el valor predeterminado no está presente (por ejemplo, se ha eliminado la VPC o subred predeterminada y no se ha introducido ninguna anulación de metadatos), la restauración no se realizará correctamente.

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

DynamoDB	`deletionProtection` , donde el valor se establece en `false`
	
	`encryptionType` toma el valor `Default`
	
	`targetTableName` , donde el valor se establece en un valor aleatorio que empieza por `awsbackup-restore-test-`
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` , cuyo valor se establece en una zona de disponibilidad aleatoria
	
	`encrypted` , cuyo valor se establece en `true`
		`availabilityZone`
		
		`kmsKeyId`

Amazon EC2	El valor de `disableApiTermination` se establece en `false`	`iamInstanceProfileName` el valor puede ser nulo o `UseBackedUpValue`
		
		`instanceType`

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

	El valor de `instanceType` se establece en el instancEtype del punto de recuperación que se está restaurando
	
	El valor de `requiredImdsV2` se establece en `true`
		`requireImdsV2`
		
		`securityGroupIds`
		
		`subnetId`

Amazon EFS	El valor de `encrypted` se establece en `true` El valor de `file-system-id` se establece en el ID del sistema de archivos del punto de recuperación que se está restaurando `kmsKeyId value` toma el valor `alias/aws/elasticfilesystem` El valor de `newFileSystem` se establece en `true` El valor de `performanceMode` se establece en `generalPurpose`	`kmsKeyId`

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

Amazon FSx para Lustre	`lustreConfiguration` tiene claves anidadas. Una clave anidada es `automaticBackupRetentionDays`, cuyo valor se establece en `0`	`kmsKeyId`
		
		`lustreConfiguration` tiene la clave anidada `logConfiguration`
		
		`securityGroupIds`
		
		`subnetIds`, *obligatorios para restauración correcta*

Amazon FSx para ONTAP NetApp	`name` se establece en un valor aleatorio que empieza por `awsbackup_restore_test_` `ontapConfiguration` tiene claves anidadas, incluidas: • `junctionPath` donde `/name` es el nombre del volumen que se está restaurando • `sizeInMegabytes`, cuyo valor se establece en el tamaño en megabytes del punto de recuperación que se está restaurando • `snapshotPolicy` cuyo se establece en `none`	`ontapConfiguration` tiene claves anidadas anulables específicas, incluidas: • `junctionPath` • `ontapVolumeType` • `securityStyle` • `sizeInMegabytes` • `storageEfficiencyEnabled` • `storageVirtualMachineId`, *obligatorios para restauración correcta* • `tieringPolicy`

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

Amazon FSx para OpenZFS	`openZfzConfiguration` , que tiene claves anidadas, incluidas:
	• `automaticBackupRetentionDays` con valor establecido en `0`
	• `deploymentType` con un valor establecido en el tipo de implementación del punto de recuperación que se está restaurando
	• `throughputCapacity` , cuyo valor se basa en el `deploymentType` . Si `deploymentType` es `SINGLE_AZ_1` , el valor se establece en 64; si `deploymentType` es `SINGLE_AZ_2 or MULTI_AZ_1` , el valor se establece en `160`
		`kmsKeyId`
		`openZfsConfiguration` tiene claves anidadas anulables específicas, incluidas:
		• `deploymentType`
		• `throughputCapacity`
		• `diskiopsConfiguration`
		`securityGroupIds`
		`subnetIds`

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

Amazon FSx para Windows File Server	`windowsConfiguration` , que tiene claves anidadas, incluidas:
	• `automaticBackupRetentionDays` con valor establecido en `0`
	• `deploymentType` con un valor establecido en el tipo de implementación del punto de recuperación que se está restaurando
	• `throughputCapacity` con valor establecido en `8`
		`kmsKeyId`
		`securityGroupIds`
		`subnetIds` *obligatorios para restauración correcta*
		`windowsConfiguration` , con claves anidadas anulables específicas
		• `throughputCapacity`
		• `activeDirectoryId` *necesario para una restauración correcta si no `selfManagedActiveDirectoryConfiguration` está incluido*
		• `selfManagedActiveDirectoryConfiguration` *necesario para una restauración correcta si no `activeDirectoryId` está incluido*
		• `preferredSubnetId`

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

Clústeres de Amazon RDS, Aurora, Amazon DocumentDB y Amazon Neptune	`availabilityZones` con un valor establecido en una lista de hasta tres zonas de disponibilidad aleatorias
	
	`dbClusterIdentifier` con un valor aleatorio que empieza por `awsbackup-restore-test`
	
	`engine` con un valor establecido en el motor del punto de recuperación que se está restaurando
		`availabilityZones`
		
		`databaseName`
		
		`dbClusterParameterGroupName`
		
		`dbSubnetGroupName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`engine`
		
		`engineMode`
		
		`engineVersion`
		
		`kmskeyId`
		
		`port`
		
		`optionGroupName`
		
		`scalingConfiguration`
		
		`vpcSecurityGroupIds`

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

Instancias de Amazon RDS	`dbInstanceIdentifier` con un valor aleatorio que empieza por `awsbackup-restore-test-`
	
	`deletionProtection` con valor establecido en `false`
	
	`multiAz` con valor establecido en `false`
	
	`publiclyAccessible` con un valor establecido en false
		`allocatedStorage`
		
		`availabilityZones`
		
		`dbInstanceClass`
		
		`dbName`
		
		`dbParameterGroupName`
		
		`dbSubnetGroupName`
		
		`domain`
		
		`domainIamRoleName`
		
		`enableCloudwatchLogsExports`
		
		`enableIamDatabaseAuthentication`
		
		`iops`
		
		`licensemodel`
		
		`multiAz`
		
		`optionGroupName`
		
		`port`
		
		`processorFeatures`
		
		`publiclyAccessible`
		
		`storageType`
		
		`vpcSecurityGroupIds`

Tipo de recurso	Claves y valores de metadatos de restauración inferidos	Metadatos anulables

Amazon Simple Storage Service (Amazon S3)	`destinationBucketName` con un valor aleatorio que empieza por `awsbackup-restore-test-`
	
	`encrypted` con valor establecido en `true`
	
	`encryptionType` con valor establecido en `SSE-S3`
	
	`newBucket` con valor establecido en `true`
		`encryptionType`
		
		`kmsKey`

Restablecer la validación de las pruebas

Tiene la opción de crear una validación basada en eventos que se ejecute cuando se complete un trabajo de prueba de restauración.

En primer lugar, crea un flujo de trabajo de validación con cualquier objetivo compatible con Amazon EventBridge, por ejemplo AWS Lambda. En segundo lugar, añade una EventBridge regla que se encargue de que el trabajo de restauración alcance el estado`COMPLETED`. En tercer lugar, cree un plan de pruebas de restauración (o deje que uno existente se ejecute según lo programado). Por último, una vez finalizada la prueba de restauración, supervise los registros del flujo de trabajo de validación para asegurarse de que se ha ejecutado según lo esperado (una vez ejecutada la validación, aparecerá el estado de la validación en la AWS Backup consola).

1. Configure el flujo de trabajo de validación

   Puede configurar un flujo de trabajo de validación mediante Lambda o cualquier otro objetivo compatible con. EventBridge Por ejemplo, si está validando una prueba de restauración que contiene una instancia de Amazon EC2, puede incluir un código que haga ping a un punto final de comprobación de estado.

   Puede usar los detalles del evento para determinar qué recursos validar.

Puede usar una capa Lambda personalizada para usar el SDK más reciente (ya que aún no `PutRestoreValidationResult` está disponible a través del SDK de Lambda).

He aquí un ejemplo:

```
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. Añadir una EventBridge regla

   Cree una EventBridge regla que escuche el `COMPLETED`evento de restauración del trabajo.

   Si lo desea, puede filtrar los eventos por tipo de recurso o restaurar el ARN del plan de pruebas. Establezca el objetivo de esta regla para invocar el flujo de trabajo de validación que definió en el paso 1. A continuación se muestra un ejemplo:

```
{
  "source":[
    "aws.backup"
  ],
  "detail-type":[
    "Restore Job State Change"
  ],
```

```
  "detail":{
    "resourceType":[
      "..."
    ],
    "restoreTestingPlanArn":[
      "..."
    ],
    "status":[
      "COMPLETED"
    ]
  }
}
```

3. Deje que el plan de pruebas de restauración se ejecute y complete

   El plan de pruebas de restauración se ejecutará de acuerdo con la programación que haya configurado.

   Consulte Crear un plan de pruebas de restauración si aún no tiene uno o Actualizar un plan de pruebas de restauración si desea cambiar la configuración.

4. Supervise los resultados

   Una vez que el plan de pruebas de restauración se haya ejecutado según lo programado, puede comprobar los registros del flujo de trabajo de validación para asegurarse de que se ha ejecutado correctamente.

   Puede llamar a la API `PutRestoreValidationResult` para publicar los resultados, que luego se podrán ver en la AWS Backup consola y mediante las llamadas a la AWS Backup API que describen y enumeran los trabajos de restauración, como `DescribeRestoreJob` o`ListRestoreJob`.

   Una vez establecido un estado de validación, no se puede cambiar.

Visualización de una lista de copias de seguridad

Puede ver una lista de sus copias de seguridad mediante la AWS Backup consola o mediante programación.

Temas

- Listado de copias de seguridad por recurso protegido en la consola

- Listado de copias de seguridad por almacén de copias de seguridad en la consola
- Listado de copias de seguridad mediante programación

Listado de copias de seguridad por recurso protegido en la consola

Siga estos pasos para ver una lista de las copias de seguridad de un recurso concreto en la consola de AWS Backup .

1. Inicie sesión en la AWS Backup consola AWS Management Console y ábrala en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Protected resources (Recursos protegidos).
3. Elija un recurso protegido en la lista para ver la lista de copias de seguridad. Solo los recursos de los que se ha hecho una copia de seguridad AWS Backup aparecen en la lista Recursos protegidos.

Puede ver las copias de seguridad para el recurso. Desde esta vista, también puede elegir una copia de seguridad y restaurarla.

Listado de copias de seguridad por almacén de copias de seguridad en la consola

Siga estos pasos para ver una lista de copias de seguridad organizadas en un almacén de copias de seguridad.

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación, elija Backup vaults (Almacenes de copia de seguridad).
3. En la sección Backups (Copias de seguridad), vea la lista de todas las copias de seguridad organizadas en este almacén de copias de seguridad. En esta vista, puede ordenar las copias de seguridad por cualquiera de los encabezados de las columnas (incluido el estado), así como seleccionar una copia de seguridad para restaurarla, editarla o eliminarla.

Listado de copias de seguridad mediante programación

Puede enumerar las copias de seguridad mediante programación mediante las operaciones de la API `ListRecoveryPoint`:

- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByResource

Por ejemplo, el siguiente comando AWS Command Line Interface (AWS CLI) muestra todas las copias de seguridad con el EXPIRED estado:

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

Puede usar AWS Backup Audit Manager para auditar el cumplimiento de sus AWS Backup políticas con respecto a los controles que defina. Un control es un procedimiento diseñado para auditar la conformidad de un requisito de copia de seguridad, como la frecuencia de la copia de seguridad o el periodo de retención de la copia de seguridad.

AWS Backup Audit Manager le ayuda a responder a preguntas como:

- “¿Estoy haciendo copias de seguridad de todos mis recursos?”
- “¿Están cifradas todas mis copias de seguridad?”
- “¿Mis copias de seguridad se realizan a diario?”

Puede utilizar AWS Backup Audit Manager para encontrar la actividad y los recursos de respaldo que aún no cumplen con los controles que ha definido. Tenga en cuenta que solo se incluirán los recursos activos cuando los controles evalúen la conformidad de los recursos. Por ejemplo, se evaluará una instancia de Amazon EC2 en estado de ejecución. Las instancias EC2 en estado detenido no se incluirán en la evaluación de conformidad.

También puede usarlo para generar automáticamente un seguimiento de auditoría de informes diarios y bajo demanda para fines de control de copia de seguridad.

Los siguientes pasos proporcionan una descripción general de cómo utilizar AWS Backup Audit Manager. Para ver tutoriales detallados, elija uno de los temas al final de esta página.

1. Cree marcos que contengan una o más plantillas de control de gobernanza. Las preguntas anteriores son ejemplos de tres plantillas de control de gobernanza. Puede personalizar los parámetros de algunas plantillas de control de gobernanza. Por ejemplo, puede personalizar el último control para que pregunte: “¿Mis copias de seguridad se realizan semanalmente?” en lugar de a diario.
2. Consulte su marco para ver cuántos de sus recursos cumplen (o no) con los controles que definió en ese marco.
3. Cree informes sobre su estado de copia de seguridad y conformidad. Guarde estos informes como evidencia fehaciente de sus prácticas de conformidad o para identificar las actividades y los recursos de copia de seguridad individuales que aún no cumplen con las normas.

AWS Backup Audit Manager genera automáticamente un nuevo informe cada 24 horas y lo publica en Amazon S3. También puede generar informes bajo demanda.

> **Note**
>
> Antes de crear su primer marco relacionado con la conformidad, debe activar el seguimiento de los recursos. De este modo, podrá AWS Config realizar un seguimiento de sus AWS Backup recursos. Para obtener documentación técnica sobre cómo gestionar el seguimiento de los recursos, consulte Configuración AWS Config con la consola en la Guía para AWS Config desarrolladores.
> Al activar el seguimiento de los recursos, se aplican cargos. Para obtener información sobre el seguimiento de los recursos, los precios y la facturación de AWS Backup Audit Manager, consulte Medición, costes y facturación.

Temas

Uso de marcos de auditoría

Un marco es un conjunto de controles que le ayuda a evaluar sus prácticas de copia de seguridad. Puede utilizar controles personalizables y prediseñados para definir sus políticas y evaluar si sus prácticas de copia de seguridad cumplen con sus políticas. También puede configurar informes diarios automáticos para obtener información sobre el estado de conformidad de sus marcos.

Cada marco se aplica a una sola cuenta y Región de AWS. Puede implementar un máximo de 15 marcos por cuenta y región. No puede implementar marcos duplicados (marcos que contengan los mismos controles y parámetros).

Hay dos tipos diferentes de marcos:

- El marco de AWS Backup (recomendado): utilice el marco de AWS Backup para implementar todos los controles disponibles a fin de monitorizar la actividad, la cobertura y los recursos de copia de seguridad según las prácticas recomendadas.
- Un marco personalizado que usted defina: utilice un marco personalizado para elegir uno o más controles específicos y personalizar los parámetros de control.

Temas

Elección de controles

La siguiente tabla muestra los controles de AWS Backup Audit Manager, sus parámetros personalizables y sus tipos de recursos de AWS Config registro. Cada control requiere el tipo de recurso de registro `AWS Config: resource compliance` porque este tipo registra su estado de conformidad.

Controles disponibles

Nombre del control	Descripción del control	Parámetros personalizables	AWS Config tipo de recurso de registro
Recursos de copias de seguridad protegidos por planes de copia de seguridad	Evalúa si los recursos están protegidos por un plan de copia de seguridad.	Ninguna	`AWS Backup: backup selection`
El plan de copia de seguridad tiene	Evalúa si la frecuencia de las copias de seguridad es de al	Frecuencia de copia de seguridad; periodo de retención	`AWS Backup: backup plans`

Nombre del control	Descripción del control	Parámetros personalizables	AWS Config tipo de recurso de registro
frecuencia mínima y retención	menos [1 día] y el periodo de retención es de al menos [35 días].		
Los almacenes impiden la eliminación manual de los puntos de recuperación	Evalúa si las bóvedas de respaldo no permiten la eliminación manual de los puntos de recuperación, excepto para determinadas funciones AWS Identity and Access Management (IAM). De forma predeterminada, no hay excepciones a los roles de IAM. Tampoco hay excepciones a las funciones de IAM cuando se implementa este control con el marco. AWS Backup	Hasta 5 roles de IAM que permiten la eliminación manual de los puntos de recuperación	`AWS Backup: backup vaults`
Los puntos de recuperación están cifrados	Evalúa si los puntos de recuperación están cifrados.	Ninguna	`AWS Backup: recovery points`
Se ha establecido una retención mínima para el punto de recuperación	Evalúa si el periodo de retención del punto de recuperación es de al menos [35 días].	Periodo de retención del punto de recuperación	`AWS Backup: recovery points`

Nombre del control	Descripción del control	Parámetros personalizables	AWS Config tipo de recurso de registro
Se ha programado una copia de la copia de seguridad entre regiones	Evalúa si un recurso está configurado para crear copias de sus copias de seguridad en otra Región de AWS.	Región de AWS	`AWS Backup: backup selection`
Se ha programado una copia de la copia de seguridad entre cuentas	Evalúa si un recurso tiene configurada una copia de la copia de la copia de seguridad entre cuentas.	AWS ID de cuenta	`AWS Backup: backup selection`
Las copias de seguridad están protegidas por AWS Backup Vault Lock	Evalúa si un recurso está configurado para que se hagan copias de seguridad en un almacén de copias de seguridad bloqueado.	Días de retención mínimos; días de retención máximos	`AWS Backup: backup selection`
Se creó el último punto de recuperación	Evalúa si se creó un punto de recuperación dentro del periodo de tiempo especificado.	Valor en horas [1 a `744`] o días [1 a `31`].	`AWS Backup recovery points`
El tiempo de restauración de los recursos cumple el objetivo	Evalúa si el trabajo de pruebas de restauración se completó dentro del tiempo de restauración objetivo	Valor en minutos	Ninguna

Para obtener información detallada sobre estos controles, consulte Controles y corrección.

Para obtener una lista AWS Backup de los recursos compatibles que no admiten todos los controles, consulte la sección AWS Backup Audit Manager de la Disponibilidad de características por recurso tabla.

> **Note**
>
> Si no desea utilizar ninguno de los controles anteriores, puede seguir utilizando AWS Backup Audit Manager para crear informes diarios de sus trabajos de copia de seguridad, copia y restauración. Consulte Uso de informes de auditoría.

Activación del seguimiento de recursos

Antes de crear su primer marco relacionado con la conformidad, debe activar el seguimiento de los recursos. De este modo, podrá AWS Config realizar un seguimiento de sus AWS Backup recursos. Para obtener documentación técnica sobre cómo gestionar el seguimiento de los recursos, consulte Configuración AWS Config con la consola en la Guía para AWS Config desarrolladores.

Al activar el seguimiento de los recursos, se aplican cargos. Para obtener información sobre el seguimiento de los recursos, los precios y la facturación de AWS Backup Audit Manager, consulte Medición, costes y facturación.

Temas

- Activación del seguimiento de recursos mediante la consola
- Activación del seguimiento de recursos mediante la AWS Command Line Interface (AWS CLI)
- Activación del seguimiento de recursos mediante una plantilla de AWS CloudFormation

Activación del seguimiento de recursos mediante la consola

Active el seguimiento de recursos mediante la consola:

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, en Audit Manager, elija Marcos.
3. Para activar el seguimiento de recursos, seleccione Administrar el seguimiento de recursos.
4. Selecciona Ir a la AWS Config configuración.
5. Elija Habilitar o deshabilitar el registro.

6. Elija Habilitar el registro para todos los tipos de recursos siguientes o elija habilitar el registro para algunos tipos de recursos. Consulte Controles y correcciones de AWS Backup Audit Manager para ver qué tipos de recursos se requieren para sus controles.

   - `AWS Backup: backup plans`
   - `AWS Backup: backup vaults`
   - `AWS Backup: recovery points`
   - `AWS Backup: backup selection`

   > **Note**
   >
   > AWS Backup Audit Manager requiere `AWS Config: resource compliance` para cada control.

7. Elija Close.
8. Espere a que el banner azul con el texto Activando el seguimiento de recursos pase al banner verde con el texto El seguimiento de recursos está activado.

Puede comprobar si ha activado el seguimiento de recursos y, de ser así, qué tipos de recursos está grabando en dos lugares de la AWS Backup consola. En el panel de navegación izquierdo:

- Elija Marcos y, a continuación, elija el texto en estado de registro de AWS Config .
- Elija Configuración y, a continuación, elija el texto en estado de registro de AWS Config .

Activación del seguimiento de recursos mediante la AWS Command Line Interface (AWS CLI)

Si aún no lo has incorporado AWS Config, puede que sea más rápido hacerlo con el. AWS CLI

Para activar el seguimiento de recursos mediante la AWS CLI:

1. Escriba el siguiente comando para determinar si ya ha habilitado el registro de AWS Config .

   ```
   $ aws configservice describe-configuration-recorders
   ```

   a. Si la lista `ConfigurationRecorders` está vacía de esta manera:

```
{
  "ConfigurationRecorders": []
}
```

El registro no está habilitado. Continúe con el paso 2 para crear el registro.

b. Si ya ha habilitado el registro para todos los recursos, el resultado `ConfigurationRecorders` tendrá el siguiente aspecto:

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
      "name":"default"
    }
  ]
}
```

Como ha habilitado todos los recursos, ya ha activado el seguimiento de recursos. No necesita completar el resto de este procedimiento para utilizar AWS Backup Audit Manager.

c. Si su `ConfigurationRecorders` no está vacío, pero no ha habilitado el registro para todos los recursos, agregue recursos de copia de seguridad al registro existente mediante el siguiente comando. Después, vaya al paso 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. Cree una AWS Config grabadora con los tipos de recursos de 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. Describa su AWS Config grabadora.

```
$ aws configservice describe-configuration-recorders
```

Compruebe que tiene los tipos de recursos de AWS Backup Audit Manager comparando el resultado con el siguiente resultado esperado.

```
{
  "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. Cree un bucket de Amazon S3 como destino para almacenar los archivos AWS Config de configuración.

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. Utilice *policy.json* para conceder AWS Config permiso de acceso a su bucket. Consulte el siguiente ejemplo de *policy.json.*

```
$ 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. Configura tu depósito como canal de entrega AWS Config

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. Habilita la AWS Config grabación

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name default
```

8. Verifique que `"FrameworkStatus":"ACTIVE"` en la última línea de su resultado de `DescribeFramework` es como sigue.

```
$ 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"
}
```

Activación del seguimiento de recursos mediante una plantilla de AWS CloudFormation

Para ver una AWS CloudFormation plantilla que active el seguimiento de recursos, consulte Uso de AWS Backup Audit Manager con AWS CloudFormation.

Creación de marcos mediante la consola de AWS Backup

Tras activar el seguimiento de recursos, cree un marco mediante los siguientes pasos.

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Marcos.
3. Elija Crear marco.
4. En Nombre del marco, introduzca un nombre exclusivo. El nombre del marco debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).
5. De forma opcional, puede introducir una Descripción del marco.
6. En Controles, se mostrarán los controles activos. De forma predeterminada, se muestran todos los controles aptos para un recurso.

   Para cambiar los controles que están activos, haga clic en Editar controles.

   a. La primera casilla de verificación indica si el control está activado. Para desactivar un control, quite la marca de la casilla.

   b. En Elegir recursos para evaluar, puede seleccionar cómo elegir los recursos, ya sea por tipo, por etiquetas o por un único recurso.

La lista de controles de AWS Backup Audit Manager describe las opciones de personalización de cada control.

7. De forma opcional, puede agregar el marco seleccionando Añadir nueva etiqueta. Puede utilizar etiquetas para buscar y filtrar los marcos o hacer un seguimiento de los costos.
8. Elija Crear marco.

AWS Backup Audit Manager puede tardar varios minutos en crear el marco.

Si se produce el error `AlreadyExists`, ya existe un marco con los mismos controles y parámetros. Para crear correctamente un nuevo marco, al menos un control o parámetro debe ser diferente de los marcos existentes.

Crear marcos mediante la AWS Backup API

La siguiente tabla contiene ejemplos de solicitudes de API CreateFramework para cada control, junto con ejemplos de respuestas de API a las solicitudes DescribeFramework correspondientes. Para trabajar con AWS Backup Audit Manager mediante programación, puede consultar estos fragmentos de código.

Controlar	Solicitud de **CreateFramework**	Respuesta 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":`	`{"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_`

Controlar	Solicitud de **CreateFramework**	Respuesta de **DescribeFramework**

	<pre>["RDS"] // Evaluate only RDS instances
	}
	}
	],
	"IdempotencyToken": "Control1",
	"FrameworkTags": {"key1": "foo"}
	}</pre>
		<pre>PROTECTED_BY_BACKUP_PLAN",
		"ControlInputParameters":[],
		"ControlScope": {"ComplianceResourceTypes": ["RDS"]
		}
		}
		],
		"CreationTime": 1516925490,
		"DeploymentStatus": "Active",
		"FrameworkStatus": "Completed",
		"IdempotencyToken": "Control1",
		"FrameworkTags": {"key1": "foo"}
		}</pre>

Controlar	Solicitud de **CreateFramework**	Respuesta 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": {

Controlar	Solicitud de **CreateFramework**	Respuesta de **DescribeFramework**
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	"Tags": {"key1": "prod"} } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

Controlar	Solicitud de **CreateFramework**	Respuesta 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

Controlar	Solicitud de **CreateFramework**	Respuesta 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>

Controlar	Solicitud de **CreateFramework**	Respuesta 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":

Controlar	Solicitud de **CreateFramework**	Respuesta 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>

Controlar	Solicitud de **CreateFramework**	Respuesta 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"} }

Controlar	Solicitud de **CreateFramework**	Respuesta 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"} }

Controlar	Solicitud de **CreateFramework**	Respuesta 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"} }

Controlar	Solicitud de **CreateFramework**	Respuesta 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"} }

Controlar	Solicitud de **CreateFramework**	Respuesta 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"} }

Controlar	Solicitud de **CreateFramework**	Respuesta de **DescribeFramework**
	}	

Visualización del estado de conformidad del marco

Una vez que haya creado un marco de auditoría, aparecerá en la tabla Marcos. Para ver esta tabla, seleccione Frameworks en el panel de navegación izquierdo de la AWS Backup consola. Para ver los resultados de la auditoría de su marco, elija el Nombre del marco. Al hacerlo, accederá a la página de Detalles del marco, que tiene dos secciones: Resumen y Controles.

La sección Resumen muestra los siguientes estados de izquierda a derecha:

- El estado de conformidad es el estado de conformidad general de su marco de auditoría, determinado por el estado de conformidad de cada uno de sus controles. El estado de conformidad de cada control viene determinado por el estado de conformidad de cada recurso que evalúa.

  El estado de conformidad del marco es `Compliant` únicamente si todos los recursos incluidos en el ámbito de sus evaluaciones de control han superado dichas evaluaciones. Si uno o más recursos no superaron una evaluación de control, el estado de conformidad será `Non-Compliant`. Para obtener información sobre cómo encontrar los recursos no conformes, consulte Búsqueda de recursos no conformes. Para obtener información sobre cómo conseguir la conformidad de sus recursos, consulte la sección de corrección de Controles y correcciones de AWS Backup Audit Manager.
- El estado del marco se refiere a si ha activado el seguimiento de recursos para todos sus recursos. Los posibles estados son:
  - `Active` cuando el registro está activado para todos los recursos que el marco evalúa.
  - `Partially active` cuando el registro está desactivado para al menos un recurso que el marco evalúa.
  - `Inactive` cuando el registro está desactivado para todos los recursos que el marco evalúa.
  - `Unavailable`cuando AWS Backup Audit Manager no puede validar el estado de la grabación en este momento.

  Para corregir un estado **`Inactive`** o **`Partially active`**

  1. En el panel de navegación izquierdo, elija Marcos.

2. Elija Administrar el seguimiento de recursos.
3. Siga las instrucciones de la ventana emergente para habilitar el registro que antes no estaba habilitado para sus tipos de recursos.

Para obtener más información sobre los tipos de recursos que requieren un seguimiento de los recursos en función de los controles que haya incluido en sus marcos, consulte el componente de recursos de Controles y correcciones de AWS Backup Audit Manager.

- El estado de implementación hace referencia al estado de implementación de su marco. Este estado suele ser `Completed`, pero también puede ser `Create in progress` `Update in progress`, `Delete in progress` y `Failed`.
  - Un estado `Failed` significa que el marco no se implementó correctamente. Elimine el marco y, a continuación, vuelva a crearlo mediante la consola de AWS Backup o la API de AWS Backup.
- Los controles conformes muestran un recuento de los controles del marco con todas las evaluaciones aprobadas.
- Los controles no conformes muestran un recuento de los controles del marco con al menos una evaluación no aprobada.

La sección Controles muestra la siguiente información:

- El estado de control se refiere al estado de conformidad de cada control. Un control puede ser `Compliant`, lo que significa que todos los recursos superan esa evaluación; `Non-compliant`, lo que significa que al menos un recurso no supera esa evaluación, o `Insufficient data`, lo que significa que el control no ha encontrado ningún recurso que evaluar dentro del ámbito de la evaluación.
- El ámbito de la evaluación puede limitar cada control a uno o más Tipos de recursos, un ID de recurso o una Clave de etiqueta y un Valor de etiqueta, en función de la forma en que haya personalizado el control al crear el marco de auditoría. Si todos los campos están vacíos (lo que se muestra mediante un guión, “-”), el control evalúa todos los recursos aplicables.

Búsqueda de recursos no conformes

AWS Backup Audit Manager le ayuda a encontrar los recursos que no cumplen con las normas de dos maneras.

- En Visualización del estado de conformidad del marco, elija el nombre del control en la Sección de detalles. Al hacerlo, accederá a la AWS Config consola, donde podrá ver una lista de sus `Non-Compliant` recursos.
- Después de Crear un plan de informes con la plantilla de conformidad del recurso que incluye el marco, puede Ver el informe para identificar todos los recursos `Non-Compliant` en todos los controles.

  Además, `Resource compliance report` muestra la última vez que AWS Backup Audit Manager evaluó cada uno de sus controles por última vez.

Actualización de los marcos de auditoría

Puede actualizar la descripción, los controles y los parámetros de un marco de auditoría existente.

Para actualizar un marco existente

1. En el panel de navegación izquierdo de la AWS Backup consola, elija Frameworks.
2. Elija el marco que desee editar por el Nombre del marco.
3. Elija Editar.

Eliminación de los marcos de auditoría

Para eliminar un marco existente

1. En el panel de navegación izquierdo de la AWS Backup consola, elija Frameworks.
2. Elija el marco que desee eliminar por el Nombre del marco.
3. Elija Eliminar.
4. Escriba el nombre del marco y elija Eliminar el marco.

Uso de informes de auditoría

AWS Backup Los informes de Audit Manager se generan automáticamente como evidencia de su AWS Backup actividad, como:

- Qué trabajos de copia de seguridad finalizaron y cuándo
- De qué recursos hizo una copia de seguridad

Existen dos tipos de informes. Al crear un informe, usted elige el tipo de informe que desea crear.

Uno de ellos es el informe de trabajos, que muestra los trabajos finalizados en las últimas 24 horas y todos los trabajos activos. Los informes de trabajos no muestran un estado de `completed with issues`. Para encontrar este estado, puede filtrar los `Completed` trabajos con uno o más mensajes de estado. AWS Backup solo incluirá un mensaje de estado como parte del estado de un `Completed` trabajo si el mensaje requiere atención o acción.

El segundo tipo de informe es un informe de conformidad. Los informes de conformidad pueden monitorizar los niveles de recursos o los diferentes controles vigentes.

AWS Backup Audit Manager envía un informe diario a su bucket de Amazon S3. Si el informe es para la región actual y la cuenta actual, puede elegir recibirlo en formato CSV o JSON. De lo contrario, el informe está disponible en formato CSV. La duración del informe diario puede fluctuar durante varias horas porque AWS Backup Audit Manager realiza una aleatorización para mantener su rendimiento. También puede ejecutar un informe bajo demanda en cualquier momento.

Todos los titulares de cuentas pueden crear informes entre regiones; los titulares de cuentas de administración y de administrador delegado también pueden crear informes entre cuentas.

Puede tener un máximo de 20 planes de informes por cada uno. Cuenta de AWS

> **Note**
>
> Los recursos como RDS que no tienen la capacidad de mostrar los bytes incrementales de datos de una copia de seguridad específica mostrarán el valor `backupSizeInBytes` como 0.

Para permitir que AWS Backup Audit Manager cree informes diarios o bajo demanda, primero debe crear un plan de informes a partir de una plantilla de informe.

Temas

- Elección de la plantilla de informe
- Creación de planes de informes mediante la consola de AWS Backup
- Crear planes de informes mediante la API AWS Backup
- Creación de informes bajo demanda
- Visualización de los informes de auditoría
- Actualización de los planes de informes

- Eliminación de los planes de informes

Elección de la plantilla de informe

Una plantilla de informe define la información que su plan de informes incluye en el informe. Cuando automatiza sus informes mediante un plan de informes, AWS Backup Audit Manager le proporciona los informes de las 24 horas anteriores. AWS Backup Audit Manager crea estos informes entre la 1 y las 5 a.m. UTC. Ofrece las siguientes plantillas de informes.

Plantillas de informes de copia de seguridad

Plantillas de informes de copia de seguridad. Estas plantillas le proporcionan actualizaciones diarias sobre sus trabajos de copia de seguridad, restauración o copia. Puede utilizar estos informes para monitorizar su estado operativo e identificar cualquier error que pueda requerir la adopción de medidas adicionales. La tabla siguiente enumera el nombre de cada plantilla de informe de copia de seguridad y su resultado de muestra.

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
BACKUP_JOB_REPORT	{ "reportItems": [{ "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2", "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-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a", "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON


```
      "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"
    }
  ]
}
```

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON

COPY_JOB_REPORT	{
	"reportItems": [
	{
	"reportTimePeriod": "2021-07-14T15:48:31Z - 2021-07-15T15:48:31Z",
	"accountId": "112233445566",
	"region": "us-west-2",
	"copyJobId": "E0AD48A9-0560-B668-3EF0-941FDC0AD6B1",
	"jobStatus": "RUNNING",
	"resourceType": "EC2",
	"resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
	"backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a",
	"backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",
	"creationDate": "2021-07-15T15:42:04.771Z",
	"backupSizeInBytes": 8589934592,
	"sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-007b3819f25697299",
	"sourceBackupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
	"destinationRecoveryPointArn": "arn:aws:ec2:us-east-2::image/ami-0eba2199a0bcece3c",
	"destinationBackupVaultArn": "arn:aws:backup:us-east-2:112233445566:backup-vault:Default",
	"iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	}

Plantilla de informe de copia de seguridad	Informe de muestra en formato JSON
	] }

RESTORE_JOB_REPORT	{
	"reportItems": [
	{
	"reportTimePeriod": "2021-07-14T15:53:30Z - 2021-07-15T15:53:30Z",
	"accountId": "112233445566",
	"region": "us-west-2",
	"restoreJobId": "4CACA67D-4E12-DC05-6C2B-0E97D01FA41E",
	"jobStatus": "RUNNING",
	"recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-00201ecb57a5271ae",
	"creationDate": "2021-07-15T15:52:49.797Z",
	"backupSizeInBytes": 8589934592,
	"percentDone": "0.00%",
	"iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	}
	]
	}

Plantillas de informes de conformidad

Las plantillas de informes de conformidad le proporcionan informes diarios sobre la conformidad de su actividad y sus recursos de copia de seguridad con respecto a los controles que haya definido en uno o más marcos. Si el estado de conformidad de uno de sus marcos es `Non-compliant`, revise un informe de conformidad para identificar los recursos no conformes.

Tipos de Plantillas de informes de conformidad

- `Control compliance report` le ayuda a realizar un seguimiento del estado de conformidad de los controles que ha definido en sus marcos.
- `Resource compliance report` le ayuda a realizar un seguimiento del estado de conformidad de sus recursos con respecto a los controles que ha definido en sus marcos. Estos informes incluyen resultados de evaluación detallados, incluida información de identificación sobre los recursos no conformes que puede utilizar para identificar y corregir esos recursos.

La siguiente tabla muestra resultados de ejemplo de un informe de conformidad.

Plantilla de informe de conformidad	Informe de muestra en formato JSON
CONTROL_COMPLIANCE_REPORT	{ "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_R ESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08- 17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_H ours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7",

Plantilla de informe de conformidad	Informe de muestra en formato 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
\"}"
    }
  ]
}
```

Plantilla de informe de conformidad	Informe de muestra en formato 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"
	    }
	  ]
	}

Creación de planes de informes mediante la consola de AWS Backup

Existen dos tipos de informes. Uno de ellos es el informe de trabajos, que muestra los trabajos finalizados en las últimas 24 horas y todos los trabajos activos. El segundo tipo de informe es un informe de conformidad. Los informes de conformidad pueden monitorizar los niveles de recursos o los diferentes controles vigentes. Al crear un informe, elige el tipo de informe que se va a crear.

NOTA: Según el tipo de cuenta, la pantalla de la consola puede variar. Solo las cuentas de administración tendrán la funcionalidad de varias cuentas.

Al igual que en un plan de copia de seguridad, usted crea un plan de informes para automatizar la creación de sus informes y definir su bucket de Amazon S3 de destino. Un plan de informes requiere tener un bucket de S3 que reciba los informes. Para obtener instrucciones sobre cómo configurar un nuevo bucket de S3, consulte el Paso 1: Crear su primer bucket de S3 en la Guía del usuario de Amazon Simple Storage Service.

Para crear su plan de informes en la AWS Backup consola

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Informes.
3. Elija Crear plan de informe.
4. Elija una de las plantillas de informes de la lista desplegable.
5. Introduzca un Nombre del plan de informe único. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).
6. De forma opcional, puede introducir una Descripción del plan de informe.
7. Plantillas de informes de conformidad para una sola cuenta. Elija uno o más marcos sobre los que informar. Puede agregar un máximo de 1000 marcos a un plan de informes.
    1. Elija su AWS región mediante el menú desplegable.
    2. Elija un marco de esa región mediante el menú desplegable.
    3. Elija Agregar marco.
8. De forma opcional, para agregar etiquetas a su plan de informes, elija Agregar etiquetas al plan de informe.
9. Si utiliza una cuenta de administración, puede especificar qué cuentas desea incluir en este plan de informes. Puede seleccionar Solo mi cuenta, que generará informes solo sobre la cuenta

en la que ha iniciado sesión actualmente. O bien, puede seleccionar una o más cuentas de mi organización (disponibles para las cuentas de administración y de administrador delegado).

10. (Si va a crear un informe de conformidad para una sola región, omita este paso). Puede elegir las regiones que desea incluir en el informe. Haga clic en el menú desplegable para ver las regiones a su disposición. Seleccione Todas las regiones disponibles o las regiones que prefiera.

    - La casilla Incluir regiones nuevas cuando se incorporen a Backup Audit Manager activará la inclusión de nuevas regiones en sus informes cuando estén disponibles.

11. Elija el Formato del archivo de su informe. Todos los informes se pueden exportar en formato CSV. Además, los informes para una sola región y una sola región se pueden exportar en formato JSON.
12. Elija el Nombre del bucket de S3 mediante la lista desplegable.
13. De forma opcional, puede introducir un prefijo del bucket.

    AWS Backup entrega tu cuenta corriente, a la que reporta la región actual. `s3://your-bucket-name/prefix/Backup/accountID/Region/year/month/day/report-name`

    AWS Backup entrega sus informes multicuentas a `s3://your-bucket-name/prefix/Backup/crossaccount/Region/year/month/day/report-name`

    AWS Backup entrega sus informes interregionales a `s3://your-bucket-name/prefix/Backup/accountID/crossregion/year/month/day/report-name`

14. Elija Crear plan de informe.

A continuación, debe permitir que su bucket de S3 reciba informes desde AWS Backup. Tras crear un plan de informes, AWS Backup Audit Manager genera automáticamente una política de acceso al bucket de S3 para que la aplique.

Si cifra el bucket con una clave de KMS personalizada, la política de claves de KMS debe cumplir los siguientes requisitos:

- El `Principal` atributo debe incluir el ARN del rol vinculado al servicio Backup Audit Manager. `AWSServiceRolePolicyForBackupReports`

- El `Action` atributo debe incluir `kms:GenerateDataKey` y como mínimo. `kms:Decrypt`

La política AWSServiceRolePolicyForBackupReportstiene estos permisos.

Para ver y aplicar esta política de acceso a su bucket de S3

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Elija Editar.
5. Elija Ver política de acceso para el bucket de S3. Puede usar también la política al final de este procedimiento.
6. Elija Copiar permisos.
7. Elija Editar política del bucket. Tenga en cuenta que, hasta que no se cree el informe de respaldo por primera vez, la función vinculada al servicio a la que se hace referencia en la política de bucket de S3 no existirá todavía, lo que generará el error «Principal no válido».
8. Copie los permisos a la Política.

Ejemplo de política de bucket

```
{
  "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 utilizas una configuración personalizada AWS Key Management Service para cifrar el bucket de S3 de destino que almacena los informes, incluye las siguientes acciones en tu política:

```
"Action":[
  "kms:GenerateDataKey",
  "kms:Encrypt"
],
"Resource":[
  "*"
],
```

Crear planes de informes mediante la API AWS Backup

También puede trabajar con los planes de informes mediante programación.

Existen dos tipos de informes. Uno de ellos es el informe de trabajos, que muestra los trabajos finalizados en las últimas 24 horas y todos los trabajos activos. El segundo tipo de informe es un informe de conformidad. Los informes de conformidad pueden monitorizar los niveles de recursos o los diferentes controles vigentes. Al crear un informe, elige el tipo de informe que se va a crear.

Al igual que en un plan de copia de seguridad, usted crea un plan de informes para automatizar la creación de sus informes y definir su bucket de Amazon S3 de destino. Un plan de informes requiere tener un bucket de S3 que reciba los informes. Para obtener instrucciones sobre cómo configurar un nuevo bucket de S3, consulte el Paso 1: Crear su primer bucket de S3 en la Guía del usuario de Amazon Simple Storage Service.

Si cifra el bucket con una clave de KMS personalizada, la política de claves de KMS debe cumplir los siguientes requisitos:

- El `Principal` atributo debe incluir el ARN del rol vinculado al servicio Backup Audit Manager. `AWSServiceRolePolicyForBackupReports`

- El `Action` atributo debe incluir `kms:GenerateDataKey` y como mínimo. `kms:Decrypt`

La política AWSServiceRolePolicyForBackupReportstiene estos permisos.

Para los informes de una sola cuenta y una sola región, utilice la siguiente sintaxis para llamar a 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"
}
```

Cuando llame a DescribeReportPlan con el nombre exclusivo de un plan de informes, la API de AWS Backup responde con la siguiente información.

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

Para los informes de varias cuentas y varias regiones, utilice la siguiente sintaxis para llamar a 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"
   }
}
```

Cuando llame a DescribeReportPlan con el nombre exclusivo de un plan de informes, la API de AWS Backup responde con la siguiente información para varias cuentas y varias regiones:

```
{
   "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"
         }
      }
}
```

Creación de informes bajo demanda

Puede generar nuevos informes cuando lo desee creando un informe bajo demanda siguiendo los siguientes pasos. AWS Backup Audit Manager envía su informe bajo demanda al bucket de Amazon S3 que especificó en su plan de informes.

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Elija Crear informe en diferido.

Puede generar un informe bajo demanda para un plan de informes existente.

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Informes.
3. En Planes de informes, haga clic en el botón de opción situado junto al nombre del plan para seleccionarlo.
4. Haga clic en Acciones y, a continuación, en Crear informe en diferido.

Puede hacer esto para varios informes, incluso mientras se generan los informes.

Visualización de los informes de auditoría

Puede abrir, ver y analizar los informes de AWS Backup Audit Manager mediante los programas que suele utilizar para trabajar con archivos CSV o JSON. Tenga en cuenta que los informes de varias regiones o cuentas solo están disponibles en formato CSV.

Los archivos grandes se dividen en varios informes si el tamaño total del archivo supera los 50 MB. Si los archivos resultantes pesan más de 50 MB, AWS Backup Audit Manager creará archivos CSV adicionales con el resto del informe.

Para ver un informe

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. En Trabajos de informe, haga clic en el enlace del informe para verlo.
5. Si el Estado del informe tiene un subrayado punteado, selecciónelo para obtener información sobre el informe.
6. Elija qué informe desea ver según su Hora de finalización.
7. Elija el enlace de S3. Esto abre el bucket de S3 de destino.
8. En Nombre, elija el nombre del informe que desea ver.
9. Puede guardar el informe en su equipo, elija Descargar.

Actualización de los planes de informes

Puede actualizar la descripción, el destino de entrega y el formato de un plan de informes existente. Si procede, también puede agregar o eliminar marcos del plan de informes.

Para actualizar un plan de informes existente

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Elija Editar.
5. Puede editar los detalles del plan del informe, incluidos el nombre y la descripción del informe, así como las cuentas y regiones que se incluyen en el informe.

Eliminación de los planes de informes

Puede eliminar un plan de informes existente. Cuando elimine un plan de informes, todos los informes que ya haya creado dicho plan permanecerán en su bucket de Amazon S3 de destino.

Para eliminar un plan de informes existente

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.

2. En el panel de navegación izquierdo, elija Informes.
3. En Nombre del plan de informe, elija el nombre de un plan para seleccionarlo.
4. Elija Eliminar.
5. Introduzca el nombre del plan de informes y, a continuación, elija Eliminar el plan de informe.

Uso de AWS Backup Audit Manager con AWS CloudFormation

Proporcionamos las siguientes AWS CloudFormation plantillas de muestra para su consulta:

Temas

- Activación del seguimiento de recursos
- Implementación de controles predeterminados
- Exención de roles de IAM de la evaluación de control
- Creación de un plan de informes

Activación del seguimiento de recursos

La siguiente plantilla activa el seguimiento de recursos, tal y como se describe en Activación del seguimiento de recursos.

```
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
```

Implementación de controles predeterminados

La siguiente plantilla crea un marco con los controles predeterminados descritos en Controles y correcciones de AWS Backup.

```
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
```

Exención de roles de IAM de la evaluación de control

El control BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED permite eximir hasta cinco roles de IAM que aún pueden eliminar manualmente puntos de recuperación. La siguiente plantilla implementa este control y también exime dos roles de 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
```

Creación de un plan de informes

La siguiente plantilla crea un plan de informes.

```
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
```

Uso de AWS Backup Audit Manager con AWS Audit Manager

AWS Backup Los controles de Audit Manager se corresponden con controles estándar prediseñados AWS Audit Manager, lo que le permite importar las conclusiones de conformidad de AWS Backup Audit Manager a sus AWS Audit Manager informes. Puede que desee hacerlo para ayudar a un responsable de conformidad, director de auditoría u otro compañero que informe sobre las actividades de copia de seguridad como parte de la postura de conformidad general de su organización.

Puede importar los resultados de conformidad de sus controles de AWS Backup Audit Manager a sus AWS Audit Manager marcos. AWS Audit Manager Para permitir la recopilación automática de datos de los controles de AWS Backup Audit Manager, cree un control personalizado AWS Audit Manager siguiendo las instrucciones para personalizar un control existente de la Guía del AWS Audit Manager usuario. Al seguir estas instrucciones, tenga en cuenta que la fuente de datos de los AWS Backup controles es AWS Config.

Para obtener una lista de AWS Backup los controles, consulte Elegir los controles.

Controles y corrección

En esta página se enumeran los controles disponibles para AWS Backup Audit Manager. Puede elegir el panel de información derecho para ver una lista de controles y pasar a un control específico. Para comparar rápidamente los controles, consulta la tabla en Elección de controles. Para definir los controles mediante programación, consulte los fragmentos de código en Creación de marcos mediante la API de AWS Backup.

Puede usar hasta 50 controles por cuenta y región. Usar el mismo control en dos marcos diferentes cuenta como usar dos controles del límite de 50 controles.

En esta página se muestra cada control con la siguiente información:

- Descripción. Los valores entre corchetes (“[]”) son los valores de los parámetros predeterminados.
- Los recursos que evalúa el control.
- Los parámetros del control.
- Ocasión en la que se produce la ejecución del control.
- El alcance del control, de la siguiente manera:
  - Puede especificar Recursos por tipo. Para ello, elija uno o más servicios compatibles con AWS Backup.
  - Puede especificar un ámbito de Recursos etiquetados con una única clave de etiqueta y un valor opcional.
  - Puede especificar un único recurso mediante la lista desplegable Recurso único.
- Medidas correctivas para que los recursos aplicables logren la conformidad.

Tenga en cuenta que solo se incluirán los recursos activos cuando los controles evalúen la conformidad de los recursos. Por ejemplo, el control Último punto de recuperación creado evaluará

una instancia de Amazon EC2 en estado en ejecución. Las instancias EC2 en estado detenido no se incluirán en la evaluación de conformidad.

Recursos de copias de seguridad protegidos por planes de copia de seguridad

Descripción: evalúa si los recursos están protegidos por un plan de copia de seguridad.

Recurso: `AWS Backup: backup selection`

Parámetros: ninguno

Ocurre: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo (predeterminado)
- Recurso único

Corrección: asigne los recursos a un plan de copia de seguridad. AWS Backup protege automáticamente sus recursos después de que los asigne a un plan de copia de seguridad. Para obtener más información, consulte Asignación de recursos a un plan de copia de seguridad.

Frecuencia mínima y retención mínima del plan de copia de seguridad

Descripción: evalúa si los planes de copia de seguridad contienen al menos una regla de copia de seguridad según la cual la frecuencia de copia de seguridad sea de al menos [1 día] y el periodo de retención sea de al menos [35 días].

Recurso: `AWS Backup: backup plans`

Parámetros:

- Frecuencia de copia de seguridad requerida en número de horas o días.
- Periodo de retención obligatorio en días, semanas, meses o años. Recomendamos conservar el almacenamiento en caliente durante un período de al menos una semana para poder AWS Backup realizar copias de seguridad incrementales siempre que sea posible y evitar cargos adicionales.

Ocurre: cambios en la configuración

Ámbito:

- Recursos etiquetados
- Recurso único

Corrección: actualice un plan de copia de seguridad para cambiar su frecuencia de copia de seguridad, su periodo de retención o ambos. La actualización del plan de copia de seguridad cambia el periodo de retención de los puntos de recuperación que el plan crea después de la actualización.

Los almacenes impiden la eliminación manual de los puntos de recuperación

Descripción: evalúa si los almacenes de copias de seguridad no permiten la eliminación manual de los puntos de recuperación, excepto mediante determinados roles de IAM.

Recurso: `AWS Backup: backup vaults`

Parámetros:: los nombres de recursos de Amazon (ARN) de hasta cinco roles de IAM que pueden eliminar manualmente puntos de recuperación.

Ocurre: cambios en la configuración

Ámbito:

- Recursos etiquetados
- Recurso único

Corrección: cree o modifique una política de acceso basada en recursos en un almacén de copias de seguridad. Para ver un ejemplo de la política e instrucciones sobre cómo establecer una política de acceso en un almacén de copias de seguridad, consulte Denegacion del acceso para eliminar puntos de recuperación en un almacén de copias de seguridad.

Los puntos de recuperación están cifrados

Descripción: evalúa si los puntos de recuperación están cifrados.

Recurso: `AWS Backup: recovery points`

Parámetros: ninguno

Ocurre: cambios en la configuración

Ámbito:

- Recursos etiquetados

Corrección: configure el cifrado de los puntos de recuperación. La forma de configurar el cifrado de los puntos de AWS Backup recuperación varía según el tipo de recurso.

Puede configurar el cifrado para los tipos de recursos que admitan una AWS Backup administración completa de su uso AWS Backup. Si el tipo de recurso no admite la AWS Backup administración completa, debe configurar su cifrado de respaldo siguiendo las instrucciones de ese servicio, como el cifrado de Amazon EBS en la Guía del usuario de Amazon Elastic Compute Cloud. Para ver la lista de tipos de recursos que admiten la AWS Backup administración completa, consulte la sección « AWS Backup Administración completa» de la Disponibilidad de características por recurso tabla.

Se ha establecido una retención mínima para el punto de recuperación

Descripción: evalúa si el periodo de retención del punto de recuperación es de al menos [35 días].

Recurso: `AWS Backup: recovery points`

Parámetros: periodo de retención obligatorio en días, semanas, meses o años. Recomendamos conservar el almacenamiento en caliente durante un período de al menos una semana para poder AWS Backup realizar copias de seguridad incrementales siempre que sea posible y evitar cargos adicionales.

Ocurre: cambios en la configuración

Ámbito:

- Recursos etiquetados

Corrección: cambie los periodos de retención de sus puntos de recuperación. Para obtener más información, consulte Edición de una copia de seguridad.

Se ha programado una copia de la copia de seguridad entre regiones

Descripción: Evalúa si un recurso está configurado para crear copias de sus copias de seguridad en otra AWS región.

Recurso: `AWS Backup: backup selection`

Parámetros:

- Seleccione los Región de AWS lugares donde debe estar la copia de seguridad (opcional)
- Región

Ocurre: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Solución: actualice un plan de respaldo para cambiar el Región de AWS lugar donde debe estar la copia de seguridad.

Se ha programado una copia de la copia de seguridad entre cuentas

Descripción: evalúa si un recurso está configurado para crear copias de sus copias de seguridad en otra cuenta. Puede agregar hasta 5 cuentas para que el control las evalúe. La cuenta de destino debe estar en la misma organización que la cuenta de origen en AWS Organizations.

Recurso: `AWS Backup: backup selection`

Parámetros:

- Seleccione los ID de AWS cuenta en los que debe estar la copia de seguridad (opcional)
- ID de cuenta

Ocurre: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Solución: actualice un plan de respaldo para cambiar o agregar los ID de AWS cuenta en los que debería estar la copia.

Las copias de seguridad están protegidas por AWS Backup Vault Lock

Descripción: evalúa si un recurso tiene copias de seguridad inmutables almacenadas en un almacén de copias de seguridad bloqueado.

Recurso: `AWS Backup: backup selection`

Parámetros:

- Introduzca los días de retención mínimos y máximos de AWS Backup Vault Lock (opcional)
- Días de retención mínimos
- Días de retención máximos

Ocurre: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Corrección: bloquee un almacén de copias de seguridad para establecer su nombre, cambiar sus días de retención mínimos o máximos, o ambos. También puede incluir `ChangeableForDays` para un bloqueo del almacén en modo de cumplimiento.

Se creó el último punto de recuperación

Descripción: este control evalúa si se ha creado un punto de recuperación dentro del periodo de tiempo especificado (en días u horas).

El control es conforme si se ha creado un punto de recuperación del recurso dentro del periodo de tiempo especificado. El control no es conforme si no se ha creado un punto de recuperación dentro del número de días u horas especificado.

Recurso: `AWS Backup: recovery points`

Parámetros:

- Introduzca el periodo de tiempo especificado en números enteros, ya sea en horas o en días.
- Los valores de `hours` pueden oscilar entre `1` y `744`.
- El valor de `days` puede oscilar entre `1` y `31`.

Ocurre: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados
- Recursos por tipo
- Recurso único

Corrección:

- Actualice un plan de copia de seguridad para cambiar el periodo de tiempo especificado para la creación del punto de recuperación.
- Además, puede crear una copia de seguridad bajo demanda.

El tiempo de restauración de los recursos cumple el objetivo

Descripción: evalúa si la restauración de los recursos protegidos se completó dentro del tiempo de restauración objetivo.

Este control comprueba si el tiempo de restauración de un recurso concreto cumple la duración objetivo. La regla es NON_COMPLIANT si `LatestRestoreExecutionTimeMinutes` de un tipo de recurso es mayor que `maxRestoreTime` en minutos.

Parámetros:

- `maxRestoreTime` (en minutos)

Ocurre: automáticamente cada 24 horas

Ámbito:

- Recursos etiquetados

- Recursos por tipo
- Recurso único

> **Note**
>
> AWS Backup no proporciona ningún acuerdo de nivel de servicio (SLA) durante el tiempo de restauración. Los tiempos de restauración pueden variar en función de la carga y la capacidad del sistema, incluso en el caso de restauraciones que contengan los mismos recursos.

Administrar AWS Backup recursos en múltiples Cuentas de AWS

> **Note**
>
> Antes de administrar los recursos Cuentas de AWS en varios AWS Backup ingresos, sus cuentas deben pertenecer a la misma organización del AWS Organizations servicio.

Puede utilizar la función de administración multicuenta AWS Backup para gestionar y supervisar los trabajos de copia de seguridad, restauración y copia con AWS Organizations los Cuentas de AWS que haya configurado. AWS Organizationses un servicio que ofrece una administración basada en políticas para múltiples cuentas de administración Cuentas de AWS desde una única cuenta de administración. Le permite estandarizar la forma en que implementa las políticas de copia de seguridad, minimizando los errores manuales y el esfuerzo simultáneamente. Desde una vista central, puede identificar fácilmente los recursos en todas las cuentas que cumplan los criterios que le interesan.

Si lo configuras AWS Organizations, puedes configurarlo AWS Backup para monitorear las actividades de todas tus cuentas en un solo lugar. También puede crear una política de copias de seguridad y aplicarla a determinadas cuentas que formen parte de su organización y ver las actividades agregadas de las tareas de copia de seguridad directamente desde la AWS Backup consola. Esta funcionalidad permite a los administradores de copias de seguridad monitorizar eficazmente el estado del trabajo de copia de seguridad en cientos de cuentas de toda la empresa desde una sola cuenta maestra. Se aplican las Cuotas para AWS Organizations.

Por ejemplo, se define una política de copia de seguridad A que toma copias de seguridad diarias de recursos específicos y las mantiene durante 7 días. Puede aplicar la política de copia de seguridad A a toda la organización. (Esto significa que cada cuenta de la organización obtiene esa política de copia de seguridad, lo que crea un plan de copia de seguridad correspondiente que está visible en esa cuenta). A continuación, crea una unidad organizativa denominada Finance y decide mantener sus copias de seguridad durante solo 30 días. En este caso, se define una política de copia de seguridad B, que anula el valor del ciclo de vida y se adjunta a esa unidad organizativa Finance. Esto significa que todas las cuentas bajo la unidad organizativa Finance obtienen un nuevo plan de copia de seguridad efectivo que toma copias de seguridad diarias de todos los recursos especificados y las mantiene durante 30 días.

En este ejemplo, la política de copia de seguridad A y la política de copia de seguridad B se fusionaron en una única política de copia de seguridad, que define la estrategia de protección para todas las cuentas de la unidad organizativa denominada Finance. Todas las demás cuentas de la organización permanecen protegidas por la política de copia de seguridad A. La combinación se realiza solo para las políticas de copia de seguridad que comparten el mismo nombre de plan de copia de seguridad. También puede hacer que la política A y la política B coexistan en esa cuenta sin ninguna combinación. Solo puede utilizar operadores avanzados de fusión en la vista JSON de la consola. Para obtener más información sobre la combinación de políticas, consulte Definición de políticas, sintaxis de políticas y herencia de políticas en la Guía del usuario de AWS Organizations . Para obtener referencias y casos de uso adicionales, consulte el blog Cómo administrar copias de seguridad a gran escala AWS Organizations con su uso AWS Backup y el tutorial en vídeo Cómo gestionar las copias de seguridad a escala AWS Organizations con su uso AWS Backup.

Consulte la disponibilidad de funciones por AWS región para ver dónde está disponible la función de administración multicuenta.

Para utilizar la administración entre cuentas, debe seguir estos pasos:

1. Cree una cuenta de administración AWS Organizations y añada cuentas a la cuenta de administración.
2. Habilite la función de administración multicuenta en AWS Backup.
3. Cree una política de respaldo para aplicarla a todos los usuarios Cuentas de AWS de su cuenta de administración.

> **Note**
>
> Para los planes de copia de seguridad administrados por Organizations, la configuración de suscripción del recurso en la cuenta de administración anula la configuración de la cuenta de un miembro, aunque estén configuradas una o varias cuentas de administrador delegado. Las cuentas de administrador delegado son cuentas de miembros con características mejoradas y no pueden anular la configuración como una cuenta de administración.

4. Gestione los trabajos de copia de seguridad, restauración y copia en todos sus archivos Cuentas de AWS.

Temas

Creación de una cuenta de administración en Organizations

En primer lugar, debe crear su organización y configurarla con las cuentas de AWS los miembros integradas AWS Organizations.

Para crear una cuenta de administración en AWS Organizations y añadir cuentas

- Para obtener instrucciones, consulte Tutorial: Creación y configuración de una organización en la Guía del usuario de AWS Organizations .

Habilitación de la administración entre cuentas

Antes de poder utilizar la gestión multicuenta AWS Backup, tienes que activar la función (es decir, activarla). Una vez habilitada la función, puede crear políticas de copia de seguridad que le permitan automatizar la administración simultánea de varias cuentas.

Para habilitar la administración entre cuentas

1. Ábrela Consola de AWS Backup en https://console.aws.amazon.com/backup/. Debe iniciar sesión con las credenciales de la cuenta de administración.
2. En el panel de navegación izquierdo, elija Settings (Configuración) para abrir la página de administración entre cuentas.
3. En la sección Backup policies (Políticas de copia de seguridad), elija Enable (Habilitar).

   Esto le da acceso a todas las cuentas y le permite crear políticas que automatizan la administración de varias cuentas en su organización simultáneamente.

4. En la sección Supervisión entre cuentas elija Enable (Habilitar).

   Esto le permite monitorizar las actividades de copia de seguridad, copia y restauración de todas las cuentas de su organización desde su cuenta de administración.

Administrador delegado

La administración delegada proporciona una forma cómoda para que los usuarios asignados a una cuenta de miembro registrado realicen la mayoría de las tareas AWS Backup administrativas. Puede optar por delegar la administración de AWS Backup una cuenta de miembro en AWS Organizations, lo que amplía la capacidad AWS Backup de administrar desde fuera de la cuenta de administración y en toda la organización.

Una cuenta de administración, de forma predeterminada, es la cuenta que se usa para editar y administrar las políticas. Con la característica de administrador delegado, puede delegar estas funciones de administración a las cuentas miembro que designe. A su vez, esas cuentas pueden administrar políticas, además de la cuenta de administración.

Una vez que la cuenta miembro se haya registrado correctamente para la administración delegada, se convierte en una cuenta de administrador delegado. Tenga en cuenta que las cuentas, no los usuarios, se designan como administradores delegados.

La habilitación de cuentas de administrador delegado permite administrar las políticas de copia de seguridad, minimiza la cantidad de usuarios con acceso a la cuenta de administración y facilita la monitorización de los trabajos entre cuentas.

A continuación, se muestra una tabla que muestra las funciones de la cuenta de administración, las cuentas delegadas como administradores de Backup y las cuentas que son miembros de la AWS organización.

> **Note**
>
> Las cuentas de administrador delegado son cuentas de miembros con características mejoradas, pero no pueden anular la configuración de suscripción al servicio de otras cuentas de miembros como una cuenta de administración.

PRIVILEGIOS	CUENTA DE ADMINISTRACIÓN	ADMINISTRADOR DELEGADO	CUENTA MIEMBRO
Registrar o anular el registro de cuentas de administrador delegado	Sí	No	No
Administre las políticas de respaldo en todas las cuentas en AWS Organizat ions	Sí	Sí	No
Monitorizar los trabajos entre cuentas	Sí	Sí	No

Requisitos previos

Para poder delegar la administración de las copias de seguridad, primero debe registrar al menos una cuenta de miembro en su AWS organización como administrador delegado. Antes de poder registrar una cuenta como administrador delegado, primero debe configurar lo siguiente:

- AWS Organizations debe estar habilitada y configurada con al menos una cuenta de miembro además de la cuenta de administración predeterminada.
- En la AWS Backup consola, asegúrate de que las políticas de respaldo, la supervisión multicuenta y las funciones de copia de seguridad multicuenta estén activadas. Se encuentran debajo del panel de administradores delegados de la consola. AWS Backup
  - La monitorización entre cuentas le permite monitorizar la actividad de copia de seguridad en todas las cuentas de su organización, tanto desde la cuenta de administración como desde las cuentas de administrador delegado.
  - Opcional: copia de seguridad multicuenta, que permite a las cuentas de su organización copiar copias de seguridad a otras cuentas (para los recursos multicuenta compatibles con Backup).
  - Habilite el acceso al servicio con. AWS Backup

La configuración de la administración delegada consta de dos pasos. El primer paso es delegar la monitorización de los trabajos entre cuentas. El segundo paso es delegar la administración de las políticas de copia de seguridad.

Registro de una cuenta miembro como cuenta del administrador delegado

Esta es la primera sección: Uso de la AWS Backup consola para registrar una cuenta de administrador delegado a fin de supervisar los trabajos entre cuentas. Para delegar AWS Backup políticas, utilizará la consola Organizations en la siguiente sección.

Para registrar una cuenta de miembro mediante la AWS Backup consola:

1. Ábrala Consola de AWS Backup en https://console.aws.amazon.com/backup/. Debe iniciar sesión con las credenciales de la cuenta de administración.
2. En Mi cuenta, en el panel de navegación izquierdo de la consola, elija Configuración.
3. En el panel Administradores delegados, haga clic en Registrar administrador delegado o Agregar administrador delegado.
4. En la página Registrar administrador delegado, seleccione la cuenta que desee registrar y, a continuación, elija Registrar cuenta.

Esta cuenta designada ahora se registrará como un administrador delegado, con privilegios administrativos para monitorizar los trabajos en todas las cuentas de la organización. Además, podrá ver y editar las políticas (delegación de políticas). Esta cuenta miembro no puede registrar ni anular el registro de otras cuentas de administrador delegado. Puede usar la consola para registrar un máximo de 5 cuentas como administradores delegados.

Para registrar una cuenta miembro mediante programación:

Utilice el comando CLI `register-delegated-administrator`. Puede especificar los siguientes parámetros en su solicitud de CLI:

- `service-principal`
- `account-id`

A continuación se muestra un ejemplo de una solicitud de CLI para registrar una cuenta miembro mediante programación:

```
aws organizations register-delegated-administrator \
```

```
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Anulación del registro de una cuenta miembro

Utilice el siguiente procedimiento para eliminar el acceso administrativo AWS Backup anulando el registro de una cuenta de miembro de su AWS organización que anteriormente había sido designada como administrador delegado.

Para anular el registro de una cuenta miembro con la consola

1. Ábrala en https://console.aws.amazon.com/backup/ Consola de AWS Backup . Debe iniciar sesión con las credenciales de la cuenta de administración.
2. En Mi cuenta, en el panel de navegación izquierdo de la consola, elija Configuración.
3. En la sección Administrador delegado, elija Anular el registro de cuenta.
4. Elige la cuenta o cuentas para las que desea anular el registro.
5. En el cuadro de diálogo Anular el registro de cuenta, revise las implicaciones de seguridad y, a continuación, escriba `confirm` para completar la anulación del registro.
6. Elija `Deregister account`.

Para anular el registro de una cuenta miembro mediante programación:

Utilice el comando de la CLI `deregister-delegated-administrator` para anular el registro de una cuenta de administrador delegado. Puede especificar los siguientes parámetros en su solicitud de API:

- `service-principal`
- `account-id`

A continuación se muestra un ejemplo de una solicitud de CLI para anular el registro de una cuenta miembro mediante programación:

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

Delegue AWS Backup las políticas a través de AWS Organizations

Dentro de la AWS Organizations consola, puede delegar la administración de varias políticas, incluidas las políticas de Backup.

Desde la cuenta de administración que ha iniciado sesión en la consola de AWS Organizations, puede crear, ver o eliminar una política de delegación basada en recursos para su organización. Para ver los pasos para delegar políticas, consulte Crear una política de delegación basada en recursos en la Guía del usuario de AWS Organizations .

Creación de un plan de copia de seguridad

Después de habilitar la administración entre cuentas, cree una política de copia de seguridad entre cuentas desde su cuenta de administración.

> **Warning**
>
> Al crear una política con JSON, se rechazarán los nombres de clave duplicados. El nombre de cada clave debe ser único si se incluyen varios planes, reglas o selecciones en una sola política.

Cree una política de respaldo a través de la AWS Backup consola

1. En el panel de navegación izquierdo, elija Backup policies (Políticas de copia de seguridad). En la página Backup policies (Políticas de copia de seguridad), elija Create backup policies (Crear políticas de copia de seguridad).
2. En la sección Details (Detalles), introduzca un nombre de política de copia de seguridad y proporcione una descripción.
3. En la sección Backup plans details (Detalles de planes de copia de seguridad), elija la pestaña de editor visual y haga lo siguiente:
   a. En Backup plan name (Nombre del plan de copia de seguridad), introduzca un nombre.
   b. En Regions (Regiones), elija una región de la lista.
4. En la sección Backup rule configuration (Configuración de reglas de copia de seguridad), elija Add backup rule (Agregar reglas de copia de seguridad).

El número máximo de reglas por plan de respaldo es 10. Si un plan contiene más de 10 reglas, se ignorará el plan de respaldo y no se creará ninguna copia de seguridad a partir de él.

a. En Nombre de la regla, ingrese el nombre de la regla. El nombre de la regla distingue entre mayúsculas y minúsculas y solo puede contener caracteres alfanuméricos o guiones.

b. Para Schedule (Programar), seleccione una frecuencia de copia de seguridad en la lista Frequency (Frecuencia) y elija una de las opciones de la Backup window (Ventana Copia de seguridad). Le recomendamos que elija Usar valores predeterminados de intervalo de copia de seguridad: recomendado.

5. En Lifecycle (Ciclo de vida), elija la configuración de ciclo de vida que desee.

6. En Backup vault name (Nombre de almacén de copia de seguridad), escriba un nombre. Este es el almacén de copia de seguridad donde se almacenarán los puntos de recuperación creados por las copias de seguridad.

   Asegúrese de que la bóveda de copias de seguridad esté en todas sus cuentas. AWS Backup no comprueba esto.

7. (opcional) Elija una región de destino de la lista si desea que las copias de seguridad se copien en otra Región de AWS y añada etiquetas. Puede elegir etiquetas para los puntos de recuperación que se crean, independientemente de la configuración de copia entre regiones. También puede agregar más reglas.

8. En la sección Asignación de recursos, indique el nombre del rol AWS Identity and Access Management (IAM). Para usar el rol AWS Backup de servicio, proporcione`service-role/AWSBackupDefaultServiceRole`.

   AWS Backup asume esta función en cada cuenta para obtener los permisos necesarios para realizar tareas de copia de seguridad y copia, incluidos los permisos de clave de cifrado, cuando proceda. AWS Backup también usa esta función para realizar eliminaciones durante el ciclo de vida.

   > **Note**
   >
   > AWS Backup no valida la existencia del rol o si se puede asumir el rol.
   > En el caso de los planes de respaldo creados mediante la administración multicuenta, AWS Backup utilizará la configuración opcional de la cuenta de administración y sustituirá la configuración de las cuentas específicas.

Para cada cuenta a la que desee agregar políticas de copia de seguridad, debe crear los almacenes y los roles de IAM usted mismo.

9. Agrega etiquetas para seleccionar los recursos de los que deseas hacer una copia de seguridad. El número máximo de etiquetas permitido es 30.

   AWS Organizations la política permite especificar 30 etiquetas como máximo si se crea un plan de respaldo mediante la política de Organizations. Se pueden incluir etiquetas adicionales utilizando múltiples asignaciones de recursos o contratando múltiples planes de respaldo.

   Si el número de etiquetas supera las 30 en la misma selección de copia de seguridad, ya sea modificando la selección existente o `@@append` utilizándola, el plan de copia de seguridad dejará de ser válido y se eliminará de la cuenta local.

10. En la sección Configuración avanzada, elija Windows VSS si el recurso del que desea hacer una copia de seguridad ejecuta Microsoft Windows en una instancia de Amazon EC2. Esto le permite realizar copias de seguridad de Windows VSS coherentes con la aplicación.

    Note

    AWS Backup actualmente solo admite copias de seguridad coherentes con las aplicaciones de los recursos que se ejecutan en Amazon EC2. No todos los tipos de instancia o aplicaciones son compatibles con las copias de seguridad de Windows VSS. Para obtener más información, consulte Creación de copias de seguridad de Windows VSS.

11. Elija Add backup plan (Agregar plan de copia de seguridad) para agregarlo a la política y, a continuación, elija Create backup policy (Crear política de copia de seguridad).

    La creación de una política de copia de seguridad no protege los recursos hasta que la adjunte a las cuentas. Puede elegir el nombre de la política y ver los detalles.

    El siguiente es un ejemplo de AWS Organizations política que crea un plan de respaldo. Si habilita la Copia de seguridad de Windows VSS, debe agregar permisos que le permitan realizar copias de seguridad coherentes con la aplicación, como se muestra en la sección `advanced_backup_settings` de la política.

```
{
  "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. En la sección Targets (Destinos) elija la unidad organizativa o la cuenta a la que desea adjuntar la política y elija Attach (Adjuntar). La política también se puede agregar a unidades organizativas o cuentas individuales.

> **Note**
>
> Asegúrese de validar la política y de incluir todos los campos obligatorios en la política. Si hay partes de la política que no son válidas, AWS Backup ignora esas partes, pero las partes válidas de la política funcionarán sin problema. Actualmente, AWS Backup no valida la exactitud de AWS Organizations las políticas.
> Si aplica una política a la cuenta de administración y una política diferente a una cuenta miembro, y ambas políticas entran en conflicto (por ejemplo, tienen periodos de retención de copias de seguridad diferentes), ambas políticas se ejecutarán sin problemas (es decir, las políticas se ejecutarán de forma independiente para cada cuenta). Por ejemplo, si la política de la cuenta de administración realiza una copia de seguridad de un volumen de Amazon EBS una vez al día y la política local realiza una copia de seguridad de un volumen de Amazon EBS una vez a la semana, se ejecutarán ambas políticas.
> Si faltan campos obligatorios en la política efectiva que se aplicará a una cuenta (probablemente debido a la combinación de diferentes políticas), AWS Backup no aplica la política a la cuenta. Si algunos ajustes no son válidos, AWS Backup los ajusta.

Independientemente de la configuración de suscripción de una cuenta de miembro en un plan de respaldo creado a partir de una política de respaldo, AWS Backup utilizará la configuración de suscripción especificada en la cuenta de administración de la organización.

Cuando se adjunta una política a una unidad organizativa, cada cuenta que se une a esta unidad organizativa obtiene esta política automáticamente y cada cuenta que se quita de la unidad organizativa pierde esta política. Los planes de copia de seguridad correspondientes se eliminan automáticamente de esa cuenta.

Monitorización de actividades en varias Cuentas de AWS

Para supervisar los trabajos de copia de seguridad, copia y restauración en todas las cuentas, debe habilitar la supervisión entre cuentas. Esto le permite monitorizar las actividades de copia de seguridad en todas las cuentas desde la cuenta de administración de la organización. Después de

participar, todos los trabajos de la organización que se crearon después de la suscripción están visibles. Cuando se desactiva, AWS Backup mantiene los trabajos en la vista conjunta durante 30 días (desde que se llega a un estado de finalización). Los trabajos creados después de la exclusión no son visibles y no muestran los trabajos de copia de seguridad recién creados. Para obtener instrucciones de aceptación, consulte Habilitación de la administración entre cuentas.

Para supervisar varias cuentas

1. Ábrela Consola de AWS Backup en https://console.aws.amazon.com/backup/. Debe iniciar sesión con las credenciales de la cuenta de administración.
2. En el panel de navegación izquierdo, elija Settings (Configuración) para abrir la página de administración entre cuentas.
3. En la sección Supervisión entre cuentas elija Enable (Habilitar).

   Esto le permite monitorizar las actividades de copia de seguridad y restauración de todas las cuentas de su organización desde su cuenta de administración.
4. En el panel de navegación izquierdo, elija Cross-account monitoring (Supervisión entre cuentas).
5. En la página Cross-account monitoring (Supervisión entre cuentas) elija la pestaña Backup jobs (Trabajos de copia de seguridad), Restore jobs (Trabajos de restauración) o Copy jobs (Trabajos de copia) para ver todos los trabajos creados en todas sus cuentas. Puedes ver cada uno de estos trabajos por Cuenta de AWS ID y puedes ver todos los trabajos de una cuenta concreta.
6. En el cuadro de búsqueda, puede filtrar los trabajos por Account ID (ID de cuenta), Status (Estado), o Job ID (ID de trabajo).

   Por ejemplo, puede elegir la pestaña Backup jobs (Trabajos de copia de seguridad) y ver todos los trabajos de copia de seguridad creados en todas sus cuentas. Puede filtrar la lista por Account ID (ID de cuenta) y ver todos los trabajos de copia de seguridad creados en esa cuenta.

Reglas de suscripción de recursos

Si el plan de respaldo de una cuenta de miembro se creó mediante una política de respaldo a nivel de organización, la configuración de AWS Backup suscripción de la cuenta de administración de la organización anulará la configuración de suscripción de esa cuenta de miembro, pero solo para ese plan de respaldo.

Si la cuenta miembro también tiene planes de copia de seguridad a nivel local creados por los usuarios, dichos planes de copia de seguridad seguirán la configuración de suscripción de la cuenta miembro, sin referencia a la configuración de suscripción de la cuenta de administración de Organizations.

Definición de políticas, sintaxis de políticas y herencia de políticas

Los siguientes temas están documentados en la Guía del usuario. AWS Organizations

- Políticas de copia de seguridad: consulte Políticas de copia de seguridad.
- Sintaxis de políticas: consulte Ejemplos y sintaxis de políticas de copia de seguridad.
- Herencia para tipos de políticas de administración: consulte Herencia para tipos de políticas de administración.

AWS Backup y AWS CloudFormation

En general

Con AWS CloudFormation, puede aprovisionar y administrar sus recursos de AWS de forma segura y repetible mediante las plantillas que cree. Puede utilizar plantillas de AWS CloudFormation y conjuntos de pilas para administrar sus planes de copia de seguridad, selecciones de recursos de copia de seguridad y almacenes de copias de seguridad. Para obtener información sobre el uso de AWS CloudFormation, consulte ¿Cómo funciona AWS CloudFormation? en la Guía del usuario de AWS CloudFormation.

Antes de crear su plantilla de AWS CloudFormation o conjunto de pilas, debe tener en cuenta lo siguiente:

- Cree plantillas independientes para sus planes de copia de seguridad y sus almacenes de copias de seguridad. Solo puede eliminar los almacenes de copias de seguridad que estén vacíos. No puede eliminar una pila que tenga almacenes de copias de seguridad si contienen puntos de recuperación.
- Verifique que tiene disponible un rol de servicio antes de crear la pila. El rol de servicio predeterminado de AWS Backup se crea automáticamente la primera vez que asigna recursos a un plan de copia de seguridad. Si no ha asignado recursos al plan de copia de seguridad, hágalo antes de crear la pila. También puede especificar un rol personalizado que haya creado. Para obtener más información acerca de los roles de , consulte Funciones de servicio de IAM.

Implementación de un almacén de copias de seguridad, un plan de copia de seguridad y una asignación de recursos mediante AWS CloudFormation

Para ver ejemplos de plantillas de AWS CloudFormation que implementan un almacén de copia de seguridad, planes de copia de seguridad y asignación de recursos, consulte Asignación de recursos mediante AWS CloudFormation.

Implementación de planes de copia de seguridad mediante AWS CloudFormation

Para ver ejemplos de plantillas de AWS CloudFormation que implementan planes de copia de seguridad, consulte Plantillas de AWS CloudFormation para planes de copia de seguridad.

Implementación de marcos y planes de informes de AWS Backup Audit Manager mediante AWS CloudFormation

Para ver ejemplos de plantillas de AWS CloudFormation que implementan marcos y planes de informes de AWS Backup Audit Manager, consulte Plantillas de AWS CloudFormation para planes de copia de seguridad.

Implementación de planes de copia de seguridad en todas las cuentas mediante AWS CloudFormation

Puede utilizar conjuntos de pilas de AWS CloudFormation en varias cuentas en una AWS Organization. Hay plantillas de muestra disponibles en la Guía del usuario de AWS CloudFormation.

Un excelente punto de partida y referencia es la publicación Automate centralized backup at scale across AWS services using AWS Backup. Por Ibukun Oyewumi y Sabith Venkitachalapathy (julio de 2021).

Más información sobre AWS CloudFormation

Para obtener información sobre el uso de AWS CloudFormation con AWS Backup, consulte la AWS Backup Resource Type Reference en la Guía del usuario de AWS CloudFormation.

Para obtener más información sobre el control de acceso a los recursos del servicio de AWS cuando utiliza AWS CloudFormation, consulte Controlar el acceso con AWS Identity and Access Management en la Guía del usuario de AWS CloudFormation.

Seguridad en AWS Backup

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS Backup, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad con respecto a AWS Backup incluye, pero no se limita a, lo siguiente. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.
  - Responder a las comunicaciones que reciba de AWS.
  - Administrar las credenciales que usted y su equipo utilizan. Para obtener más información, consulte Administración de identidad y acceso en AWS Backup.
  - Configurar los planes de copia de seguridad y las asignaciones de recursos para que reflejen las políticas de protección de datos de su organización. Para obtener más información, consulte Administración de planes de copia de seguridad.
  - Probar periódicamente la capacidad de encontrar determinados puntos de recuperación y restaurarlos. Para obtener más información, consulte Trabajar con copias de seguridad.
  - Incorporar AWS Backup los procedimientos en los procedimientos escritos de recuperación ante desastres y continuidad empresarial de su organización. Para empezar, consulte Introducción a AWS Backup.
  - Asegúrese de que sus empleados estén familiarizados con los procedimientos organizativos y hayan practicado utilizarlos AWS Backup junto con ellos en caso de una emergencia. Para obtener más información, consulte AWS Well-Architected Framework.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Backup. Los siguientes temas muestran cómo configurarlo AWS Backup para

cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS Backup recursos.

Temas

Validación de conformidad para AWS Backup

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñar una arquitectura basada en la seguridad y el cumplimiento de la HIPAA Amazon Web Services: este documento técnico describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Protección de datos en AWS Backup

AWS Backup se ajusta al modelo de responsabilidad AWS compartida, que incluye normas y directrices para la protección de datos. AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los AWS servicios. AWS mantiene el control de los datos alojados en esta infraestructura, incluidos los controles de configuración de seguridad para gestionar el contenido y los datos personales de los clientes. AWS los clientes y los socios de AWS Partner Network (APN),

que actúan como controladores o procesadores de datos, son responsables de cualquier dato personal que introduzcan en la Nube de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure cuentas de usuario individuales con AWS Identity and Access Management (IAM). Esto ayuda a garantizar que a cada usuario solo se le otorguen los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice una capa de conexión segura (SSL)/seguridad de la capa de transporte (TLS) para comunicarse con los recursos de AWS .
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de los AWS servicios.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Nombre. Esto incluye cuando trabaja con AWS Backup u otros AWS servicios mediante la consola, la API o AWS los SDK. AWS CLI Es posible que cualquier dato que ingrese en AWS Backup o en otros servicios se incluya en los registros de diagnóstico. Cuando proporcione una URL a un servidor externo, no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

Para obtener más información sobre la protección de datos, consulte la entrada de blog relativa al modelo de responsabilidad compartida de AWS y GDPR en el blog de seguridad de AWS .

Cifrado de copias de seguridad en AWS Backup

> **Note**
>
> AWS Backup Audit Manager le ayuda a detectar automáticamente las copias de seguridad no cifradas.

Puede configurar el cifrado para los tipos de recursos que permiten una AWS Backup administración total de su uso AWS Backup. Si el tipo de recurso no admite la AWS Backup administración completa, debe configurar su cifrado de respaldo siguiendo las instrucciones de ese servicio, como el cifrado de Amazon EBS en la Guía del usuario de Amazon Elastic Compute Cloud. Para ver la lista

de tipos de recursos que admiten la AWS Backup administración completa, consulte la sección « AWS Backup Administración completa» de la Disponibilidad de características por recurso tabla.

En la siguiente tabla se muestra cada tipo de recurso admitido, cómo está configurado el cifrado para las copias de seguridad y si se admite el cifrado independiente para las copias de seguridad. Cuando AWS Backup cifra de forma independiente una copia de seguridad, utiliza el algoritmo de cifrado AES-256 estándar del sector.

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
Amazon Simple Storage Service (Amazon S3)	Las copias de seguridad de Amazon S3 se cifran mediante una clave AWS KMS (AWS Key Management Service) asociada a la bóveda de copias de seguridad. La clave AWS KMS puede ser una CMK administrada por el cliente o una CMK AWS administrada asociada al servicio. AWS Backup AWS Backup cifra todas las copias de seguridad incluso si los buckets de Amazon S3 de origen no están cifrados.	Compatible
Máquinas virtuales de VMware	Las copias de seguridad de las máquinas virtuales siempre están cifradas. La clave de AWS KMS cifrado para las copias de seguridad de las máquinas virtuales se configura en el AWS Backup almacén en el que se almacenan las copias de	Compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
	seguridad de las máquinas virtuales.	
Amazon DynamoDB después de habilitar Copia de seguridad avanzada de DynamoDB	Las copias de seguridad de DynamoDB siempre están cifradas. La clave de AWS KMS cifrado de las copias de seguridad de DynamoDB se configura en AWS Backup el almacén en el que se almacenan las copias de seguridad de DynamoDB.	Compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
Amazon DynamoDB sin habilitar Copia de seguridad avanzada de DynamoDB	Las copias de seguridad de DynamoDB se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar la tabla de DynamoDB de origen. Las instantáneas de tablas de DynamoDB sin cifrar también están sin cifrar. **Note** AWS Backup Para crear una copia de seguridad de una tabla de DynamoDB cifrada, debe añadir los `kms:Decrypt` permisos `kms:GenerateDataKey` y la función de IAM utilizada para la copia de seguridad . Como alternativa, puede utilizar el rol de servicio predeterminado. AWS Backup	No compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
Amazon Elastic File System (Amazon EFS)	Las copias de seguridad de Amazon EFS siempre están cifradas. La clave de AWS KMS cifrado de las copias de seguridad de Amazon EFS se configura en el AWS Backup almacén en el que se almacenan las copias de seguridad de Amazon EFS.	Compatible
Amazon Elastic Block Store (Amazon EBS)	De forma predeterminada, las copias de seguridad de Amazon EBS se cifran con la clave que se utilizó para cifrar el volumen de origen, o no se cifran. Durante la restauración, puede especificar una clave de KMS para anular el método de cifrado predeterminado.	No compatible
AMI de Amazon Elastic Compute Cloud (Amazon EC2)	Las AMI no están cifradas. Las instantáneas de EBS se cifran según las reglas de cifrado predeterminadas para las copias de seguridad de EBS (consulte la entrada correspondiente a EBS). Las instantáneas de EBS de datos y volúmenes raíz se pueden cifrar y adjuntar a una AMI.	No compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
Amazon Relational Database Service (Amazon RDS)	Las instantáneas de Amazon RDS se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar la base de datos de Amazon RDS de origen. Las instantáneas de bases de datos de Amazon RDS sin cifrar también están sin cifrar. **Note** AWS Backup actualmente es compatible con todos los motores de bases de datos de Amazon RDS, incluido Amazon Aurora.	No compatible
Amazon Aurora	Las instantáneas de clúster de Aurora se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el clúster de Amazon Aurora de origen. Las instantáneas de clústeres de Aurora sin cifrar también están sin cifrar.	No compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
AWS Storage Gateway	Las instantáneas de Storage Gateway se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el volumen de Storage Gateway de origen. Las instantáneas de volúmenes de Storage Gateway sin cifrar también están sin cifrar. **Note** No es necesario utilizar una clave administrada por el cliente en todos los servicios para habilitar Storage Gateway. Basta con replicar la copia de seguridad de Storage Gateway en un almacén donde se haya configurado una clave de KMS. Esto se debe a que Storage Gateway no tiene una clave AWS KMS administrada específica del servicio.	No compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
Amazon FSx	Las características de cifrado de los sistemas de archivos de Amazon FSx varían en función del sistema de archivos subyacente. Para obtener más información sobre su sistema de archivos de Amazon FSx concreto, consulte la Guía del usuario de FSx correspon diente.	No compatible
Amazon DocumentDB	Las instantáneas de clúster de Amazon DocumentDB se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el clúster de Amazon DocumentDB de origen. Las instantáneas de clústeres de Amazon DocumentDB sin cifrar también están sin cifrar.	No compatible
Amazon Neptune	Las instantáneas de clúster de Neptune se cifran automátic amente con la misma clave de cifrado que se utilizó para cifrar el clúster de Neptune de origen. Las instantáneas de clústeres de Neptune sin cifrar también están sin cifrar.	No compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
Amazon Timestream	Las copias de seguridad de las instantáneas de la tabla de Timestream siempre están cifradas. La clave de cifrado de AWS KMS para las copias de seguridad de Timestream se configura en el almacén de copias de seguridad donde se almacenan las copias de seguridad de Timestream.	Compatible
Amazon Redshift	Las instantáneas de clúster de Amazon Redshift se cifran automáticamente con la misma clave de cifrado que se utilizó para cifrar el clúster de Amazon Redshift de origen. Las instantáneas de clústeres de Amazon Redshift sin cifrar también están sin cifrar.	No compatible
AWS CloudFormation	CloudFormation las copias de seguridad siempre están cifradas. La clave de CloudFormation cifrado de las CloudFormation copias de seguridad se configura en el CloudFormation almacén en el que se almacenan las CloudFormation copias de seguridad.	Compatible

Tipo de recurso	Cómo configurar el cifrado	AWS Backup Cifrado independiente
Bases de datos de SAP HANA en instancias de Amazon EC2	Las copias de seguridad de las bases de datos de SAP HANA siempre están cifradas. La clave de AWS KMS cifrado para las copias de seguridad de las bases de datos de SAP HANA se configura en el AWS Backup almacén en el que se almacenan las copias de seguridad de las bases de datos.	Compatible

Cifrado de copias de seguridad

Al copiar copias de AWS Backup seguridad entre cuentas o regiones, cifra AWS Backup automáticamente esas copias para la mayoría de los tipos de recursos, incluso si la copia de seguridad original no está cifrada. AWS Backup cifra la copia con la clave KMS del almacén de destino. Sin embargo, las instantáneas de los clústeres de Aurora, Amazon DocumentDB y Neptune sin cifrar tampoco están cifradas.

Copias cifradas y de respaldo

No se admite la copia multicuenta con claves de KMS AWS administradas en el caso de recursos que no estén completamente gestionados por AWS Backup. Consulte para AWS Backup Administración completa determinar qué recursos se administran por completo.

En el caso de los recursos que se administran en su totalidad AWS Backup, las copias de seguridad se cifran con la clave de cifrado del almacén de copias de seguridad. En el caso de los recursos que no se administran por completo AWS Backup, las copias multicuenta utilizan la misma clave de KMS que el recurso de origen. Para obtener más información, consulte Claves de cifrado y copias multicuenta.

Cifrado de credenciales del hipervisor de máquinas virtuales

Las máquinas virtuales administradas por un hipervisor utilizan una AWS Backup Gateway para conectar los sistemas en las instalaciones a AWS Backup. Es importante que los hipervisores cuenten con la misma seguridad sólida y fiable. Esta seguridad se puede lograr cifrando el hipervisor, ya sea mediante claves AWS propias o administradas por el cliente.

AWS claves propias y administradas por el cliente

AWS Backup proporciona cifrado para las credenciales del hipervisor a fin de proteger la información confidencial de inicio de sesión de los clientes mediante claves AWS de cifrado propias. En su lugar, tiene la opción de utilizar claves administradas por el cliente.

De forma predeterminada, las claves que se utilizan para cifrar las credenciales en el hipervisor son AWS claves propias. AWS Backup utiliza estas claves para cifrar automáticamente las credenciales del hipervisor. No puede ver, administrar ni usar las claves AWS propias, ni puede auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulta las claves AWS propias en la Guía para AWS KMS desarrolladores.

Como alternativa, las credenciales se pueden cifrar mediante claves administradas por el cliente. AWS Backup admite el uso de claves simétricas administradas por el cliente que usted crea, posee y administra para realizar el cifrado. Como usted tiene el control total de este cifrado, puede realizar tareas como las siguientes:

- Establecer y mantener políticas de claves
- Establecer y mantener concesiones y políticas de IAM
- Habilitar y deshabilitar políticas de claves
- Rotar el material criptográfico
- Agregar etiquetas.
- Crear alias de clave
- Programar la eliminación de claves

Cuando utilizas una clave gestionada por el cliente, AWS Backup valida si tu rol tiene permiso para descifrar con esta clave (antes de ejecutar una tarea de copia de seguridad o restauración). Debe agregar la acción `kms:Decrypt` al rol utilizado para iniciar un trabajo de copia de seguridad o restauración.

Como la acción `kms:Decrypt` no se puede agregar al rol de copia de seguridad predeterminado, debe usar un rol distinto del rol de copia de seguridad predeterminado para usar las claves administradas por el cliente.

Para obtener más información, consulte las claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service .

Concesión necesaria cuando se utilizan claves administradas por el cliente

AWS KMS requiere una concesión para utilizar la clave gestionada por el cliente. Al importar una configuración de hipervisor cifrada con una clave gestionada por el cliente, AWS Backup crea una concesión en tu nombre enviando una `CreateGrant`solicitud a AWS KMS. AWS Backup utiliza las concesiones para acceder a una clave de KMS en la cuenta de un cliente.

Puede revocar el acceso a la concesión o eliminar el acceso a AWS Backup la clave gestionada por el cliente en cualquier momento. Si lo hace, todas las puertas de enlace asociadas al hipervisor ya no podrán acceder al nombre de usuario y la contraseña del hipervisor cifrados por la clave administrada por el cliente, lo que afectará a sus trabajos de copia de seguridad y restauración. En concreto, los trabajos de copia de seguridad y restauración que realice en las máquinas virtuales de este hipervisor darán como resultado un error.

La puerta de enlace de la copia de seguridad utiliza la operación `RetireGrant` para eliminar una concesión cuando se elimina un hipervisor.

Monitorización de claves de cifrado

Cuando utilizas una clave gestionada por el AWS KMS cliente con tus AWS Backup recursos, puedes utilizar AWS CloudTrailAmazon CloudWatch Logs para realizar un seguimiento de las solicitudes que se AWS Backup envían a AWS KMS.

Busca AWS CloudTrail eventos con los siguientes `"eventName"` campos para supervisar AWS KMS las operaciones solicitadas para acceder AWS Backup a los datos cifrados por tu clave gestionada por el cliente:

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

Gestión de identidad y acceso en AWS Backup

El acceso a AWS Backup requiere credenciales. Estas credenciales deben tener permisos para acceder a los recursos de AWS como, por ejemplo, una base de datos de Amazon DynamoDB o un sistema de archivos de Amazon EFS. Además, los puntos de recuperación creados AWS Backup por algunos servicios AWS Backup compatibles no se pueden eliminar mediante el servicio de origen (como Amazon EFS). Puede eliminar esos puntos de recuperación utilizando AWS Backup.

En las siguientes secciones se proporcionan detalles sobre cómo utilizar AWS Identity and Access Management (IAM) y cómo ayudar AWS Backup a proteger el acceso a los recursos.

> **Warning**
>
> AWS Backup utiliza la misma función de IAM que eligió al asignar recursos para administrar el ciclo de vida de sus puntos de recuperación. Si elimina o modifica esa función, AWS Backup no podrá administrar el ciclo de vida de los puntos de recuperación. Cuando esto ocurra, intentará utilizar un rol vinculado al servicio para administrar su ciclo de vida. En un pequeño porcentaje de casos, es posible que esto tampoco funcione y deje puntos de recuperación `EXPIRED` en el almacenamiento, lo que podría generar costos no deseados. Para eliminar los puntos de recuperación `EXPIRED`, elimínelos manualmente mediante el procedimiento descrito en Eliminación de copias de seguridad.

Temas

Autenticación

El acceso a AWS Backup los AWS servicios de los que está realizando una copia de seguridad requieren credenciales que AWS pueda utilizar para autenticar sus solicitudes. Puede acceder AWS con cualquiera de los siguientes tipos de identidades:

- Cuenta de AWS usuario root: cuando te registras AWS, proporcionas una dirección de correo electrónico y una contraseña asociadas a tu AWS cuenta. Se trata de su usuario raíz de la Cuenta de AWS . Sus credenciales proporcionan acceso completo a todos tus AWS recursos.

  > **Important**
  >
  > Por razones de seguridad, recomendamos que utilice el usuario raíz solo para crear un administrador. El administrador es un usuario de IAM con permisos completos en su Cuenta de AWS. Entonces, podrá utilizar este usuario administrador para crear otros roles y usuarios de IAM con permisos limitados. Para obtener más información, consulte Prácticas recomendadas de IAM y Creación del primer grupo y usuario de administrador de IAM en la Guía del usuario de IAM.

- Usuario de IAM: un usuario de IAM es una identidad dentro de su Cuenta de AWS que tiene permisos personalizados específicos (por ejemplo, permisos para crear un almacén de copias de seguridad para almacenar sus copias de seguridad). Puede utilizar un nombre de usuario y una contraseña de IAM para iniciar sesión en AWS páginas web seguras AWS Management Console, como los foros de AWS debate o el AWS Support Centro.

  Además de un nombre de usuario y una contraseña, también puede generar claves de acceso para cada usuario. Puede usar estas claves al acceder a AWS los servicios mediante programación, ya sea a través de uno de los diversos SDK o mediante la (AWS Command Line Interface CLI AWS). El SDK y las herramientas de la AWS CLI usan claves de acceso para firmar criptográficamente la solicitud. Si no utiliza las herramientas de AWS , debe firmar usted mismo la solicitud. Para obtener más información acerca de la autenticación de solicitudes, consulte Proceso de firma Signature Version 4 en la Referencia general de AWS.

- Rol de IAM: un rol de IAM es otra identidad de IAM que puede crear en la cuenta y que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Una función de IAM le permite obtener claves de acceso temporales que se pueden utilizar para acceder AWS a los servicios y recursos. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

  - Acceso de usuario federado: en lugar de crear un usuario de IAM, puede utilizar identidades de usuario preexistentes AWS Directory Service, del directorio de usuarios de su empresa o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un proveedor de identidad. Para obtener más información acerca de los usuarios federados, consulte Usuarios federados y roles en la Guía del usuario de IAM.

- Administración multicuenta: puedes usar un rol de IAM en tu cuenta para conceder otros Cuenta de AWS permisos a fin de administrar los recursos de tu cuenta. Para ver un ejemplo, consulte el tutorial: Delegar el acceso a todos los roles de Cuentas de AWS IAM en la Guía del usuario de IAM.
- AWS acceso al servicio: puede utilizar un rol de IAM en su cuenta para conceder a un AWS servicio permisos de acceso a los recursos de su cuenta. Para obtener más información, consulte Creación de un rol para delegar permisos a un AWS servicio en la Guía del usuario de IAM.
- Aplicaciones que se ejecutan en Amazon Elastic Compute Cloud (Amazon EC2): puede utilizar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia de Amazon EC2 y que realizan solicitudes de API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene la función y permite a los programas que se encuentran en ejecución en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

Control de acceso

Puedes tener credenciales válidas para autenticar tus solicitudes, pero a menos que tengas los permisos adecuados, no podrás acceder a AWS Backup recursos como las bóvedas de respaldo. Tampoco puedes hacer copias de seguridad de AWS recursos como los volúmenes de Amazon Elastic Block Store (Amazon EBS).

Cada AWS recurso es propiedad de un Cuenta de AWS, y los permisos para crear o acceder a un recurso se rigen por las políticas de permisos. El administrador de una cuenta puede adjuntar políticas de permisos a las identidades AWS Identity and Access Management (de IAM) (es decir, a los usuarios, grupos y roles). Y algunos servicios también permiten asociar políticas de permisos a recursos.

> **Note**
>
> Un administrador de la cuenta (o usuario administrador) es un usuario con permisos de administrador. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

En las secciones siguientes se explica cómo funcionan las políticas de acceso y como puede utilizarlas para proteger sus copias de seguridad.

Temas

Recursos y operaciones

Un recurso es un objeto que existe dentro de un servicio. AWS Backup los recursos incluyen planes de respaldo, bóvedas de respaldo y copias de seguridad. Backup es un término general que se refiere a los distintos tipos de recursos de respaldo que existen en AWS. Por ejemplo, las instantáneas de Amazon EBS, las instantáneas de Amazon Relational Database Service (Amazon RDS) y las copias de seguridad de Amazon DynamoDB son todos tipos de recursos de copia de seguridad.

En AWS Backup, las copias de seguridad también se denominan puntos de recuperación. Cuando lo usa AWS Backup, también trabaja con los recursos de otros AWS servicios que intenta proteger, como los volúmenes de Amazon EBS o las tablas de DynamoDB. Estos recursos tienen nombres de recurso de Amazon (ARN) únicos asociados a ellos. Los ARN identifican los recursos de forma

exclusiva. AWS Debe tener un ARN cuando sea preciso especificar un recurso de forma inequívoca para todo AWS, como en las políticas de IAM o las llamadas a la API.

En la siguiente tabla se muestran recursos, subrecursos, formato de ARN y un ID único de ejemplo.

AWS Backup ARN de recursos

Tipo de recurso	Formato de ARN	ID único de ejemplo
Plan de copias de seguridad	`arn:aws:backup:` *region*`:`*account-id*`:backup-plan:*`	
Almacén de copias de seguridad	`arn:aws:backup:` *region*`:`*account-id*`:backup-vault:*`	
Punto de recuperación para Amazon EBS	`arn:aws:ec2:` *region*`::snapshot/*`	`snapshot/snap-05f426fd8kdjb4224`
Punto de recuperación para imágenes de Amazon EC2	`arn:aws:ec2:` *region*`::image/ami-*`	`image/ami-1a2b3e4f5e6f7g890`
Punto de recuperación para Amazon RDS	`arn:aws:rds:` *region*`:`*account-id*`:snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Punto de recuperación para Aurora	`arn:aws:rds:` *region*`:`*account-id*`:cluster-snapshot:awsbackup:*`	`awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453`
Punto de recuperación para Storage Gateway	`arn:aws:ec2:` *region*`::snapshot/*`	`snapshot/snap-0d40e49137e31d9e0`

Tipo de recurso	Formato de ARN	ID único de ejemplo
Punto de recuperación para DynamoDB sin Copia de seguridad avanzada de DynamoDB	`arn:aws:dynamodb:region:account-id:table/*/backup/*`	`table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3`
Punto de recuperación para DynamoDB con Copia de seguridad avanzada de DynamoDB habilitado	`arn:aws:backup:region:account-id:recovery-point:*`	`12a34a56-7bb8-901c-cd23-4567d8e9ef01`
Punto de recuperación para Amazon EFS	`arn:aws:backup:region:account-id:recovery-point:*`	`d99699e7-e183-477e-bfcd-ccb1c6e5455e`
Punto de recuperación para Amazon FSx	`arn:aws:fsx:region:account-id:backup/backup-*`	`backup/backup-1a20e49137e31d9e0`
Punto de recuperación para máquina virtual	`arn:aws:backup:region:account-id:recovery-point:*`	`1801234a-5b6b-7dc8-8032-836f7ffc623b`
Punto de recuperación para la copia de seguridad continua de Amazon S3	`arn:aws:backup:region:account-id:recovery-point:*`	*my-bucket* `-5ec207d0`
Punto de recuperación para la copia de seguridad periódica de S3	`arn:aws:backup:region:account-id:recovery-point:*`	*my-bucket* `-20211231900000-5ec207d0`
Punto de recuperación para Amazon DocumentDB	`arn:aws:rds:region:account-id:cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`

Tipo de recurso	Formato de ARN	ID único de ejemplo
Punto de recuperación de Neptuno	`arn:aws:rds:` *region*`:` *account-id* `:cluster-snapshot:awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Punto de recuperación para Amazon Redshift	`arn:aws:redshift:` *region*`:` *account-id* `:snapshot:` *resource*`/awsbackup:*`	`awsbackup:job-ab12cd3e-4567-8901-fg1h-234567i89012`
Punto de recuperación para Amazon Timestream	`arn:aws:backup:` *region*`:` *account-id* `:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012_beta`
Punto de recuperación de la plantilla AWS CloudFormation	`arn:aws:backup:` *region*`:` *account-id* `:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`
Punto de recuperación para la base de datos SAP HANA en la instancia Amazon EC2	`arn:aws:backup:` *region*`:` *account-id* `:recovery-point:*`	`recovery-point:1a2b3cde-f405-6789-012g-3456hi789012`

Todos los recursos que permiten una AWS Backup administración completa tienen puntos de recuperación en ese formato, lo que facilita la aplicación de políticas de permisos para proteger esos puntos de recuperación`arn:aws:backup:`*region*`:`*account-id:*`:recovery-point:*`. Para ver qué recursos admiten la AWS Backup administración completa, consulte esa sección de la Disponibilidad de características por recurso tabla.

AWS Backup proporciona un conjunto de operaciones para trabajar con AWS Backup los recursos. Para ver la lista de las operaciones disponibles, consulte AWS Backup Acciones.

Propiedad del recurso

Cuenta de AWS Es propietario de los recursos que se crean en la cuenta, independientemente de quién los haya creado. En concreto, el propietario del recurso es el Cuenta de AWS de la entidad principal (es decir, el usuario Cuenta de AWS raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos. Los siguientes ejemplos ilustran cómo funciona:

- Si utiliza sus credenciales de usuario Cuenta de AWS raíz Cuenta de AWS para crear un almacén de respaldo, será el Cuenta de AWS propietario del almacén.
- Si crea un usuario de IAM en su cuenta Cuenta de AWS y le concede permisos para crear una bóveda de copias de seguridad, el usuario podrá crear una bóveda de copias de seguridad. Sin embargo, la cuenta de AWS a la que pertenece el usuario será la propietaria del recurso del almacén de copias de seguridad.
- Si crea una función de IAM Cuenta de AWS con permisos para crear una bóveda de copias de seguridad, cualquier persona que pueda asumir esa función podrá crear una bóveda. Usted Cuenta de AWS, al que pertenece el rol, es propietario del recurso de la bóveda de respaldo.

Especificación de los elementos de las políticas: acciones, efectos y entidades principales

Para cada AWS Backup recurso (consulteRecursos y operaciones), el servicio define un conjunto de operaciones de API (consulteAcciones). Para conceder permisos para estas operaciones de la API, AWS Backup define un conjunto de acciones que puede especificar en una política. Para realizar una operación API pueden ser necesarios permisos para más de una acción.

A continuación se indican los elementos más básicos de la política:

- Recurso: en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte Recursos y operaciones.
- Acción: utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar.
- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.

- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos).

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte IAM JSON Policy Reference (Referencia de la política JSON de IAM) en la Guía del usuario de IAM.

Para ver una tabla que muestra todas las acciones de la AWS Backup API, consultePermisos de la API: referencia de acciones, recursos y condiciones.

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de IAM para especificar las condiciones en la que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte Condition en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

AWS Backup define su propio conjunto de claves de condición. Para ver una lista de claves de AWS Backup condición, consulte las claves de condición AWS Backup en la Referencia de autorización de servicio.

Permisos de la API: referencia de acciones, recursos y condiciones

Cuando configure Control de acceso y escriba una política de permisos que se pueda asociar a una identidad de IAM (políticas basadas en identidad), puede utilizar la siguiente lista como referencia. La incluye cada operación de la AWS Backup API, las acciones correspondientes para las que puedes conceder permisos para realizar la acción y el AWS recurso para el que puedes conceder los permisos. Las acciones se especifican en el campo `Action` de la política y el valor del recurso se especifica en el campo `Resource` de la política. Si el campo `Resource` está en blanco, puede usar el comodín (*) para incluir todos los recursos.

Puedes usar claves AWS de condición generales en tus AWS Backup políticas para expresar las condiciones. Para obtener una lista completa de las claves AWS anchas, consulta las claves disponibles en la Guía del usuario de IAM.

[1] Utiliza la política de acceso al depósito existente.

[2] Consulte los ARN AWS Backup ARN de recursos de puntos de recuperación específicos de cada recurso.

[3] `StartRestoreJob` deben tener el par clave-valor en los metadatos del recurso. Para obtener los metadatos del recurso, llame a la API `GetRecoveryPointRestoreMetadata`.

[4] Algunos tipos de recursos requieren que el rol que realiza la copia de seguridad tenga un permiso de etiquetado específico `backup:TagResource` si planea incluir etiquetas de recursos originales en la copia de seguridad o agregar etiquetas adicionales a una copia de seguridad. Cualquier copia de seguridad con un ARN que comience por `arn:aws:backup:region:account-id:recovery-point:` o que sea continua requiere este permiso. `backup:TagResource`el permiso debe aplicarse a `"resourcetype": "arn:aws:backup:region:account-id:recovery-point:*"`

Para obtener más información, consulte Acciones, recursos y claves de condición de AWS Backup en la Referencia de autorizaciones de servicio.

Permisos de copia de etiquetas

Cuando AWS Backup realiza un trabajo de copia de seguridad o copia, intenta copiar las etiquetas del recurso de origen (o del punto de recuperación en el caso de una copia) al punto de recuperación.

> **Note**
>
> AWS Backup no copia las etiquetas de forma nativa durante los trabajos de restauración. Para ver una arquitectura basada en eventos que copie las etiquetas durante los trabajos de restauración, consulte Cómo conservar las etiquetas de recursos en AWS Backup los trabajos de restauración.

Durante un trabajo de copia de seguridad o copia, AWS Backup agrega las etiquetas que especifique en su plan de copia de seguridad (o plan de copia o copia de seguridad bajo demanda) con las etiquetas del recurso de origen. Sin embargo, AWS impone un límite de 50 etiquetas por recurso, que AWS Backup no se puede superar. Cuando un trabajo de copia de seguridad o copia agrega etiquetas del plan y del recurso de origen, podría detectar más de 50 etiquetas en total, no podrá completar el trabajo y dará como resultado un error. Esto es coherente con las mejores AWS

prácticas de etiquetado en general. Para obtener más información, consulte Tag limits en la Guía de referencia general de AWS .

- Su recurso tiene más de 50 etiquetas después de agregar las etiquetas de los trabajos de respaldo con las etiquetas de los recursos de origen. AWS admite hasta 50 etiquetas por recurso. Para obtener más información, consulte Tag limits.
- La función de IAM que le proporciones AWS Backup carece de permisos para leer las etiquetas de origen o establecer las etiquetas de destino. Para obtener más información y un ejemplo de las políticas del rol de IAM, consulte Políticas administradas.

Puede utilizar su plan de copia de seguridad para crear etiquetas que contradigan las etiquetas del recurso de origen. Cuando ambas estén en conflicto, prevalecerán las etiquetas del plan de copia de seguridad. Utilice esta técnica si prefiere no copiar el valor de una etiqueta del recurso de origen. Especifique la misma clave de etiqueta, pero con un valor diferente o vacío, utilizando su plan de copia de seguridad.

Permisos necesarios para asignar etiquetas a copias de seguridad

Tipo de recurso	Permiso necesario
Sistema de archivos de Amazon EFS	`elasticfilesystem:DescribeTags`
Sistema de archivos de Amazon FSx	`fsx:ListTagsForResource`
Base de datos de Amazon RDS y clúster de Amazon Aurora	`rds:AddTagsToResource` `rds:ListTagsForResource`
Volumen de Storage Gateway	`storagegateway:ListTagsForResource`
Instancia de Amazon EC2 y volumen de Amazon EBS	`EC2:CreateTags` `EC2:DescribeTags`

DynamoDB no admite la asignación de etiquetas a las copias de seguridad a menos que habilite primero la Copia de seguridad avanzada de DynamoDB.

Cuando una copia de seguridad de Amazon EC2 crea un punto de recuperación de imágenes y un conjunto de instantáneas, AWS Backup copia las etiquetas en la AMI resultante. AWS Backup también copia las etiquetas de los volúmenes asociados a la instancia de Amazon EC2 en las instantáneas resultantes.

Políticas de acceso

Una política de permisos describe quién tiene acceso a qué. Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en identidades (o políticas de IAM). Las políticas asociadas a un recurso se denominan políticas basadas en recursos. AWS Backup admite tanto las políticas basadas en la identidad como las políticas basadas en los recursos.

> **Note**
>
> En esta sección se analiza el uso de la IAM en el contexto de. AWS Backup No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte ¿Qué es IAM? en la Guía del usuario de IAM. Para obtener más información acerca de la sintaxis y las descripciones de las políticas de IAM, consulte Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Políticas basadas en identidades (políticas de IAM)

Las políticas basadas en identidad son políticas que puede asociar a identidades de IAM, como usuarios o roles. Por ejemplo, puede definir una política que permita a un usuario ver los AWS recursos y realizar copias de seguridad, pero que le impida restaurar las copias de seguridad.

Para obtener más información sobre usuarios, grupos, roles y permisos, consulte Identidades (usuarios, grupos y roles) en la Guía del usuario de IAM.

Para obtener más información acerca de cómo utilizar políticas de IAM para controlar el acceso a las copias de seguridad, consulte Políticas gestionadas para AWS Backup.

Políticas basadas en recursos

AWS Backup admite políticas de acceso basadas en recursos para las bóvedas de respaldo. De este modo, puede definir una política de acceso que puede controlar qué usuarios tienen qué tipo de acceso a cualquiera de las copias de seguridad organizadas en un almacén de copias de seguridad. Las políticas de acceso basadas en recursos para almacenes de copia de seguridad ofrecen una manera fácil de controlar el acceso a sus copias de seguridad.

Las políticas de acceso a la bóveda de Backup controlan el acceso de los usuarios cuando se utilizan AWS Backup las API. También se puede acceder a algunos tipos de copia de seguridad, como instantáneas de Amazon Elastic Block Store (Amazon EBS) y Amazon Relational Database Service (Amazon RDS), mediante las API de esos servicios. Puede crear políticas de acceso independientes en IAM que controlan el acceso a esas API con el fin de controlar plenamente el acceso a las copias de seguridad.

Para obtener información sobre cómo crear una política de acceso para almacenes de copias de seguridad, consulte Definición de políticas de acceso en los almacenes de copias de seguridad.

Funciones de servicio de IAM

Una función AWS Identity and Access Management (IAM) es similar a la de un usuario, ya que es una AWS identidad con políticas de permisos que determinan lo que la identidad puede y no puede hacer en AWS ella. No obstante, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Una función de servicio es una función que asume un AWS servicio para realizar acciones en su nombre. Como servicio que realiza las operaciones de copia de seguridad en su nombre, AWS Backup requiere transferirle un rol que debe adoptar al realizar las operaciones de copia de seguridad en su nombre. Para obtener más información acerca de los roles de IAM, consulte Roles de IAM en la guía del usuario de IAM.

El rol al que se transfiera AWS Backup debe tener una política de IAM con los permisos que le permitan realizar las acciones asociadas AWS Backup a las operaciones de copia de seguridad, como crear, restaurar o caducar copias de seguridad. Se requieren permisos diferentes para cada uno de los AWS servicios compatibles AWS Backup . El rol también debe AWS Backup figurar como entidad de confianza, lo que AWS Backup permite asumirlo.

Al asignar recursos a un plan de copia de seguridad, o si realiza una copia de seguridad, copia o restauración bajo demanda, debe asignar una función de servicio que tenga acceso para realizar las operaciones subyacentes en los recursos especificados. AWS Backup utiliza esta función para crear, etiquetar y eliminar recursos de su cuenta.

Usa AWS roles para controlar el acceso a las copias de seguridad

Puede utilizar roles para controlar el acceso a sus copias de seguridad definiendo roles muy acotados y especificando quién puede transferir dicho rol a AWS Backup. Por ejemplo, puede crear un rol que solo conceda permisos para realizar copias de seguridad de las bases de datos de Amazon Relational Database Service (Amazon RDS) y que solo conceda permiso a los propietarios de las bases de datos de Amazon RDS para transferir ese rol. AWS Backup AWS

Backup proporciona varias políticas administradas predefinidas para cada uno de los servicios compatibles. Puede asociar estas políticas administradas a los roles que cree. Esto facilita la creación de funciones específicas del servicio que tengan los permisos correctos que AWS Backup se necesitan.

Para obtener más información sobre las políticas AWS administradas para AWS Backup, consulte. Políticas gestionadas para AWS Backup

Función de servicio predeterminada para AWS Backup

Cuando utilice la AWS Backup consola por primera vez, puede optar por AWS Backup crear un rol de servicio predeterminado para usted. Este rol tiene los permisos AWS Backup necesarios para crear y restaurar copias de seguridad en su nombre.

> **Note**
>
> El rol predeterminado se crea automáticamente si usa la AWS Management Console. Puede crear el rol predeterminado con AWS Command Line Interface (AWS CLI), pero debe hacerlo manualmente.

Si prefiere usar roles personalizados, como roles independientes para diferentes tipos de recursos, también puede hacerlo y transferir sus roles personalizados a AWS Backup. Para ver ejemplos de roles que permiten la copia de seguridad y la restauración para tipos de recursos individuales, consulte la tabla Políticas administradas por el cliente.

El rol de servicio predeterminado se denomina`AWSBackupDefaultServiceRole`. Este rol de servicio contiene dos políticas administradas AWSBackupServiceRolePolicyForBackupy AWSBackupServiceRolePolicyForRestores.

`AWSBackupServiceRolePolicyForBackup`incluye una política de IAM que otorga AWS Backup permisos para describir el recurso del que se está haciendo la copia de seguridad y la posibilidad de crear, eliminar, describir o añadir etiquetas a una copia de seguridad, independientemente de la AWS KMS clave con la que esté cifrada.

`AWSBackupServiceRolePolicyForRestores`incluye una política de IAM que concede AWS Backup permisos para crear, eliminar o describir el nuevo recurso que se está creando a partir de una copia de seguridad, independientemente de la AWS KMS clave con la que esté cifrado. También incluye permisos para etiquetar el recurso recién creado.

Para restaurar una instancia de Amazon EC2, debe lanzar una instancia nueva.

Creación del rol de servicio en la consola

Las acciones específicas que se realizan en la AWS Backup consola crean el rol de servicio AWS Backup predeterminado.

Para crear el rol de servicio AWS Backup predeterminado en su AWS cuenta

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Para crear el rol de su cuenta, asigne recursos a un plan de copia de seguridad o cree una copia de seguridad bajo demanda.

   a. Cree un plan de copia de seguridad y asigne recursos a la copia de seguridad. Consulte Creación de una copia de seguridad programada.

   b. Como alternativa, cree una copia de seguridad bajo demanda. Consulte Creación de una copia de seguridad bajo demanda.
3. Siga estos pasos para comprobar que ha creado `AWSBackupDefaultServiceRole` en su cuenta:

   a. Espere unos minutos. Para obtener más información, consulte Los cambios que realizo no están siempre visibles inmediatamente en la Guía del usuario de AWS Identity and Access Management.

   b. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.

   c. En el menú de navegación izquierdo, elija Roles.

   d. En la barra de búsqueda, escriba `AWSBackupDefaultServiceRole`. Si existe esta selección, ha creado el rol AWS Backup predeterminado y ha completado este procedimiento.

   e. Si `AWSBackupDefaultServiceRole` sigue sin aparecer, agregue los siguientes permisos al usuario de IAM o al rol de IAM que utilice para acceder a la consola.

```
{
  "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":"*"
    }
  ]
}
```

Para las regiones de China, sustituya *aws* por *aws-cn*. En el AWS GovCloud (US) caso de las regiones, sustituya *aws* por *aws-us-gov*.

f. Si no puede agregar permisos a su usuario de IAM o rol de IAM, pida a su administrador que cree manualmente un rol con un nombre distinto de `AWSBackupDefaultServiceRole` y asocie ese rol a estas políticas administradas:

- `AWSBackupServiceRolePolicyForBackup`
- `AWSBackupServiceRolePolicyForRestores`

Políticas gestionadas para AWS Backup

Las políticas administradas son políticas independientes basadas en la identidad que puede adjuntar a varios usuarios, grupos y funciones de su organización. Cuenta de AWS Al asociar una política a una entidad principal, concederá a la entidad los permisos que están definidos en la política.

AWS las políticas gestionadas las crea y administra. AWS No puede cambiar los permisos definidos en las políticas AWS gestionadas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política.

Las políticas administradas por el cliente te proporcionan controles detallados para configurar el acceso a las copias de seguridad. AWS Backup Por ejemplo, puede utilizarlas para dar acceso al

administrador de copias de seguridad de su base de datos a las copias de seguridad de Amazon RDS, pero no a las de Amazon EFS.

Para obtener más información, consulte las políticas administradas en la Guía del usuario de IAM.

AWS políticas gestionadas

AWS Backup proporciona las siguientes políticas AWS administradas para casos de uso comunes. Estas políticas facilitan la definición de los permisos adecuados y controlan el acceso a sus copias de seguridad. Existen dos tipos de políticas administradas. Un tipo está diseñado para asignarlo a usuarios para controlar su acceso a AWS Backup. El otro tipo de política administrada está diseñado para asociarlo a los roles que transfiere a AWS Backup. En la siguiente tabla se muestran todas las políticas administradas que AWS Backup proporciona y describe la forma en que se definen. Encontrará estas políticas administradas en la sección Políticas de la consola de IAM.

Políticas

- AWSBackupAuditAccess
- AWSBackupDataTransferAccess
- AWSBackupFullAccess
- AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync
- AWSBackupOperatorAccess
- AWSBackupOrganizationAdminAccess
- AWSBackupRestoreAccessForSAPHANA
- AWSBackupServiceLinkedRolePolicyForBackup
- AWSBackupServiceLinkedRolePolicyForBackupTest
- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores
- AWSBackupServiceRolePolicyForS3Backup
- AWSBackupServiceRolePolicyForS3Restore
- AWSServiceRolePolicyForBackupReports
- AWSServiceRolePolicyForBackupRestoreTesting

AWSBackupAuditAccess

Esta política otorga permisos a los usuarios para crear controles y marcos que definan sus expectativas de AWS Backup recursos y actividades, y para auditar AWS Backup los recursos y las actividades comparándolos con los controles y marcos definidos. Esta política otorga permisos AWS Config y servicios similares para describir las expectativas de los usuarios y realizar las auditorías.

Esta política también otorga permisos para entregar informes de auditoría a Amazon S3 y servicios similares, y permite a los usuarios buscar y abrir sus informes de auditoría.

Para ver los permisos de esta política, consulte AWSBackupAuditAccessla Referencia de políticas AWS gestionadas.

AWSBackupDataTransferAccess

Esta política proporciona permisos para las API de transferencia de datos del plano de AWS Backup almacenamiento, lo que permite al agente AWS Backint completar la transferencia de los datos de respaldo con el plano AWS Backup de almacenamiento. Puede adjuntar esta política a las funciones que asumen las instancias de Amazon EC2 que ejecutan SAP HANA con el agente Backint.

Para ver los permisos de esta política, consulte la Referencia AWSBackupDataTransferAccessde políticas AWS administradas.

AWSBackupFullAccess

El administrador de copias de seguridad tiene pleno acceso a AWS Backup las operaciones, incluida la creación o edición de planes de copia de seguridad, la asignación de AWS recursos a los planes de copia de seguridad y la restauración de las copias de seguridad. Los administradores de las copias de seguridad tienen la responsabilidad de determinar e imponer medidas de conformidad definiendo planes de copias de seguridad que cumplan los requisitos empresariales y normativos de su organización. Los administradores de Backup también se aseguran de que AWS los recursos de su organización estén asignados al plan adecuado.

Para ver los permisos de esta política, consulte AWSBackupFullAccessla Referencia de políticas AWS gestionadas.

AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync

Para ver los permisos de esta política, consulte la Referencia de políticas AWS administradas.

AWSBackupOperatorAccess

Los operadores de copia de seguridad son usuarios que son responsables de garantizar una correcta copia de seguridad de los recursos de los que son responsables. Los operadores de backup tienen permisos para asignar AWS recursos a los planes de backup que crea el administrador de backup. También tienen permisos para crear copias de seguridad bajo demanda de sus AWS recursos y para configurar el período de retención de las copias de seguridad bajo demanda. Los operadores de copia de seguridad no tienen permisos para crear o editar los planes de copias de seguridad o eliminar copias de seguridad programadas después de que se hayan creado. Los operadores de copia de seguridad puede restaurar las copias de seguridad. Puede limitar los tipos de recursos que un operador de copia de seguridad puede asignar a un plan de copia de seguridad o restaurar desde una copia de seguridad. Para ello, se permite que solo se transfieran determinadas funciones de servicio AWS Backup que tengan permisos para un tipo de recurso determinado.

Para ver los permisos de esta política, consulte AWSBackupOperatorAccessla Referencia de políticas AWS administradas.

AWSBackupOrganizationAdminAccess

El administrador de la organización tiene pleno acceso a AWS Organizations las operaciones, incluidas la creación, edición o eliminación de políticas de copia de seguridad, la asignación de políticas de copia de seguridad a las cuentas y unidades organizativas y la supervisión de las actividades de copia de seguridad dentro de la organización. Los administradores de la organización son responsables de proteger las cuentas de la misma mediante la definición y asignación de políticas de copia de seguridad que cumplan con los requisitos reglamentarios y empresariales de su organización.

Para ver los permisos de esta política, consulta la Referencia AWSBackupOrganizationAdminAccessde políticas AWS gestionadas.

AWSBackupRestoreAccessForSAPHANA

Esta política otorga AWS Backup permiso para restaurar una copia de seguridad de SAP HANA en Amazon EC2.

Para ver los permisos de esta política, consulte la Referencia AWSBackupRestoreAccessForSAPHANAde políticas AWS gestionadas.

AWSBackupServiceLinkedRolePolicyForBackup

Esta política se adjunta a la función vinculada al servicio denominada AWSServiceRoleforBackup para permitir llamar AWS Backup a los AWS servicios en su nombre para gestionar las copias de seguridad. Para obtener más información, consulte the section called “Copia de seguridad y copia”.

Para ver los permisos de esta política, consulta la Referencia AWSBackupServiceLinkedRolePolicyforBackupde políticas AWS gestionadas.

AWSBackupServiceLinkedRolePolicyForBackupTest

Para ver los permisos de esta política, consulte AWSBackupServiceLinkedRolePolicyForBackupTestla Referencia de políticas AWS administradas.

AWSBackupServiceRolePolicyForBackup

Proporciona AWS Backup permisos para crear copias de seguridad de todos los tipos de recursos compatibles en su nombre.

Para ver los permisos de esta política, consulte AWSBackupServiceRolePolicyForBackupla Referencia de políticas AWS administradas.

AWSBackupServiceRolePolicyForRestores

Proporciona AWS Backup permisos para restaurar copias de seguridad de todos los tipos de recursos compatibles en su nombre.

Para ver los permisos de esta política, consulte AWSBackupServiceRolePolicyForRestoresla Referencia de políticas AWS administradas.

En el caso de las restauraciones de instancias EC2, también debe incluir los siguientes permisos para lanzar la instancia EC2:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/role-name",
            "Effect": "Allow"
        }
    ]
```

```
}
```

AWSBackupServiceRolePolicyForS3Backup

Esta política contiene los permisos necesarios AWS Backup para realizar copias de seguridad de cualquier bucket de S3. Esto incluye el acceso a todos los objetos de un depósito y a cualquier AWS KMS clave asociada.

Para ver los permisos de esta política, consulte AWSBackupServiceRolePolicyForS3Backupla Referencia de políticas AWS gestionadas.

AWSBackupServiceRolePolicyForS3Restore

Esta política contiene los permisos necesarios AWS Backup para restaurar una copia de seguridad de S3 en un bucket. Esto incluye los permisos de lectura y escritura en los depósitos y el uso de cualquier AWS KMS clave en relación con las operaciones de S3.

Para ver los permisos de esta política, consulte la Referencia AWSBackupServiceRolePolicyForS3Restorede políticas AWS gestionadas.

AWSServiceRolePolicyForBackupReports

AWS Backup usa esta política para la función AWSServiceRoleForBackupReportsvinculada al servicio. Esta función vinculada al servicio otorga AWS Backup permisos para supervisar e informar sobre la conformidad de la configuración, los trabajos y los recursos de las copias de seguridad con sus marcos.

Para ver los permisos de esta política, consulta la Referencia AWSServiceRolePolicyForBackupReportsde políticas AWS gestionadas.

AWSServiceRolePolicyForBackupRestoreTesting

Para ver los permisos de esta política, consulte AWSServiceRolePolicyForBackupRestoreTestingla Referencia de políticas AWS administradas.

Políticas administradas por el cliente

En las siguientes secciones se describen los permisos de copia de seguridad y restauración recomendados para la aplicación Servicios de AWS y las aplicaciones de terceros compatibles con ellos AWS Backup. Puede utilizar las políticas AWS gestionadas existentes como modelo al crear

sus propios documentos de políticas y, a continuación, personalizarlos para restringir aún más el acceso a sus AWS recursos.

Amazon Aurora

Copia de seguridad

Comience con las siguientes afirmaciones de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurar

Comience con la `RDSPermissions` declaración de AWSBackupServiceRolePolicyForRestores.

Amazon DynamoDB

Copia de seguridad

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamodbBackupPermissions`
- `KMSDynamoDBPermissions`

Restaurar

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForRestores:

- `DynamoDBPermissions`
- `DynamoDBBackupResourcePermissions`
- `DynamoDBRestorePermissions`
- `KMSPermissions`

Amazon EBS

Copia de seguridad

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForBackup:

- `EBSResourcePermissions`
- `EBSTagAndDeletePermissions`
- `EBSCopyPermissions`
- `EBSSnapshotTierPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurar

Comience con la `EBSPermissions` declaración de AWSBackupServiceRolePolicyForRestores.

Agregue la siguiente instrucción.

```
{
      "Effect":"Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
},
```

Amazon EC2

Copia de seguridad

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForBackup:

- `EBSCopyPermissions`
- `EC2CopyPermissions`
- `EC2Permissions`
- `EC2TagPermissions`

- `EC2ModifyPermissions`
- `EBSResourcePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurar

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForRestores:

- `EBSPermissions`
- `EC2DescribePermissions`
- `EC2RunInstancesPermissions`
- `EC2TerminateInstancesPermissions`
- `EC2CreateTagsPermissions`

Agregue la siguiente instrucción.

```
{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/role-name"
},
```

Amazon EFS

Copia de seguridad

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForBackup:

- `EFSPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Restaurar

Comience con la `EFSPermissions` declaración de AWSBackupServiceRolePolicyForRestores.

Amazon FSx

Copia de seguridad

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForBackup:

- `FsxBackupPermissions`
- `FsxCreateBackupPermissions`
- `FsxPermissions`
- `FsxVolumePermissions`
- `FsxListTagsPermissions`
- `FsxDeletePermissions`
- `FsxResourcePermissions`
- `KMSPermissions`

Restaurar

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForRestores:

- `FsxPermissions`
- `FsxTagPermissions`
- `FsxBackupPermissions`
- `FsxDeletePermissions`
- `FsxDescribePermissions`
- `FsxVolumeTagPermissions`
- `FsxBackupTagPermissions`
- `FsxVolumePermissions`
- `DSPermissions`
- `KMSDescribePermissions`

Amazon RDS

Copia de seguridad

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForBackup:

- `DynamoDBBackupPermissions`
- `RDSBackupPermissions`
- `RDSClusterModifyPermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`
- `KMSPermissions`

Restaurar

Comience con la `RDSPermissions` declaración de AWSBackupServiceRolePolicyForRestores.

Amazon S3

Copia de seguridad

Comience por AWSBackupServiceRolePolicyForS3Backup.

Agregue los `BackupVaultCopyPermissions` estados de cuenta `BackupVaultPermissions` y si necesita copiar las copias de seguridad a una cuenta diferente.

Restaurar

Comience por AWSBackupServiceRolePolicyForS3Restore.

AWS Storage Gateway

Copia de seguridad

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForBackup:

- `StorageGatewayPermissions`
- `EBSTagAndDeletePermissions`
- `GetResourcesPermissions`
- `BackupVaultPermissions`

Agregue la siguiente instrucción.

```
{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
},
```

Restaurar

Comience con las siguientes declaraciones de AWSBackupServiceRolePolicyForRestores:

- `StorageGatewayVolumePermissions`
- `StorageGatewayGatewayPermissions`
- `StorageGatewayListPermissions`

Máquina virtual

Copia de seguridad

Comience con la `BackupGatewayBackupPermissions` declaración de AWSBackupServiceRolePolicyForBackup.

Restaurar

Comience con la `GatewayRestorePermissions` declaración de AWSBackupServiceRolePolicyForRestores.

Respaldo cifrado

Para restaurar una copia de seguridad cifrada, siga uno de estos procedimientos:

- Añada su función a la lista de permitidos para la política AWS KMS clave
- Añada las siguientes instrucciones AWSBackupServiceRolePolicyForRestoresa su función de IAM para las restauraciones:
  - `KMSDescribePermissions`
  - `KMSPermissions`
  - `KMSCreateGrantPermissions`

Actualizaciones de políticas para AWS Backup

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas AWS Backup desde que este servicio comenzó a rastrear estos cambios.

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	AWS Backup permiso agregado `backup:TagResource` a esta política. El permiso es necesario para obtener permisos de etiquetado durante la creación de un punto de recuperación.	17 de mayo de 2024
AWSBackupServiceRolePolicyForS3Backup: actualización de una política actual	AWS Backup permiso añadido `backup:TagResource` a esta política. El permiso es necesario para obtener permisos de etiquetado durante la creación de un punto de recuperación.	17 de mayo de 2024
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	AWS Backup permiso añadido `backup:TagResource` a esta política. El permiso es necesario para obtener permisos de etiquetado durante la creación de un punto de recuperación.	17 de mayo de 2024
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregó el permiso. `rds:DeleteDBInstanceAutomatedBackups`	1 de mayo de 2024

Cambio	Descripción	Fecha
	Este permiso es necesario AWS Backup para admitir copias de seguridad continuas y point-in-time-restore de instancias de Amazon RDS.	
AWSBackupFullAccess: actualización de una política actual	AWS Backup actualizó el nombre de recurso de Amazon (ARN) con el permiso `storagegateway:ListVolumes` de `arn:aws:storagegateway:*:*:gateway/*` a para adaptarse a un cambio * en el modelo de API de Storage Gateway.	1 de mayo de 2024
AWSBackupOperatorAccess: actualización de una política actual	AWS Backup actualizó el nombre de recurso de Amazon (ARN) con el permiso `storagegateway:ListVolumes` de `arn:aws:storagegateway:*:*:gateway/*` a para adaptarse a un cambio * en el modelo de API de Storage Gateway.	1 de mayo de 2024

Cambio	Descripción	Fecha
AWSServiceRolePolicyForBackupRestoreTesting: actualización de una política actual	Se agregaron los siguientes permisos para describir y enumerar los puntos de recuperación y los recursos protegidos a fin de llevar a cabo los planes de pruebas de restauración: `backup:DescribeRecoveryPoint` `backup:DescribeProtectedResource` ,`backup:ListProtectedResources` , y`backup:ListRecoveryPointsByResource` . Se agregó el permiso `ec2:DescribeSnapshotTierStatus` para admitir el almacenamiento en niveles de archivo de Amazon EBS. Se agregó el permiso `rds:DescribeDBClusterAutomatedBackups` para admitir las copias de seguridad continuas de Amazon Aurora. Se agregaron los siguientes permisos para admitir las pruebas de restauración de las copias de seguridad de Amazon Redshift: `redshift:`	14 de febrero de 2024

Cambio	Descripción	Fecha
	`DescribeClusters` y. `redshift:DeleteCluster` Se agregó el permiso `timestream:DeleteTable` para admitir las pruebas de restauración de las copias de seguridad de Amazon Timestream.	
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron los permisos `ec2:DescribeSnapshotTierStatus` y`ec2:RestoreSnapshotTier` . Estos permisos son necesarios para que los usuarios tengan la opción de restaurar los recursos de Amazon EBS almacenados AWS Backup desde el almacenamiento de archivos. En el caso de las restauraciones de instancias EC2, también debe incluir los permisos que se muestran en la siguiente declaración de política para lanzar la instancia EC2:	27 de noviembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregaron los permisos `ec2:DescribeSnapshotTierStatus` y `ec2:ModifySnapshotTier` se admitió una opción de almacenamiento adicional para que los recursos de Amazon EBS respaldados se transfieran al nivel de almacenamiento de archivos. Estos permisos son necesarios para que los usuarios tengan la opción de realizar la transición de los recursos de Amazon EBS almacenados AWS Backup al almacenamiento de archivos.	27 de noviembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregaron los permisos `ec2:DescribeSnapshotTierStatus` y `ec2:ModifySnapshotTier` se admitió una opción de almacenamiento adicional para que los recursos de Amazon EBS respaldados se transfieran al nivel de almacenamiento de archivos. Estos permisos son necesarios para que los usuarios tengan la opción de realizar la transición de los recursos de Amazon EBS almacenados AWS Backup al almacenamiento de archivos. Se agregaron los permisos `rds:DescribeDBClusterSnapshots` `yrds:RestoreDBClusterToPointInTime` , que son necesarios para la PITR (point-in-time restauraciones) de los clústeres de Aurora.	

Cambio	Descripción	Fecha
AWSServiceRolePolicyForBackupRestoreTesting: política nueva	Proporciona los permisos necesarios para realizar las pruebas de restauración. Los permisos incluyen las acciones `list, read, and write` para que los siguientes servicios se incluyan en pruebas de restauración: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx para Lustre, FSx para Windows File Server, FSx para ONTAP, FSx para OpenZFS, Amazon Neptune, Amazon RDS y Amazon S3.	27 de noviembre de 2023
AWSBackupFullAccess: actualización de una política actual	Se ha añadido `restore-testing.backup.amazonaws.com` a `IamPassRolePermissions` y `IamCreateServiceLinkedRolePermissions` . Esta adición es necesaria AWS Backup para realizar las pruebas de restauración en nombre de los clientes.	27 de noviembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron los permisos `rds:DescribeDBClusterSnapshots` `yrds:RestoreDBClusterToPointInTime` , que son necesarios para la PITR (point-in-time restauraciones) de los clústeres de Aurora.	6 de septiembre de 2023
AWSBackupFullAccess: actualización de una política actual	Se agregó el permiso`rds:DescribeDBClusterAutomatedBackups` , que es necesario para realizar copias de seguridad y point-in-time restauración continuas de los clústeres de Aurora.	6 de septiembre de 2023
AWSBackupOperatorAccess: actualización de una política actual	Se agregó el permiso`rds:DescribeDBClusterAutomatedBackups` , que es necesario para realizar copias de seguridad y point-in-time restauración continuas de los clústeres de Aurora.	6 de septiembre de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregó el permisords:DescribeDBClusterAutomatedBackups . Este permiso es necesario para AWS Backup admitir la copia de seguridad y la point-in-time restauración continuas de los clústeres de Aurora. Se agregó el permiso rds:DeleteDBClusterAutomatedBackups para permitir que el AWS Backup ciclo de vida elimine y desasocie los puntos de recuperación continua de Amazon Aurora cuando finalice un período de retención. Este permiso es necesario para que el punto de recuperación de Aurora evite la transición a un estado EXIPIRED. Se agregó el permiso rds:ModifyDBCluster que AWS Backup permite interactuar con los clústeres de Aurora. Esta adición permite a los usuarios habilitar o deshabilitar las copias de seguridad continuas en función de las configuraciones deseadas.	6 de septiembre de 2023

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Se agregó la acción `ram:GetResourceShareAssociations` para conceder al usuario permiso para obtener asociaciones de recursos compartidos para un nuevo tipo de almacén.	8 de agosto de 2023
AWSBackupOperatorAccess: actualización de una política actual	Se ha añadido la acción `ram:GetResourceShareAssociations` para conceder al usuario permiso para obtener asociaciones de recursos compartidos para un nuevo tipo de almacén.	8 de agosto de 2023
AWSBackupServiceRolePolicyForS3Backup: actualización de una política actual	Se agregó el permiso `s3:PutInventoryConfiguration` para mejorar las velocidades de rendimiento de las copias de seguridad mediante el uso de un inventario por lotes.	1 de agosto de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron las siguientes acciones para conceder al usuario permisos para agregar etiquetas y restaurar los recursos: `storagegateway:AddTagsToResource elasticfilesystem:TagResource` ,, solo `ec2:CreateTags` para aquellos `ec2:CreateAction` que incluyen una `RunInstances` o `CreateVolume fsx:TagResource` , `ycloudformation:TagResource` .	22 de mayo de 2023
AWSBackupAuditAccess: actualización de una política actual	Se reemplazó la selección de recursos de la API `config:DescribeComplianceByConfigRule` por un recurso comodín para facilitar a los usuarios la selección de los recursos.	11 de abril de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregó el siguiente permiso para restaurar Amazon EFS mediante una clave administrada por el cliente:`kms:GenerateDataKeyWithoutPlaintext` . Esto ayuda a garantizar que los usuarios tengan los permisos necesarios para restaurar los recursos de Amazon EFS.	27 de marzo de 2023
AWSServiceRolePolicyForBackupReports: actualización de una política actual	Se actualizaron las `config:DescribeConfigRuleEvaluationStatus` acciones `config:DescribeConfigRules` y para permitir que AWS Backup Audit Manager acceda a las reglas administradas por AWS Backup Audit Manager AWS Config .	9 de marzo de 2023

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForS3Restore: actualización de una política actual	Se agregaron los siguientes permisos: `kms:Decrypt` `s3:PutBucketOwnershipControls` , y `s3:GetBucketOwnershipControls` a la política. `AWSBackupServiceRolePolicyForS3Restore` Estos permisos son necesarios para permitir la restauración de objetos cuando se utiliza el cifrado de KMS en la copia de seguridad original y para restaurar objetos cuando la propiedad del objeto está configurada en el bucket original en lugar de en la ACL.	13 de febrero de 2023

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Se agregaron los siguientes permisos para programar copias de seguridad mediante etiquetas VMware de máquinas virtuales y para admitir la limitación del ancho de banda basada en la programación:`backup-gateway:GetHypervisorPropertyMappings` ,,`backup-gateway:GetVirtualMachine` , `backup-gateway:PutHypervisorPropertyMappings` `backup-gateway:GetHypervisor` , `backup-gateway:StartVirtualMachinesMetadataSync` y. `backup-gateway:GetBandwidthRateLimitSchedule` `backup-gateway:PutBandwidthRateLimitSchedule`	15 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	Se agregaron los siguiente s permisos para programar copias de seguridad mediante etiquetas VMware de máquinas virtuales y para admitir la limitación del ancho de banda basada en la programación:,, y. `backup-gateway:GetHyperviso rPropertyMappings` `backup-gateway:Get VirtualMachine` `backup-gateway:Get Hypervisor` `backup-ga teway:GetBandwidth RateLimitSchedule`	15 de diciembre de 2022
AWSBackupGatewaySe rviceRolePolicyForVirtualMa chineMetadataSync: política nueva	Proporciona permisos para que AWS Backup Gateway sincronice los metadatos de las máquinas virtuales de las redes locales con Backup Gateway.	15 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de respaldo de Timestrea m:`timestream:StartAwsBackupJob` ,`timestream:GetAwsBackupStatus` ,`timestream:ListTables` ,`timestream:ListDatabases` , `timestream:ListTagsForResource` `timestream:DescribeTable` , `timestream:DescribeDatabase` y. `timestream:DescribeEndpoints`	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de restauración de Timestrea m:`timestream:StartAwsRestoreJob` ,`timestrea m:GetAwsRestoreStatus` ,`timestrea m:ListTables` ,`timestrea m:ListTagsForResource` , `timestream:ListDatabases` `timestrea m:DescribeTable` , `timestream:DescribeDatabase` y. `s3:GetBucketAcl` `timestrea m:DescribeEndpoints`	13 de diciembre de 2022
AWSBackupFullAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Timestrea m:`timestream:ListTables` ,, y. `timestrea m:ListDatabases` `s3:ListAllMyBuckets` `timestream:DescribeEndpoints`	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Timestream: `timestream:ListDatabases`, `timestream:ListTables`. `s3:ListAllMyBuckets` `timestream:DescribeEndpoints`	13 de diciembre de 2022
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Timestream: `timestream:ListDatabases`, `timestream:ListTables`, `timestream:ListTagsForResource`, `timestream:DescribeDatabase` `timestream:DescribeTable`, `timestream:GetAwsBackupStatus` y `timestream:GetAwsRestoreStatus` `timestream:DescribeEndpoints`	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Amazon Redshift: `redshift:DescribeClusters redshift:DescribeClusterSubnetGroups ,redshift:DescribeNodeConfigurationOptions ,redshift:DescribeOrderableClusterOptions ,, redshift:DescribeClusterParameterGroups redshift:DescribeClusterTracks redshift:DescribeSnapshotSchedules` , y. `ec2:DescribeAddresses`	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir los recursos de Amazon Redshift: `redshift:DescribeClusters` ,`redshift:DescribeClusterSubnetGroups` ,, `redshift:DescribeNodeConfigurationOptions` `redshift:DescribeOrderableClusterOptions` ,`redshift:DescribeClusterParameterGroups`, . `redshift:DescribeClusterTracks` `redshift:DescribeSnapshotSchedules` , y. `ec2:DescribeAddresses`	27 de noviembre de 2022
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de restauración de Amazon Redshift: `redshift:RestoreFromCluster` `Snapshot` , `redshift:RestoreTableFromClusterSnapshot` `redshift:DescribeClusters` , y. `redshift:DescribeTableRestoreStatus`	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de copia de seguridad de Amazon Redshift: `redshift:CreateClusterSnapshot` `redshift:DescribeClusterSnapshots` ,`redshift:DescribeTags` , `redshift:DeleteClusterSnapshot` `redshift:DescribeClusters` , y. `redshift:CreateTags`	27 de noviembre de 2022
AWSBackupFullAccess: actualización de una política actual	Se agregó el siguiente permiso para respaldar CloudFormation los recursos: `cloudformation:ListStacks` .	27 de noviembre de 2022
AWSBackupOperatorAccess: actualización de una política actual	Se agregó el siguiente permiso para respaldar CloudFormation los recursos: `cloudformation:ListStacks` .	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregaron los siguientes permisos para respaldar CloudFormation los recursos: `redshift:DescribeClusterSnapshots redshift:DescribeTags ,redshift:DeleteClusterSnapshot , yredshift:DescribeClusters .`	27 de noviembre de 2022
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de respaldo de la pila de AWS CloudFormation aplicaciones: `cloudformation:GetTemplate cloudformation:DescribeStacks , ycloudformation:ListStackResources .`	16 de noviembre de 2022
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron los siguientes permisos para admitir los trabajos de respaldo de la pila de AWS CloudFormation aplicaciones: `cloudformation:CreateChangeSet y cloudformation:DescribeChangeSet`	16 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupOrganizationAdminAccess: actualización de una política actual	Se agregaron los siguientes permisos a esta política para permitir a los administradores de la organización utilizar la función de administrador delegado:`organizations:ListDelegatedAdministrator` , y `organizations:RegisterDelegatedAdministrator` `organizations:DeregisterDelegatedAdministrator`	27 de noviembre de 2022
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregaron los siguientes permisos para admitir SAP HANA en instancias de Amazon EC2:`ssm-sap:GetOperation` ,`ssm-sap:ListDatabases` , `ssm-sap:BackupDatabase` `ssm-sap:UpdateHanaBackupSettings` `ssm-sap:GetDatabase` , y. `ssm-sap:ListTagsForResource`	20 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir SAP HANA en instancias de Amazon EC2:`ssm-sap:GetOperation` , `ssm-sap:ListDatabases` `ssm-sap:GetDatabase` , y. `ssm-sap:ListTagsForResource`	20 de noviembre de 2022
AWSBackupOperatorAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir SAP HANA en instancias de Amazon EC2:`ssm-sap:GetOperation` , `ssm-sap:ListDatabases` `ssm-sap:GetDatabase` , y. `ssm-sap:ListTagsForResource`	20 de noviembre de 2022
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregó el siguiente permiso para admitir SAP HANA en instancias de Amazon EC2:. `ssm-sap:GetOperation`	20 de noviembre de 2022
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregó el siguiente permiso para admitir los trabajos de restauración de Backup Gateway en una instancia EC2:`ec2:CreateTags` .	20 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupDataTransferAccess: actualización de una política actual	Se agregaron los siguientes permisos para admitir la transferencia segura de datos de almacenamiento para los recursos de SAP HANA On Amazon EC2: `backup-storage:StartObject backup-storage:PutChunk ,backup-storage:GetChunk ,backup-storage:ListChunks , backup-storage:ListObjects backup-storage:GetObjectMetadata , y. backup-storage:NotifyObjectComplete`	20 de noviembre de 2022

Cambio	Descripción	Fecha
AWSBackupRestoreAccessForSAPHANA: actualización de una política actual	Se agregaron los siguientes permisos para que los propietarios de los recursos realicen la restauración de los recursos de SAP HANA en 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` , y. `ssm-sap:ListTagsForResource`	20 de noviembre de 2022
AWSBackupServiceRolePolicyForS3Backup: actualización de una política actual	Se agregó el permiso `s3:GetBucketAcl` para admitir las operaciones de respaldo AWS Backup de Amazon S3.	24 de agosto de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron las siguientes acciones para conceder acceso a la creación de una instancia de base de datos que admita la funcionalidad de zonas de disponibilidad múltiple (Multi-AZ):. `rds:CreateDBInstance`	20 de julio de 2022
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregó el `s3:GetBucketTagging` permiso para conceder al usuario permiso para seleccionar los buckets de los que realizar copias de seguridad con un comodín de recursos. Sin este permiso, los usuarios que seleccionen los depósitos de los que se va a hacer una copia de seguridad con un comodín de recursos no tendrán éxito.	6 de mayo de 2022
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregaron recursos de volumen en el ámbito de `fsx:ListTagsForResource` las acciones existentes `fsx:CreateBackup` y se agregaron nuevas acciones `fsx:DescribeVolumes` para admitir FSx para las copias de seguridad a nivel de volumen de ONTAP.	27 de abril de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregaron las siguientes acciones para conceder a los usuarios permisos para restaurar FSx para los volúmenes ONTAP`fsx:DescribeVolumes` ,`fsx:CreateVolumeFromBackup` , `fsx:DeleteVolume` y. `fsx:UntagResource`	27 de abril de 2022
AWSBackupServiceRolePolicyForS3Backup: actualización de una política actual	Se agregaron las siguientes acciones para conceder al usuario permisos para recibir notificaciones de cambios en sus buckets de Amazon S3 durante las operaciones de respaldo: `s3:GetBucketNotification` y`s3:PutBucketNotification` .	25 de febrero de 2022

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForS3Backup: política nueva	Se agregaron las siguientes acciones para conceder al usuario permisos para hacer copias de seguridad de sus buckets de Amazon S3: `s3:GetInventoryConfiguration` `s3:PutInventoryConfiguration` ,`s3:ListBucketVersions` ,`s3:ListBucket` ,`s3:GetBucketTagging` ,`s3:GetBucketVersioning` ,, `s3:GetBucketNotification` `s3:GetBucketLocation` , y `s3:ListAllMyBuckets` Se agregaron las siguientes acciones para conceder al usuario permisos para hacer copias de seguridad de sus objetos de Amazon S3: `s3:GetObject` `s3GetObjectAcl` `s3:GetObjectVersionTagging` `s3:GetObjectVersionAcl` ,,`s3:GetObjectTagging` , y`s3:GetObjectVersion` . Se agregaron las siguientes acciones para conceder al usuario permisos para hacer	17 de febrero de 2022

Cambio	Descripción	Fecha
	copias de seguridad de sus datos cifrados de Amazon S3: `kms:Decrypt ykms:DescribeKey` . Se agregaron las siguientes acciones para conceder al usuario permisos para realizar copias de seguridad incrementales de sus datos de Amazon S3 utilizando EventBridge las reglas de Amazon: `events:DescribeRule events:EnableRule events:PutRule events:DeleteRule events:PutTargets ,events:RemoveTargets ,events:ListTargetsByRule ,events:DisableRule ,,cloudwatch:GetMetricData , yevents:ListRules` .	

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForS3Restore: política nueva	Se agregaron las siguientes acciones para conceder al usuario permisos para restaurar sus buckets de Amazon S3: `s3:CreateBucket s3:ListBucketVersions ,,s3:ListBucket , s3:GetBucketVersioning s3:GetBucketLocation , ys3:PutBucketVersioning .` Se agregaron las siguientes acciones para conceder al usuario permisos para restaurar sus buckets de Amazon S3: `s3:GetObject s3:GetObjectVersion s3:DeleteObject ,s3:PutObjectVersionAcl ,s3:GetObjectVersionAcl ,s3:GetObjectTagging ,s3:PutObjectTagging ,s3:GetObjectAcl , s3:PutObjectAcl s3:PutObject , ys3:ListMultipartUploadParts .` Se agregaron las siguientes acciones para conceder	17 de febrero de 2022

Cambio	Descripción	Fecha
	al usuario permisos para cifrar los datos restaurados de Amazon S3: `kms:Decrypt kms:DescribeKey` , `ykms:GenerateDataKey` .	
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregó `s3:ListAllMyBuckets` para conceder al usuario permisos para ver una lista de sus depósitos y elegir cuáles asignar a un plan de respaldo.	14 de febrero de 2022
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregó `backup-gateway:ListVirtualMachines` para conceder al usuario permisos para ver una lista de sus máquinas virtuales y elegir cuáles asignar a un plan de respaldo. Se agregó `backup-gateway:ListTagsForResource` para conceder al usuario permisos para enumerar las etiquetas de sus máquinas virtuales.	30 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregó `backup-gateway:Backup` para conceder al usuario permisos para restaurar las copias de seguridad de sus máquinas virtuales. AWS Backup también se agregó `backup-gateway:ListTagsForResource` para conceder al usuario permisos para enumerar las etiquetas asignadas a las copias de seguridad de sus máquinas virtuales.	30 de noviembre de 2021
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se agregó `backup-gateway:Restore` para conceder al usuario permisos para restaurar las copias de seguridad de sus máquinas virtuales.	30 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Se agregaron las siguientes acciones para conceder a los usuarios permisos para usar AWS Backup Gateway para realizar copias de seguridad , restaurar y administrar sus máquinas virtuales: 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-ga	30 de noviembre de 2021

Cambio	Descripción	Fecha
	`teway:UntagResourc e` ,`backup-gateway:Upd ateGatewayInformat ion` , y`backup-ga teway:UpdateHyperv isor` .	
AWSBackupOperatorAccess: actualización de una política actual	Se agregaron las siguiente s acciones para conceder al usuario permisos para hacer copias de seguridad de sus máquinas virtuales: `backup-gateway:ListGateways` `backup-gateway:Lis tHypervisors` ,`backup-gateway:ListTagsForR esource` , y`backup-ga teway:ListVirtualM achines` .	30 de noviembre de 2021
AWSBackupServiceLi nkedRolePolicyForBackup: actualización de una política actual	Se agregó `dynamodb: ListTagsOfResource` para conceder al usuario permisos para enumerar las etiquetas de sus tablas de DynamoDB para realizar copias de seguridad mediante las funciones avanzadas de copia AWS Backup de seguridad de DynamoDB.	23 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregó `dynamodb:StartAwsBackupJob` para conceder al usuario permisos para hacer copias de seguridad de sus tablas de DynamoDB mediante funciones de copia de seguridad avanzadas. Se agregó `dynamodb:ListTagsOfResource` para conceder al usuario permisos para copiar etiquetas de sus tablas de DynamoDB de origen a sus copias de seguridad.	23 de noviembre de 2021
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se ha añadido `dynamodb:RestoreTableFromAwsBackup` para conceder permisos al usuario para restaurar las tablas de DynamoDB de las que se ha hecho una copia de seguridad mediante las funciones avanzadas AWS Backup de copia de seguridad de DynamoDB.	23 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se ha añadido `dynamodb:RestoreTableFromAwsBackup` para conceder permisos al usuario para restaurar las tablas de DynamoDB de las que se ha hecho una copia de seguridad mediante las funciones avanzadas AWS Backup de copia de seguridad de DynamoDB.	23 de noviembre de 2021
AWSBackupOperatorAccess: actualización de una política actual	Se eliminaron las acciones `rds:DescribeDBSnapshots` porque eran `backup:GetRecoveryPointRestoreMetadata` redundantes. AWS Backup no necesitaba ambas `backup:GetRecoveryPointRestoreMetadata` y `backup:Get*` como parte de`AWSBackupOperatorAccess` . Además, AWS Backup no necesitaba ambos `rds:DescribeDBSnapshots` y `rds:describeDBSnapshots` como parte de`AWSBackupOperatorAccess` .	23 de noviembre de 2021

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregaron las nuevas acciones `elasticfilesystem:DescribeFileSystems` `dynamodb:ListTables` ,`storagegateway:ListVolumes` ,`ec2:DescribeVolumes` , `ec2:DescribeInstances` `rds:DescribeDBInstances` `rds:DescribeDBClusters` , y `fsx:DescribeFileSystems` para permitir a los clientes ver y elegir de una lista de los recursos AWS Backup compatibles a la hora de seleccionar qué recursos asignar a un plan de respaldo.	10 de noviembre de 2021
AWSBackupAuditAccess: política nueva	Se agregó `AWSBackupAuditAccess` para conceder al usuario permisos para usar AWS Backup Audit Manager. Los permisos incluyen la capacidad de configurar marcos de conformidad y generar informes.	24 de agosto de 2021

Cambio	Descripción	Fecha
AWSServiceRolePolicyForBackupReports: política nueva	Se ha añadido `AWSServiceRolePolicyForBackupReports` para conceder permisos a una función vinculada a un servicio con el fin de automatizar la supervisión de la configuración, las tareas y los recursos de la copia de seguridad para garantizar el cumplimiento de los marcos configurados por el usuario.	24 de agosto de 2021
AWSBackupFullAccess: actualización de una política actual	Se ha añadido `iam:CreateServiceLinkedRole` para crear una función vinculada al servicio (haciendo todo lo posible) para automatizar la eliminación de los puntos de recuperación caducados. Sin esta función vinculada al servicio, AWS Backup no se pueden eliminar los puntos de recuperación caducados después de que los clientes eliminen la función de IAM original que utilizaron para crear sus puntos de recuperación.	5 de julio de 2021

Cambio	Descripción	Fecha
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregó la nueva acción `dynamodb:DeleteBackup` para conceder `DeleteRecoveryPoint` permiso para automatizar la eliminación de puntos de recuperación de DynamoDB vencidos en función de la configuración del ciclo de vida de su plan de respaldo.	5 de julio de 2021
AWSBackupOperatorAccess: actualización de una política actual	Se eliminaron las acciones `backup:GetRecoveryPointRestoreMetadata` `rds:DescribeDBSnapshots` porque eran redundantes. AWS Backup no necesitaba ambas `backup:GetRecoveryPointRestoreMetadata` y `backup:Get*` como parte de `AWSBackupOperatorAccess` Además, AWS Backup no necesitaba ambas `rds:DescribeDBSnapshots` y `rds:describeDBSnapshots` como parte de `AWSBackupOperatorAccess`	25 de mayo de 2021

Cambio	Descripción	Fecha
AWSBackupOperatorAccess: actualización de una política actual	Eliminó las acciones `backup:GetRecoveryPointRestoreMetadata` y `rds:DescribeDBSnapshots` porque eran redundantes. AWS Backup no necesitaba ambas `backup:GetRecoveryPointRestoreMetadata` y `backup:Get*` como parte de `AWSBackupOperatorAccess`. Además, AWS Backup no necesitaba ambos `rds:DescribeDBSnapshots` y `rds:describeDBSnapshots` como parte de `AWSBackupOperatorAccess`.	25 de mayo de 2021
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se ha añadido la nueva acción `fsx:TagResource` para conceder `StartRestoreJob` permiso para aplicar etiquetas a los sistemas de archivos Amazon FSx durante el proceso de restauración.	24 de mayo de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForRestores: actualización de una política actual	Se han añadido las nuevas acciones `ec2:DescribeImages` y `ec2:DescribeInstances` se ha concedido un `StartRestoreJob` permiso que le permita restaurar las instancias de Amazon EC2 desde los puntos de recuperación.	24 de mayo de 2021
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se agregó la nueva acción `fsx:CopyBackup` para conceder `StartCopyJob` permiso que le permita copiar los puntos de recuperación de Amazon FSx en todas las regiones y cuentas.	12 de abril de 2021
AWSBackupServiceLinkedRolePolicyForBackup: actualización de una política actual	Se agregó la nueva acción `fsx:CopyBackup` para conceder `StartCopyJob` permiso que le permita copiar los puntos de recuperación de Amazon FSx en todas las regiones y cuentas.	12 de abril de 2021

Cambio	Descripción	Fecha
AWSBackupServiceRolePolicyForBackup: actualización de una política actual	Se actualizó para cumplir con el siguiente requisito: AWS Backup Para crear una copia de seguridad de una tabla de DynamoDB cifrada, debe añadir los `kms:Decrypt` permisos `kms:GenerateDataKey` y la función de IAM utilizada para la copia de seguridad.	10 de marzo de 2021

Cambio	Descripción	Fecha
AWSBackupFullAccess: actualización de una política actual	Actualizado para cumplir con los siguientes requisitos: AWS Backup Para configurar copias de seguridad continuas para su base de datos de Amazon RDS, compruebe que el permiso de API `rds:ModifyDBInstance` existe en la función de IAM definida en la configuración de su plan de backup. Para restaurar las copias de seguridad continuas de Amazon RDS, debe agregar el permiso `rds:RestoreDBInstanceToPointInTime` al rol de IAM que envió para el trabajo de restauración. En la AWS Backup consola, para describir el intervalo de tiempo disponible para la point-in-time recuperación, debe incluir el permiso de la `rds:DescribeDBInstanceAutomatedBackups` API en la política gestionada por IAM.	10 de marzo de 2021

Cambio	Descripción	Fecha
AWS Backup comenzó a rastrear los cambios	AWS Backup comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	10 de marzo de 2021

Uso de roles vinculados a servicios de AWS Backup

AWS Backup usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Temas

- Uso de roles para realizar copias de seguridad y copiar
- Uso de funciones para AWS Backup Audit Manager
- Uso de roles para pruebas de restauración

Uso de roles para realizar copias de seguridad y copiar

AWS Backup usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Backup , ya que no es necesario añadir manualmente los permisos necesarios. AWS Backup define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Backup puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege sus AWS Backup recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para AWS Backup

AWS Backup utiliza el rol vinculado al servicio denominado AWSServiceRoleForBackup: proporciona AWS Backup permisos para enumerar los recursos de los que puede hacer copias de seguridad y para copiar copias de seguridad.

AWS Backup también utiliza la función para eliminar todas las copias de seguridad de todos los tipos de recursos, excepto Amazon EC2.

El rol AWSServiceRoleForBackup vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `backup.amazonaws.com`

Para ver los permisos de esta política, consulte la Referencia AWSBackupServiceLinkedRolePolicyforBackupde políticas AWS administradas.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS Backup

No necesita crear manualmente un rol vinculado a servicios. Al enumerar los recursos de los que hacer copias de seguridad, configurar copias de seguridad entre cuentas o realizar copias de seguridad en la AWS Management Console AWS CLI, la API o la AWS API, se AWS Backup crea automáticamente la función vinculada al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando pones en una lista los recursos que deseas guardar, configuras una copia de seguridad multicuenta o realizas copias de seguridad, vuelve a AWS Backup crear el rol vinculado al servicio para ti.

Modificación de un rol vinculado a servicios de AWS Backup

AWS Backup no permite editar el rol vinculado al AWSServiceRoleForBackup servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio de AWS Backup

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. En primer lugar, debe eliminar todos los puntos de recuperación. Luego, debe eliminar todos sus almacenes de copias de seguridad.

> **Note**
>
> Si el AWS Backup servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar AWS Backup los recursos utilizados por la AWSServiceRoleForBackup (consola)

1. Para eliminar todos los puntos de recuperación y los almacenes de copias de seguridad (excepto el almacén predeterminado), siga el procedimiento que se describe en Eliminación de un almacén de copias de seguridad.
2. Para eliminar el almacén predeterminado, utilice el siguiente comando en la AWS CLI:

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

Para eliminar AWS Backup los recursos utilizados por AWSServiceRoleForBackup (AWS CLI)

1. Para eliminar todos tus puntos de recuperación, usa delete-recovery-point.
2. Para eliminar todos los almacenes de copias de seguridad, utilice `delete-backup-vault`.

Para eliminar AWS Backup los recursos utilizados por la AWSServiceRoleForBackup (API)

1. Para eliminar todos los puntos de recuperación, utilice `DeleteRecoveryPoint`.
2. Para eliminar todos los almacenes de copias de seguridad, utilice `DeleteBackupVault`.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForBackup servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Backup

AWS Backup admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y características compatibles con AWS Backup.

Uso de funciones para AWS Backup Audit Manager

AWS Backup usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Backup , ya que no es necesario añadir manualmente los permisos necesarios. AWS Backup define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Backup puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege sus AWS Backup recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para AWS Backup

AWS Backup utiliza el rol vinculado al servicio denominado AWSServiceRoleForBackupReports: AWS Backup proporciona permiso para crear controles, marcos e informes.

El rol AWSServiceRoleForBackupReports vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `backup.amazonaws.com`

Para ver los permisos de esta política, consulte la Referencia AWSServiceRolePolicyForBackupReportsde políticas AWS administradas.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS Backup

No necesita crear manualmente un rol vinculado a servicios. Al crear un marco o un plan de informes en la AWS Management Console, la AWS CLI API o la AWS API, se AWS Backup crea automáticamente la función vinculada al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear un marco o un plan de informes, vuelve a AWS Backup crear el rol vinculado al servicio automáticamente.

Modificación de un rol vinculado a servicios de AWS Backup

AWS Backup no permite editar el rol vinculado al AWSServiceRoleForBackupReports servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio de AWS Backup

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. Debe eliminar todos los marcos y los planes de informes.

> **Note**
>
> Si el AWS Backup servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar AWS Backup los recursos utilizados por la AWSServiceRoleForBackupReports (consola)

1. Para eliminar todos los marcos, consulte Eliminación de marcos.
2. Para eliminar todos los planes de informes, consulte Eliminación de los planes de informes.

Para eliminar AWS Backup los recursos utilizados por AWSServiceRoleForBackupReports (AWS CLI)

1. Para eliminar todos los marcos, utilice delete-framework.
2. Para eliminar todos los planes de informes, utilice delete-report-plan.

Para eliminar AWS Backup los recursos utilizados por la AWSServiceRoleForBackupReports (API)

1. Para eliminar todos los marcos, utilice DeleteFramework.
2. Para eliminar todos los planes de informes, utilice DeleteReportPlan.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForBackupReports servicio. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Backup

AWS Backup admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y características compatibles con AWS Backup.

Uso de roles para pruebas de restauración

AWS Backup usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Backup Los roles vinculados al servicio están predefinidos AWS Backup e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Backup , ya que no es necesario añadir manualmente los permisos necesarios. AWS Backup define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Backup puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege sus AWS Backup recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para AWS Backup

AWS Backup utiliza el rol vinculado al servicio denominado AWSServiceRolePolicyForBackupRestoreTesting: proporciona permisos de respaldo para realizar pruebas de restauración.

El rol AWSServiceRolePolicyForBackupRestoreTesting vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `backup.amazonaws.com`

Para ver los permisos de esta política, consulte la Referencia AWSServiceRolePolicyForBackupRestoreTestingde políticas AWS administradas.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS Backup

No necesita crear manualmente un rol vinculado a servicios. Cuando realizas pruebas de restauración en la AWS Management Console AWS CLI, la API o la AWS API, se AWS Backup crea automáticamente la función vinculada al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando realizas las pruebas de restauración, vuelve a AWS Backup crear el rol vinculado al servicio para ti.

Modificación de un rol vinculado a servicios de AWS Backup

AWS Backup no permite editar el rol vinculado al AWSServiceRolePolicyForBackupRestoreTesting servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio de AWS Backup

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. Debe eliminar todos los planes de prueba de restauración.

> **Note**
>
> Si el AWS Backup servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar AWS Backup los recursos utilizados por la AWSServiceRolePolicyForBackupRestoreTesting (consola)

- Para eliminar todos los planes de prueba de restauración, consulte Pruebas de restauración.

Para eliminar AWS Backup los recursos utilizados por AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI)

- Para eliminar planes de prueba de restauración, utilice `delete-restore-testing-plan`.

Para eliminar AWS Backup los recursos utilizados por la AWSServiceRolePolicyForBackupRestoreTesting (API)

- Para eliminar planes de prueba de restauración, utilice `DeleteRestoreTestingPlan`.

Eliminación manual de un rol vinculado a servicios

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRolePolicyForBackupRestoreTesting servicio. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Backup

AWS Backup admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y características compatibles con AWS Backup.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos para limitar los permisos que AWS Backup concede a otro servicio para el recurso. Si se utilizan ambas claves contextuales de condición global, el valor `aws:SourceAccount` y la cuenta del valor `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utilicen en la misma declaración de política.

El valor de `aws:SourceArn` debe ser un almacén de AWS Backup cuando se utiliza AWS Backup para publicar temas de Amazon SNS en su nombre.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce

el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws::servicename::123456789012:*`.

Seguridad de la infraestructura en AWS Backup

Como servicio gestionado, AWS Backup está protegido por la seguridad de la red AWS global. Para obtener más información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de la infraestructura en el marco de buena AWS arquitectura del pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Backup través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o una versión posterior. Los clientes también deben admitir conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Integridad de los datos en AWS Backup

AWS Backup objetivo de integridad de los datos

AWS Backup busca mantener la integridad durante la transmisión, el almacenamiento y el procesamiento de sus datos. AWS Backup trata los datos de los recursos almacenados como información crítica independiente del contenido, ya que ofrecemos el mismo alto nivel de seguridad a los clientes, independientemente del tipo de datos que almacenen. Velamos por la seguridad de nuestros clientes y hemos implementado sofisticadas medidas técnicas y físicas contra el acceso no autorizado. Usted mantiene un control total sobre la forma en que se clasifican sus datos, las regiones en las que se almacenan y la forma en que se controlan, archivan y protegen contra su divulgación.

AWS Backup implementación de la integridad de los datos

AWS Backup trabaja en conjunto con otros servicios AWS y con Amazon para mantener la integridad de los datos que almacena y con los que interactúa. Las herramientas utilizadas pueden variar e incluyen, entre otras:

- Validación continua de los objetos con respecto a su suma de verificación para evitar que los objetos se corrompan
- Sumas de verificación internas para confirmar la integridad de los datos en tránsito y en reposo
- Las sumas de verificación se calculan a partir de los datos de las copias de seguridad creadas desde el almacén principal
- Intento automático de restablecer los niveles normales de redundancia del almacenamiento de objetos en caso de que el disco esté dañado o se detecte un error en el dispositivo
- Almacenamiento redundante de datos en varias ubicaciones físicas
- Mejora de la durabilidad de los objetos en varias zonas de disponibilidad durante la escritura inicial, que se combina con una mayor replicación en caso de que el dispositivo no esté disponible o se detecte una degradación de bits
- Sumas de verificación de todo el tráfico de la red para detectar paquetes de datos con daños durante el almacenamiento o la recuperación de los datos

AWS Backup almacena datos de forma nativa para Amazon DynamoDB con funciones avanzadas, Amazon EFS, Amazon S3, Amazon Timestream y máquinas virtuales que se ejecutan con VMware conectadas a través de Backup Gateway. AWS Backup facilita las copias de seguridad de los datos almacenados con otros servicios, como Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon EBS, Amazon EC2, Amazon FSx para Windows File Server, Amazon FSx para Lustre, Amazon FSx para OpenZFS, Amazon FSx para ONTAP, Amazon Neptune Amazon Neptune, Amazon RDS y Amazon Redshift. NetApp

Confirmación objetiva y auditoría de la integridad de los datos en AWS Backup

Los datos almacenados directamente AWS Backup y los datos almacenados en asociación con otros AWS servicios con los que AWS Backup interactúa están sujetos al riguroso proceso de Amazon Simple Storage Service (Amazon S3) que sustenta la integridad de los datos. Un auditor externo independiente confirma esta integridad mediante un informe anual de auditoría de SOC, que está disponible en AWS Artifact en la AWS Management Console.

Obligaciones legales y AWS Backup

Una retención legal es una herramienta administrativa que ayuda a evitar que las copias de seguridad se eliminen mientras están retenidas. Mientras la retención esté en vigor, las copias de seguridad retenidas no se pueden eliminar y las políticas de ciclo de vida que podrían alterar el estado de las copias de seguridad (como la transición a un estado `Deleted`) se retrasan hasta que se elimine la retención legal. Una copia de seguridad puede tener más de una retención legal.

Las retenciones legales se pueden aplicar a una o más copias de seguridad (también conocidas como puntos de recuperación) creadas AWS Backup si sus ciclos de vida lo permiten. Un tipo de copia de seguridad denominado copia de seguridad continua tiene un ciclo de vida máximo de 35 días. Las retenciones legales no prolongan el ciclo de vida continuo de las copias de seguridad.

Cuando se crea una retención legal, esta puede incorporar criterios de filtrado específicos, como los tipos de recursos y los ID de los recursos. Además, puede definir el intervalo de fechas de creación de las copias de seguridad que desee incluir en una retención legal. Las retenciones legales y las copias de seguridad tienen una relación de muchos a muchos, lo que significa que una copia de seguridad puede tener más de una retención legal e incluir más de una copia de seguridad. Cada cuenta puede tener un máximo de 50 retenciones legales activas a la vez.

Las retenciones legales solo se aplican a la copia de seguridad original en la que se colocan. Cuando una copia de seguridad se copia entre regiones o cuentas (si el recurso lo admite), no se retiene ni lleva consigo su retención legal. Una retención legal, como otros recursos, tiene asociado un nombre de recurso de Amazon (ARN) único. Solo los puntos de recuperación creados por AWS Backup pueden formar parte de una retención legal.

Tenga en cuenta que, si bien el Bloqueo de almacenes de AWS Backup proporciona protecciones adicionales e inmutabilidad de un almacén, una retención legal ofrece adicional contra la eliminación de copias de seguridad individuales (puntos de recuperación). La retención legal no caduca y conserva los datos de la copia de seguridad de forma indefinida. La retención permanece activa hasta que un usuario con permisos suficientes la libere.

Creación de una retención legal

Cuando se crea una retención legal, solo contiene los puntos de recuperación que ya se hayan creado. Las copias de seguridad (puntos de recuperación) con un estado `DELETING` o `EXPIRED` no se incluirán en la retención legal. Es posible que los puntos de recuperación (copias de seguridad) con el estado `CREATING` no se incluyan en la retención legal, según el momento en que se completen.

Los usuarios que dispongan de los permisos de IAM necesarios pueden añadir suspensiones legales.

Creación de una retención legal mediante la consola de

Para crear una retención legal

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de la izquierda de la consola, busca Mi cuenta. Elija Retenciones legales.
3. Selecciona Añadir retención legal.
4. Se muestran tres paneles: detalles de la retención legal, alcance de la retención legal y etiquetas de retención legal.

    a. En Detalles de la retención legal, introduzca el título de la retención legal y una descripción de la misma en los cuadros de texto correspondientes.
    b. En el panel Ámbito de la retención legal, elija cómo desea seleccionar el recurso que va a incluir en la retención. Al crear una retención, se elige el método utilizado para seleccionar los recursos que se encuentran dentro de la retención legal. Puede elegir incluir una de las siguientes opciones:

        - Tipos e identificadores de recursos específicos
        - Seleccione bóvedas de respaldo
        - Todos los tipos de recursos o todas las bóvedas de respaldo de su cuenta

    c. Especifique el intervalo de fechas de la retención legal. Introduzca las fechas en el formato AAAA:MM:DD (las fechas son inclusivas).
    d. Si lo desea, puede añadir etiquetas para la retención en las etiquetas de retención legal. Las etiquetas pueden ayudar a categorizar el almacén para futura referencia y organización. Puede agregar hasta 50 etiquetas.
5. Cuando esté satisfecho con la configuración de la nueva retención legal, haga clic en el botón Agregar nueva retención.

Cree una retención legal mediante el AWS CLI

Puede crear una retención legal mediante el create-legal-holdcomando.

```
aws backup create-legal-hold --title "my title" \
    --description "my description" \
```

```
    --recovery-point-selection
 "VaultNames=string,DateRange={FromDate=timestamp,ToDate=timestamp}"
```

Visualización de las retenciones legales

Puede ver los detalles de la retención legal en la AWS Backup consola o mediante programación.

Consulta las retenciones legales desde la consola

Para ver todas las retenciones legales de una cuenta mediante la consola de Backup,

1. Abra la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En la parte izquierda del panel, en Mi cuenta, haga clic en Retenciones legales.
3. La tabla de retenciones legales muestra el título, el estado, la descripción, el identificador y la fecha de creación de las retenciones existentes. Haga clic en el quilate (flecha hacia abajo) situado junto al encabezado de la tabla para filtrar la tabla por la columna seleccionada.

Visualización de las retenciones legales mediante programación

Para ver todas las retenciones legales mediante programación, puedes usar las siguientes llamadas a la API: ListLegalHoldsy. GetLegalHold

Se puede utilizar la siguiente plantilla JSON para. `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
        }
   }
}
```

Se puede utilizar la siguiente plantilla JSON para`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,
  ]

}
```

Los valores de estado posibles son los siguientes.

Estado	Descripción
CREATING	Los puntos de recuperación solicitados están en proceso de retención, y las solicitudes de eliminación de esos puntos de recuperación podrían prosperar, ya que la retención no ha terminado de crearse.
ACTIVE	Se ha creado la retención legal. Se retienen todos los puntos de recuperación incluidos en esta retención legal.
CANCELLING	Las retenciones legales están en proceso de eliminación, y las solicitudes de eliminación de puntos de recuperación bajo retención podrían tener éxito.
CANCELADO	La retención legal se libera por completo y ya no surte efecto. Los puntos de recuperación se pueden eliminar.

Liberación de una retención legal

Las suspensiones legales permanecen en vigor hasta que un usuario con permisos suficientes las elimine. La eliminación de una retención legal también se conoce como cancelación, borrado o liberación de una retención legal. Al eliminar una retención legal, se elimina de todas las copias de seguridad a las que se asoció. Todas las copias de seguridad que hayan caducado durante la retención legal se eliminarán en un plazo de 24 horas tras la retirada de la retención legal.

Liberación de una retención legal mediante la consola de

Para liberar un agarre con la consola

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. Introduzca la descripción que le gustaría asociar a la liberación.
3. Revise los detalles y, a continuación, haga clic en Liberar retención.
4. Cuando aparezca el cuadro de diálogo Liberar retención, escriba `confirm` en el cuadro de texto para confirmar su intención de liberar la retención.

    - Marque la casilla que confirma que desea cancelar la retención.

En la página Retenciones legales puede ver todas sus retenciones. Si la liberación se ha realizado correctamente, el estado de esa retención se mostrará como `Released`.

Libera una suspensión legal mediante programación

Para eliminar una retención mediante programación, usa la llamada a la API. CancelLegalHold

Usa la siguiente plantilla JSON.

```
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 le permite establecer una conexión privada entre su nube privada virtual («VPC») y los AWS Backup puntos finales mediante la creación de un punto final de VPC de interfaz. Los puntos de enlace de la interfaz funcionan con una tecnología que le permite acceder de forma privada a AWS Backup las API al restringir todo el tráfico de red entre su VPC AWS Backup y la red de Amazon. AWS PrivateLink

AWS PrivateLink le permite acceder de forma privada a AWS Backup las operaciones sin una pasarela de Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con los puntos de enlace de la AWS Backup API. Las instancias tampoco necesitan direcciones IP públicas para usar ninguna de las operaciones de API AWS Backup y API de Backup Gateway disponibles. El tráfico entre tu VPC y AWS Backup no sale de la red de Amazon.

Para obtener más información sobre puntos de conexión de VPC, consulte Puntos de conexión de VPC de interfaz (AWS PrivateLink) en la Guía del usuario de Amazon VPC.

Consideraciones sobre los puntos de conexión de Amazon VPC

Antes de configurar un punto de enlace de VPC de interfaz para puntos de enlace, consulte las propiedades y limitaciones de AWS Backup los puntos de enlace de interfaz en la Guía del usuario de Amazon VPC.

Todas AWS Backup las operaciones relacionadas con la gestión de los recursos de Amazon Backup están disponibles en su VPC mediante. AWS PrivateLink

Las políticas de los puntos de conexión de VPC son compatibles con los puntos de conexión de Backup. De forma predeterminada, se permite el acceso completo a las operaciones de Backup a través del punto de conexión. Para más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

Creación de un punto final AWS Backup de VPC

Puede crear un punto de conexión de VPC para AWS Backup usar la consola de Amazon VPC o la (AWS Command Line Interface CLI).AWS Para obtener más información, consulte Creación de un punto de enlace de interfaz en la Guía del usuario de Amazon VPC.

Cree un punto final de VPC para AWS Backup usar el nombre del servicio. `com.amazonaws.region.backup`

En la región de China (Pekín) y la región de China (Ningxia), el nombre del servicio debe ser `cn.com.amazonaws.region.backup`.

Para los puntos de conexión de la puerta de enlace de copia de seguridad, utilice `com.amazonaws.region.backup-gateway`.

Los siguientes puertos TCP deben estar permitidos en el grupo de seguridad al crear un punto de conexión de VPC para la puerta de enlace de copia de seguridad:

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

Protocolo	Puerto	Dirección	Origen	Destino	Uso
TCP	443 (HTTPS)	Salida	Puerta de enlace de copia de seguridad	AWS	Para la comunicación entre Backup Gateway y el punto final del AWS servicio

Usar un punto de enlace de la VPC

Si habilitas el DNS privado para el punto final, puedes realizar solicitudes de API al AWS Backup punto final de la VPC utilizando su nombre de DNS predeterminado para la AWS región, por ejemplo. `backup.us-east-1.amazonaws.com`

Sin embargo, para la región de China (Pekín) y la región de China (Ningxia) Regiones de AWS, las solicitudes de API deben realizarse con el punto final de la VPC `backup.cn-north-1.amazonaws.com.cn` utilizando `backup.cn-northwest-1.amazonaws.com.cn` y, respectivamente.

Para obtener más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía del usuario de Amazon VPC.

Creación de una política de punto de conexión de VPC

Puede asociar una política de punto de conexión al punto de conexión de VPC que controla el acceso a la API de Amazon Backup. La política especifica:

- La entidad de seguridad que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

> **Important**
>
> Cuando se aplica una política no predeterminada a un punto final AWS Backup de la VPC de la interfaz, es posible que determinadas solicitudes de API con errores, como las que no lleganRequestLimitExceeded, no se registren en Amazon AWS CloudTrail . CloudWatch

Para más información, consulte Control del acceso a los servicios con puntos de enlace de la VPC en la Guía del usuario de Amazon VPC.

Ejemplo: política de puntos finales de VPC para acciones AWS Backup

El siguiente es un ejemplo de una política de puntos finales para AWS Backup. Cuando se adjunta a un punto final, esta política otorga acceso a las AWS Backup acciones enumeradas para todos los principios de todos los recursos.

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
```

```
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

Ejemplo: Política de punto de conexión de VPC que deniega todo el acceso desde una cuenta de AWS especificada

La siguiente política de punto final de VPC deniega a la AWS cuenta `123456789012` todo acceso a los recursos que utilizan el punto final. La política permite todas las acciones de otras cuentas.

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

Para obtener más información sobre las respuestas de API disponibles, consulte la Guía de API.

AWS Backup Actualmente, la disponibilidad es compatible con los puntos finales de VPC en las siguientes regiones: AWS

- Región del Este de EE. UU. (Ohio)
- Región del Este de EE. UU (Norte de Virginia)
- Región del oeste de EE. UU (Oregón)
- US West (N. California) Region
- Región África (Ciudad del Cabo)

- Región de Asia-Pacífico (Hong Kong)
- Región de Asia-Pacífico (Bombay)
- Región Asia-Pacífico (Osaka)
- Región de Asia-Pacífico (Seúl)
- Región de Asia-Pacífico (Singapur)
- Región de Asia-Pacífico (Sídney)
- Asia Pacífico (Tokio)
- Región de Canadá (centro)
- Región de Europa (Fráncfort)
- Región de Europa (Irlanda)
- Región de Europa (Londres)
- Región de Europa (París)
- Región Europa (Estocolmo)
- Región Europa (Milán)
- Región Medio Oriente (Baréin)
- Región América del Sur (São Paulo)
- Región Asia-Pacífico (Yakarta)
- Región Asia-Pacífico (Osaka)
- Región China (Pekín)
- Región China (Ningxia)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (Estados Unidos-Oeste)

> **Note**
>
> AWS Backup para VMware no está disponible en las regiones de China (la región de China (Beijing) y la región de China (Ningxia)) ni en la región de Asia Pacífico (Yakarta).

Resiliencia en AWS Backup

AWS Backup se toma muy en serio su resiliencia (y la seguridad de sus datos).

AWS Backup almacena sus copias de seguridad con al menos la misma resistencia y durabilidad que las que le proporcionaría el AWS servicio original de su recurso si lo hubiera hecho allí.

AWS Backup está diseñado para utilizar la infraestructura AWS global a fin de replicar sus copias de seguridad en varias zonas de disponibilidad y lograr una durabilidad del 99,19% (11 nueves) en un año determinado, siempre que se respete la documentación actual. AWS Backup

AWS Backup cifra sus planes de copia de seguridad en reposo y realiza copias de seguridad de ellos de forma continua. También puede restringir el acceso a sus planes de respaldo mediante credenciales y políticas AWS Identity and Access Management (IAM). Para obtener más información, consulte Autenticación, Control de acceso y Prácticas recomendadas de seguridad en IAM.

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. AWS Backup almacena sus copias de seguridad en todas las zonas de disponibilidad. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples. Para obtener más información, consulte el Acuerdo de nivel de servicio (SLA) de AWS Backup.

Además, le AWS Backup permite copiar sus copias de seguridad en todas las regiones para aumentar aún más la resiliencia. Para obtener más información sobre la función de copia AWS Backup entre regiones, consulte Creación de una copia de seguridad.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura AWS global.

AWS Backup cuotas

Se aplican las siguientes cuotas cuando se trabaja con AWS Backup. Muchas AWS Backup cuotas se pueden ajustar si el servicio de tipo de recurso lo permite. Para solicitar un ajuste de cuota, describa su caso de uso a AWS Support.

AWS Backup cuotas

Recurso	Cuota	Notas
Número de almacenes de copia de seguridad por región y por cuenta	300	Puede solicitar un ajuste.
Número de puntos de recuperación por almacén de copia de seguridad	1 000 000	Puede solicitar un ajuste.
Número de planes de copia de seguridad por región y por cuenta	300	Puede solicitar un ajuste.
Número de versiones por plan de copia de seguridad	2,000	Puede solicitar un ajuste.
Número de asignaciones de recurso por plan de copia de seguridad	100	No ajustable
Número de trabajos de copia de seguridad activos por cuenta	Sin límite	
Número de copias de seguridad simultáneas por cuenta enviadas a una región de destino	100	Puede solicitar un ajuste para determinados recursos (actualmente, máquinas virtuales, DynamoDB avanzado, Timestream, Amazon EFS y bases de

Recurso	Cuota	Notas
		datos de SAP HANA en instancias de Amazon EC2)
Número de copias simultáneas por almacén de copias de seguridad de destino en la cuenta una vez alcanzado el límite (indicado arriba)	5	No ajustable
Número de copias simultáneas entre cuentas que se pueden realizar del mismo recurso en la misma región de destino	30	No ajustable.
Número de trabajos de copia de seguridad y copia simultáneos por recurso	1	No ajustable. Esta cuota le ayuda a mantener el rendimiento de sus cargas de trabajo.
Número de etiquetas de metadatos por copia de seguridad	50	No puede solicitar un ajuste. AWS impone esta cuota a todos los recursos. Consulte Tag naming limits and requirements en la Referencia general de AWS .
Número de etiquetas por recurso seleccionado en una política de copias de seguridad multicuentas	30	No ajustable. Se pueden incluir etiquetas adicionales utilizando múltiples asignaciones de recursos o planes de copias de seguridad.
Número de hipervisores	10	No ajustable
Número de retenciones legales	50 por cuenta	No ajustable

Recurso	Cuota	Notas
Número máximo de capas de copia de seguridad anidadas de pilas de aplicaciones	10	No ajustable

AWS Backup de las cuotas de recursos de Amazon Timestream

Recurso	Cuota	Notas
Número de trabajos de copia de seguridad simultáneos de Timestream por cuenta	4	Puede solicitar un ajuste.
Número de trabajos de restauración simultáneos de Timestream por cuenta	1	Puede solicitar un ajuste.

Hay cuotas para una sola asignación de recursos en una sola regla de copia de seguridad. Puede crear un plan de copia de seguridad con varias reglas de copia de seguridad.

AWS Backup Cuotas de Audit Manager

Recurso	Cuota	Notas
Número de marcos por región y por cuenta	15	Puede solicitar un ajuste.
Número de controles por región y por cuenta	50	Puede solicitar un ajuste.
Número de planes de informes por cuenta	20	Puede solicitar un ajuste.
Número de marcos por plan de informes	1 000	No ajustable

Recurso	Cuota	Notas
Número máximo de cuentas multiplicado por regiones en un plan de informes	300	No ajustable

Restaure las cuotas del plan de prueba

Recurso	Cuota	Notas
Planes de prueba de restauración	100	No ajustable
Número de etiquetas en cada plan	50	No ajustable
Selecciones por plan	30	No ajustable
ARN por selección de pruebas de restauración	30	No ajustable
Condiciones por selección	30	Incluye las contenidas en `StringEquals` y `StringNotEquals` .
Selectores de almacén por selección de pruebas de restauración	30	No ajustable
Valor máximo (en días) del periodo de selección	365 días	
Límites de horas del periodo de inicio	Mínimo: 1 hora; máximo: 168 horas	
Longitud máxima de caracteres del nombre del plan de prueba de restauración	50 caracteres	Alfanuméricos y guiones bajos, sin espacios en blanco

Recurso	Cuota	Notas
Longitud máxima de caracteres del nombre de la selección de pruebas de restauración	50 caracteres	Alfanuméricos y guiones bajos, sin espacios en blanco

AWS Backup gateway cuotas

Recurso	Cuota	Notas
Trabajos de copia de seguridad o restauración por puerta de enlace	4	No puede solicitar un ajuste. En cambio, cree más puertas de enlace y conéctelas al hipervisor.

Al administrar las copias de seguridad en varias cuentas mediante AWS Organizations, es posible que se le AWS Organizations impongan cuotas. Para conocer estas cuotas, consulte Cuotas para AWS Organizations en la Guía del usuario de AWS Organizations .

También es posible que te encuentres con cuotas impuestas por un servicio AWS Backup compatible, como las siguientes:

- Amazon Elastic File System
- Amazon Elastic Block Store (EBS)
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- Amazon FSx para Lustre
- Amazon FSx para Windows File Server
- Amazon DocumentDB
- Amazon Neptune
- Amazon Simple Storage Service

- Amazon Timestream

Monitorización

AWS Backup funciona con otras AWS herramientas para que pueda supervisar sus cargas de trabajo. Estas herramientas incluyen lo siguiente:

- AWS Backup paneles de consola
  - El panel de trabajos ofrece un monitorización de estado de los trabajos, donde puede ver métricas que muestran trabajos correctos y con error, filtradas por motivos, cuentas, región y tipo de recurso.
  - El panel de empleos está disponible en las regiones en las que se admite AWS Backup Audit Manager. Consulte estas regiones en Disponibilidad de las funciones por Región de AWS. Todas las demás regiones podrán acceder al CloudWatch Panel de control.
- Amazon CloudWatch y Amazon EventBridge para supervisar AWS Backup los procesos.
  - Puede utilizarlos CloudWatch para realizar un seguimiento de las métricas, crear alarmas y ver los paneles.
  - Se puede usar EventBridge para ver y monitorear AWS Backup eventos.

  Para obtener más información, consulte Monitorización de AWS Backup eventos con Amazon EventBridge.
- AWS CloudTrailpara supervisar las llamadas a la AWS Backup API. Puede identificar la hora, la IP de origen, los usuarios y las cuentas que realizan esas llamadas. Para obtener más información, consulte Registrar las llamadas a AWS Backup la API con CloudTrail.
- Amazon Simple Notification Service (Amazon SNS) para suscribirse a temas AWS Backup relacionados, como eventos de copia de seguridad, restauración y copia. Para obtener más información, consulte Opciones de notificación con AWS Backup.

AWS Backup paneles de consola

> **Note**
>
> El panel de trabajos está disponible en todas las regiones en las que se admite AWS Backup Audit Manager. Consulte estas regiones en Disponibilidad de las funciones por Región de AWS. Todas las demás regiones podrán acceder al CloudWatch Panel de control.

Temas

Información general de los paneles de copia de seguridad

AWS Backup proporciona un panel de tareas en la consola para ayudarle a supervisar el estado de sus tareas de backup, copia y restauración. Los mismos datos que se muestran visualmente en la consola se pueden recuperar mediante la línea de comandos AWS CLI.

El panel de trabajos se puede utilizar para identificar problemas relacionados con trabajos de copia de seguridad, copia y restauración mediante monitorización de nivel de la organización o de cuentas de miembros. Con esta información puede identificar y diagnosticar eventos y posibles problemas para garantizar la fidelidad de sus actividades.

El panel de trabajos puede mostrar dos periodos. De forma predeterminada, se muestran los datos de los últimos 14 días, pero puede cambiar la vista para mostrar los 7 últimos días. Si cambias el periodo, los datos se actualizarán para reflejar el nuevo intervalo de tiempo.

Tenga en cuenta que el panel muestra los datos hasta las 0:00 UTC más recientes; es decir, no se incluyen los datos del día actual. El panel se actualiza a diario aproximadamente entre las 1:30 y las 2:30 UTC.

Visualización del panel de trabajos

Para ver el panel de tareas, inicie sesión en la AWS Backup consola y seleccione los paneles de tareas en la barra de navegación izquierda.

En la página del panel de trabajos puede seleccionar la pestaña de trabajos de copia de seguridad, copia o restauración.

La descripción general del panel de trabajos muestra la vista agregada durante el periodo de tiempo especificado para la actividad laboral, incluidos los trabajos completados, completados con problemas, vencidos y fallidos. De forma predeterminada, se muestran los datos de los últimos 14 días, pero puede cambiar la vista para mostrar 7 días.

> **Note**
>
> `Completed with issues` es el estado de un trabajo que se muestra en la consola y que indica un trabajo completado con un mensaje de estado.

Estado del trabajo

El gráfico de líneas muestra las líneas de tasas de trabajos correctos y con error a lo largo del tiempo. La línea de tasa de trabajos correctos muestra una suma de los trabajos completados y completados con problemas. La línea de tasa de trabajos con error muestra la suma de los trabajos con error y vencidos según el intervalo de tiempo especificado.

No se incluyen los trabajos no completados o sin error (los trabajos con estado de creados, pendientes, en ejecución, anulados, cancelando o parciales); los totales porcentuales pueden no ser iguales al 100 %.

Estado del trabajo a lo largo del tiempo

Con el gráfico de barras puede generar un gráfico de barras personalizado que muestre el número de trabajos de cada categoría (completados, completados con problemas, con error y vencidos), distribuidos por días.

En los menús desplegables, elija los estados, los tipos de recursos y AWS las regiones que desee ver en el gráfico. Si desea explorar más a fondo la selección, elija Ver trabajos para ver una parte prefiltrada de la página de monitorización de trabajos/múltiples cuentas.

Puede pasar el ratón sobre una barra para mostrar una ventana emergente con datos detallados de los trabajos correspondientes a la fecha seleccionada.

Trabajos problemáticos

Un trabajo problemático es aquel que tiene el estado Con error, Vencido o Completo con problemas. Cada gráfico muestra la métrica correspondiente que contiene las cuentas, los tipos de recursos o los principales motivos con el mayor número de trabajos problemáticos.

La pantalla predeterminada ordena el widget del panel por la métrica especificada en orden descendente, empezando por la métrica con el número más alto de trabajos problemáticos que corresponden a la métrica.

La pantalla de cuentas más problemáticas solo será visible en las cuentas que tengan acceso a través de Organizations, como las cuentas administrativas y las cuentas de administrador delegado. Si es visible, puede pasar el ratón sobre una cuenta para mostrar el número de trabajos problemáticos que corresponden a la cuenta elegida.

Puede seleccionar una barra dentro del gráfico para abrir una ventana emergente. En esta ventana puede seleccionar el estado de un trabajo para abrir una tabla de monitorización de trabajos/ múltiples cuentas filtrada por el estado seleccionado.

Motivos para los trabajos problemáticos

El widget Principales motivos que ocasionan problemas muestra la categoría de códigos de mensaje a la que pertenecen los mensajes de error. Sin embargo, es posible que la categoría no explique los problemas que experimenta un trabajo. Amplíe las categorías de códigos de mensaje que aparecen a continuación para obtener más información sobre los mensajes o errores específicos que podrían surgir en sus trabajos.

"VSS_ERROR"

- "El intento de copia de seguridad de Windows VSS ha producido error porque la instancia o el agente SSM tienen un estado no válido o privilegios insuficientes."
- "El intento de copia de seguridad de Windows VSS ha producido error por falta de privilegios suficientes para realizar esta operación"
- "El intento de copia de seguridad de Windows VSS ha producido error porque ec2-vss-agent.exe no está instalado en la instancia"
- "Se ha encontrado error de trabajo de copia de seguridad de Windows VSS al intentar copia de seguridad periódica"
- "El intento de copia de seguridad de Windows VSS ha producido error porque se ha agotado el tiempo de espera en la creación de instantáneas para VSS"
- "El intento de copia de seguridad de Windows VSS ha producido error debido a una versión de Windows Server no compatible. Las versiones compatibles son Windows Server 2012 o posterior."
- "El intento de copia de seguridad de Windows VSS ha producido error porque se ha agotado el tiempo de espera en la creación de instantáneas para VSS"

"LIMIT_EXCEEDED"

- "Se ha superado el límite de suscriptores: ha alcanzado el número máximo de copias de seguridad simultáneas, que es de 300. Inténtelo de nuevo. También puedes ponerte en contacto con nosotros AWS Support para solicitar un aumento de cuota».
- "Se ha superado el número máximo permitido de instantáneas en curso para un solo volumen."
- "Se ha superado el límite máximo permitido de instantáneas activas."
- "No se pueden crear más de 20 instantáneas de usuario"
- "El conjunto de etiquetas resultante no debe tener más de 50 etiquetas de usuario."
- "Ha alcanzado el número máximo de copias de seguridad admitidas para su cuenta o base de datos. Para obtener información adicional, consulte Cuotas en la Guía para desarrolladores de Timestream."
- "Ha alcanzado su cuota de 50 000 imágenes públicas y privadas permitidas en esta región. Anule el registro de las imágenes no utilizadas o solicite un aumento en su cuota de AMI."
- «Tu copia de seguridad se ha realizado correctamente, pero no hemos podido conservar NetworkInterfaces los metadatos porque su tamaño ha superado nuestros límites internos».
- "REGEX#Superado límite de suscriptores"
- "REGEX#Especificadas más de 50 etiquetas"
- "REGEX#puede tener como máximo"

"ACCESS_DENIED"

- "No está autorizado a realizar esta operación."
- «Acceso denegado al intentar llamar al AWS Backup servicio»
- «Las imágenes de AWS Marketplace no se pueden copiar a otra AWS cuenta».
- "El trabajo de copia ha producido error porque el almacén de copia de seguridad de destino está cifrado con la clave predeterminada administrada por el servicio de copia de seguridad. El contenido de este almacén no se puede copiar. Solo se puede copiar el contenido de un almacén de Backup cifrado con una AWS KMS clave.
- Las instantáneas cifradas con la no se Clave administrada de AWS pueden compartir. Especifique otra instantánea.
- "Las instantáneas cifradas con la clave predeterminada de Amazon EBS no se pueden compartir
- "Error de trabajo de copia. La cuenta de origen y destino debe ser miembro de la misma organización."

- "REGEX#acceso denegado"
- "REGEX#no autorizado a"
- «REGEX #cannot» debe ser asumido por AWS Backup
- "REGEX#no tiene permiso"
- "REGEX#falta permiso"

"CONCURRENT_JOB"

- "El trabajo de copia de seguridad ha producido error porque había un trabajo en ejecución para el mismo recurso."

"FEATURE_NOT_ENABLED"

- "Error de trabajo de copia. La característica de copia de múltiples cuentas no está habilitada para la organización actual."

"JOB_EXPIRED"

- "El trabajo de copia de seguridad venció antes de completarse."

"INVALID_LIFECYCLE"

- "Error de trabajo de copia. La retención especificada en el trabajo no está dentro del rango especificado para el almacén de copia de seguridad de destino."
- "REGEX #no se pudo iniciar porque está dentro o demasiado cerca del periodo de mantenimiento semanal configurado"
- "REGEX#no se pudo iniciar porque está dentro o demasiado cerca del periodo de copia de seguridad automática configurado"

"INVALID_STATE"

- "REGEX#instancia no está en estado"
- "REGEX#no en el estado disponible"
- "REGEX#no en estado disponible"
- "REGEX#No puede volumen de instantáneas"

"KMS_KEY_ERROR"

- "La clave de KMS está deshabilitada o pendiente de eliminación o se ha denegado el acceso a la clave de KMS"
- "No se puede acceder al ID de clave dado"
- "Error en la copia de instantánea de AMI: no se puede acceder al ID de clave dado. Debe tener DescribeKey permisos en la CMK predeterminada»
- "REGEX#clave de kms"

"ACCESS_KEY_ERROR"

- «El identificador de clave de AWS acceso necesita una suscripción al servicio»

"HYPERVISOR_OFFLINE"

- "Esta operación no es válida para el hipervisor especificado porque no está en línea"

"RESOURCE_NOT_FOUND"

- "El volumen especificado no se ha encontrado."
- "No se encuentra la máquina virtual."
- "El ID de clave dado no existe"
- "REGEX#no existe"
- "REGEX#No se encuentra el recurso"
- "REGEX#No se encuentra cryopod"
- "REGEX#No se encuentra punto de recuperación"
- "REGEX#no se encuentra recurso"
- "REGEX#ya no está disponible"
- "REGEX#no es válido"

"RESOURCE_NOT_SUPPORTED"

- "REGEX#tipo de recurso incompatible"
- "REGEX#Tipo de recurso incompatible"

"TAG_COPY_ERROR"

- "No podemos copiar las etiquetas de recursos a la copia de seguridad debido a un error interno."
- "No podemos copiar las etiquetas de recursos a su copia de seguridad porque no está disponible el punto de recuperación de origen o destino"

"TOKEN_EXPIRED"

- "Token vencido. Inténtelo de nuevo."

"UNSUPPORTED_OPERATION"

- «CreateSnapshot El hipervisor no admite el método durante la creación de la instantánea. Trabajo de copia de seguridad cancelado"
- «UnsupportedOperation : Las copias de seguridad de Storage Gateway requieren una bóveda de respaldo creada por el usuario y una CMK en el lugar de destino».
- "REGEX#Característica no compatible con el tipo de recurso proporcionado."

"FATAL_ERROR"

- "Se ha producido un error interno."
- "El trabajo de copia detectó un error grave. Póngase en contacto con AWS Support para obtener más ayuda».
- "El trabajo de copia detectó un error grave."
- "REGEX#Trabajo de copia de seguridad encontró un error grave"

Obtención de datos del panel mediante AWS CLI

Puede utilizar la línea de comandos para recuperar los mismos datos que aparecen en la consola. Utilice uno de los siguientes comandos de la CLI:

- `list-backup-job-summaries`
- `list-copy-job-summaries`
- `list-restore-job-summaries`

Estos son los parámetros válidos que puede incluir en cada comando:

```
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)
```

En este ejemplo se muestra una solicitud en la que el usuario tiene `list-backup-job-summaries` de entrada y la solicitud pide que se devuelvan todas las cuentas disponibles con un estado de `FAILED` que supere los 14 días anteriores:

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

Para obtener un recuento de trabajos con un estado de `completed with issues`, reste el recuento de `COMPLETED` trabajos de con una `MessageCategory` de `SUCCESS` del número total de `COMPLETED`.

Monitorización de AWS Backup eventos con Amazon EventBridge

AWS Backup envía eventos a Amazon EventBridge cuando cambia el estado de un trabajo de copia de seguridad o copia. Se puede utilizar EventBridge para monitorizar AWS Backup eventos. Por ejemplo, puede recibir una alarma cuando se produce un error en una tarea de copia de seguridad. AWS Backup emite eventos de la mejor EventBridge manera posible cada 5 minutos.

Para realizar un seguimiento de los eventos mediante EventBridge, consulte lo siguiente:

- Crear una regla que reaccione a los eventos (Guía EventBridge del usuario de Amazon)
- Amazon CloudWatch Events and Metrics para AWS Backup (blog; consulte Configurar AWS Backup eventos para enviarlos a Amazon EventBridge)

Algunos eventos informan `status: COMPLETED` mientras que otros informan `state: COMPLETED`. Esto es coherente con la AWS Backup API. Algunos estados son específicos de la AWS Backup consola: el `Completed with issues` estado es una representación de los `Completed` trabajos con mensajes de estado. Para monitorizar eventos `Completed with issues`, monitorice los trabajos `COMPLETED` que tengan un mensaje de estado.

También puede utilizar la API de AWS Backup notificaciones para realizar un seguimiento de AWS Backup los eventos con Amazon Simple Notification Service (Amazon SNS). Sin embargo, EventBridge rastrea más cambios que la API de notificaciones, incluidos los cambios en los almacenes de respaldo, el estado de las tareas de copia de seguridad, la configuración regional y el número de puntos de recuperación en frío o en caliente.

Eventos

- Eventos de Backup Job
- Eventos de Backup Plan
- Eventos de Backup Vault
- Eventos de Copy Job
- Eventos de Recovery Point
- Eventos de configuración regional
- Restaurar eventos de Job

Eventos de Backup Job

Los siguientes son ejemplos de eventos.

Estado

Estado: FALLIDO


```
{
  "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
  }
}
```

Estado: COMPLETADO

```
{
  "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
  }
}
```

Estado: EN EJECUCIÓN

```
{
  "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"
    }
  }
}
```


Estado: ABORTADO


```
{
  "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
  }
}
```

Estado: CADUCADO

```
{
  "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"
    }
  }
}
```

Estado: PENDIENTE

```
{
  "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
  }
}
```

Estado: CREADO

```
{
```

```
  "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"
  }
}
```

Eventos de Backup Plan

Los siguientes son ejemplos de eventos.

Estado

- Estado: MODIFICADO
- Estado: ELIMINADO
- Estado: CREADO

Estado: MODIFICADO

```
{
  "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"
  }
}
```

Estado: ELIMINADO

```
{
  "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"
  }
}
```

Estado: CREADO

```
{
  "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"
  }
}
```

Eventos de Backup Vault

Los siguientes son ejemplos de eventos.

Estado

- Estado: CREADO
- Estado: MODIFICADO
- Estado: ELIMINADO

Estado: CREADO

```
{
  "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"
  }
}
```

Estado: MODIFICADO

```
{
  "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"
  }
}
```

Estado: ELIMINADO

```
{
  "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"
  }
}
```

Eventos de Copy Job

A continuación se muestran ejemplos de eventos.

Estado

- Estado: FALLIDO
- Estado: EN EJECUCIÓN

Estado: FALLIDO


```
{
  "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": {}
  }
}
```


Estado: EN EJECUCIÓN


```
{
  "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"
    }
  }
}
```


Estado: FINALIZADO


```
{
  "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"
    }
  }
}
```

Estado: CREADO

```
{
  "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"
  }
}
```

Eventos de Recovery Point

Los siguientes son ejemplos de eventos.

Estado

- Estado: COMPLETADO
- Estado: ELIMINADO
- Estado: MODIFICADO

Estado: COMPLETADO

```
{
    "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"
        }
    }
}
```

Estado: ELIMINADO

```
{
  "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"
    }
  }
}
```

Estado: MODIFICADO

```
{
  "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"
  }
}
```

Eventos de configuración regional

El siguiente es un evento de ejemplo.

```
{
  "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"
  }
```

```
}
```

Restaurar eventos de Job

A continuación se muestran ejemplos de eventos.

Estado

- Estado: FALLIDO
- Estado: EN EJECUCIÓN
- Estado: FINALIZADO
- Estado: PENDIENTE
- Estado: CREADO

Estado: FALLIDO

```
{
  "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."
```

```
  }
}
```

Estado: EN EJECUCIÓN

```
{
  "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"
  }
}
```

Estado: FINALIZADO

```
{
  "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"
  }
}
```

Estado: PENDIENTE

```
{
  "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"
  }
}
```

Estado: CREADO

```
{
  "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 métricas con Amazon CloudWatch

Temas

- CloudWatch Panel de control
- Métricas con CloudWatch

CloudWatch Panel de control

> **Note**
>
> El panel de la consola depende de la región desde la que se acceda a la consola. Consulte Disponibilidad de las funciones por Región de AWS para ver qué regiones tienen acceso al panel de trabajos. Las regiones que no figuren en la lista podrán acceder al CloudWatch panel.

La AWS Backup consola incluye un panel de control para ver las métricas de los trabajos de backup, copia y restauración completados o fallidos. En este panel, puede ver el estado del trabajo por periodo de tiempo y personalizarlo según el periodo de tiempo que desee.

PARA ACCEDER AL PANEL

1. Abre la AWS Backup consola en https://console.aws.amazon.com/backup.
2. En el panel de navegación izquierdo, seleccione Panel.

VISUALIZACIÓN Y COMPRENSIÓN DEL PANEL

El CloudWatch panel de control muestra varios widgets. Cada widget muestra las métricas de los trabajos por recuento. Cada widget muestra varios gráficos de líneas. Cada línea corresponde a un recurso protegido (si no ve un recurso esperado en la pantalla, asegúrese de que el recurso esté activado en Configuración). Las pantallas no muestran los trabajos en curso.

El eje y (valores verticales) muestra el recuento. El eje x (valores horizontales) muestra puntos en el tiempo. Si no hay puntos de datos que visualizar en el estado del trabajo seleccionado, el valor se establecerá en 0 con una línea horizontal en el eje x. La leyenda que muestra los recursos seguirá siendo visible.

Las métricas muestran información específica de la cuenta y de la región relacionada con el inicio de sesión actual. Para ver otras cuentas o regiones, debe iniciar sesión con la cuenta elegida.

PERSONALIZACIÓN DEL PANEL

De forma predeterminada, el periodo de tiempo que se muestra es de una semana. En el menú superior, hay opciones para redefinir el periodo de tiempo mostrado. Puede elegir entre 1 hora, 3 horas, 12 horas, 1 día, 3 días y 1 semana. Además, puede seleccionar Personalizado para

especificar un valor diferente. La personalización cambiará temporalmente la vista actual a sus especificaciones.

Si pasa el ratón por encima de un widget, se mostrará el botón Ampliar en la parte superior derecha del widget. Haga clic en Ampliar para abrir el widget en pantalla completa. En pantalla completa, hay más opciones para personalizar la visualización del gráfico, como cambiar el periodo (el tiempo entre cada punto de datos). Los cambios no se retendrán una vez que se cierre la vista de pantalla completa.

Para ver solo un tipo de recurso a la vez, haga clic en el texto de la etiqueta del tipo de recurso que desee ver en la leyenda del gráfico. De este modo se anula la selección de todos los tipos de recursos. Para revertir esta situación, haga clic en el cuadro de color de un tipo de recurso en la leyenda. Para volver a la vista predeterminada de todos los tipos de recursos con todas las etiquetas seleccionadas, vuelva a hacer clic en el texto de la etiqueta de cualquier tipo de recurso seleccionado.

Al hacer clic en los tres puntos verticales de la esquina superior derecha de un widget, se abre un menú desplegable con opciones para actualizar, ampliar, ver en métricas y ver en registros. Al «Ver en métricas», se abre la métrica utilizada en el widget de la CloudWatch consola. Allí puedes realizar cualquier cambio en el widget y añadirlo a un panel personalizado en el panel de CloudWatch control. Los cambios que realices en el CloudWatch panel de control no se reflejarán en el panel de control de la AWS Backup consola. «Ver como registros» abre la página de visualización de registros en la CloudWatch consola.

Para añadir los widgets que se muestran en tu CloudWatch panel de control personalizado, haz clic en el botón Añadir al panel de control situado en la parte superior derecha del panel de control. Se abrirá la CloudWatch consola en la que podrá seleccionar en qué panel personalizado desea añadir los seis widgets.

Para obtener más información, consulta Uso de CloudWatch las métricas de Amazon.

Métricas con CloudWatch

Se puede utilizar CloudWatch para supervisar AWS Backup las métricas. El espacio de `AWS/Backup` nombres te permite realizar un seguimiento de las siguientes métricas. AWS Backup emite métricas actualizadas CloudWatch cada 5 minutos.

El objetivo de esta página de documentación es proporcionarle los materiales de referencia que podrá utilizar CloudWatch en el seguimiento AWS Backup. Para obtener información sobre cómo

monitorear una métrica mediante CloudWatch, consulte el blog Amazon CloudWatch Events and Metrics for AWS Backup o Céntrese en las métricas y las alarmas en un solo AWS servicio en la Guía del CloudWatch usuario. Para configurar las alarmas, consulte Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario.

Categoría	Métricas	Dimensiones de ejemplo	Ejemplo de caso de uso
Jobs	Número de trabajos de copia de seguridad , restauración y copia en cada estado, lo que incluye `CREATED`, `PENDING`, `RUNNING`, `ABORTED`, `COMPLETED` , `FAILED` y `EXPIRED`. Los diferentes tipos de trabajo tienen diferentes estados disponibles.	Tipo de recurso, nombre del almacén. El nombre del almacén de los trabajos de copia es el de su almacén de destino.	Monitorice el número de trabajos de copia de seguridad que dan lugar a errores en uno o más almacenes de copia de seguridad específicos. Si hay más de cinco trabajos que tienen como resultado un error en una hora, envíe un correo electrónico o un SMS a través de Amazon SNS o abra un ticket para que el equipo de ingeniería lo investigue. Criterios del informe: hay un valor distinto de cero
Puntos de recuperación	Número de puntos de recuperación en caliente y frío en cada estado: `MODIFIED`, `COMPLETED` , `PARTIAL`, `EXPIRED`, `DELETED`.	Tipo de recurso, nombre del almacén.	Realice un seguimiento del número de puntos de recuperación eliminados de sus volúmenes de Amazon EBS y realice un seguimiento aparte

Categoría	Métricas	Dimensiones de ejemplo	Ejemplo de caso de uso
			del número de puntos de recuperación en caliente y en frío en cada almacén de copias de seguridad. Criterios del informe: hay un valor distinto de cero

> **Note**
>
> El estado de la tarea `Completed with issues` es específico únicamente de la AWS Backup consola; no se puede rastrear a través de ella CloudWatch.

La tabla siguiente enumera todas las métricas a su disposición.

Métrica	Descripción
`NumberOfBackupJobsCreated`	El número de trabajos de copia de seguridad que AWS Backup se crearon.
`NumberOfBackupJobsPending`	El número de trabajos de copia de seguridad que están a punto de ejecutarse en AWS Backup.
`NumberOfBackupJobsRunning`	El número de trabajos de copia de seguridad que se están ejecutando actualmente AWS Backup.
`NumberOfBackupJobsAborted`	El número de trabajos de copia de seguridad cancelados por el usuario.

Métrica	Descripción
`NumberOfBackupJobsCompleted`	El número de trabajos de copia de seguridad AWS Backup finalizados.
`NumberOfBackupJobsFailed`	El número de trabajos de copia de seguridad cuyo estado es`Failed`. A menudo, se debe a la programación de una tarea de copia de seguridad durante o 1 hora antes de un recurso de base de datos o 4 horas antes o durante una ventana de mantenimiento de Amazon FSx o una ventana de copia de seguridad automátic a y no se utiliza AWS Backup para realizar copias de seguridad continuas para point-in-time las restauraciones. Consulte Point-in-Time Recovery para obtener una lista de los servicios compatibles e instrucciones sobre cómo AWS Backup utilizarlos para realizar copias de seguridad continuas o reprogramar sus tareas de copia de seguridad.
`NumberOfBackupJobsExpired`	El número de trabajos de copia de seguridad cuyo estado es. `EXPIRED` Un trabajo de copia de seguridad cambia de estado `CREATED` a `EXPIRED` si una copia de seguridad no puede comenzar dentro de la ventana de inicio.
`NumberOfCopyJobsCreated`	Número de trabajos de copia entre cuentas y regiones que ha creado AWS Backup .
`NumberOfCopyJobsRunning`	Número de trabajos de copia entre cuentas y regiones que se están ejecutando en la actualidad en AWS Backup.
`NumberOfCopyJobsCompleted`	Número de trabajos de copia entre cuentas y regiones que ha finalizado AWS Backup .

Métrica	Descripción
NumberOfCopyJobsFailed	El número de trabajos de copia entre cuentas y regiones que se AWS Backup intentaron realizar pero no se pudieron completar.
NumberOfRestoreJobsPending	El número de trabajos de restauración que están a punto de ejecutarse en AWS Backup.
NumberOfRestoreJobsRunning	El número de trabajos de restauración que se están ejecutando actualmente. AWS Backup
NumberOfRestoreJobsCompleted	El número de trabajos de restauración AWS Backup finalizados.
NumberOfRestoreJobsFailed	El número de trabajos de restauración que se AWS Backup intentaron realizar pero no se pudieron completar.
NumberOfRecoveryPointsCompleted	El número de puntos de recuperación que se AWS Backup crearon.
NumberOfRecoveryPointsPartial	El número de puntos de recuperación que se AWS Backup empezaron a crear pero no se pudieron terminar. AWS reintenta el proceso más adelante, pero como el reintento se produce más tarde, conserva el punto de recuperación parcial.
NumberOfRecoveryPointsExpired	La cantidad de puntos de recuperación que se AWS Backup intentaron eliminar en función del ciclo de vida de retención de la copia de seguridad, pero que no se pudieron eliminar. Se le facturará por el almacenamiento que consuman las copias de seguridad vencidas y deberá eliminarlas manualmente.
NumberOfRecoveryPointsDeleting	La cantidad de puntos de recuperación que AWS Backup se están eliminando.

Métrica	Descripción
`NumberOfRecoveryPointsCold`	El número de puntos de recuperación AWS Backup agrupados en almacenamiento en frío.

Hay más dimensiones disponibles además de las que se indican en la tabla. Para ver todas las dimensiones de una métrica, escriba el nombre de esa métrica en el espacio de `AWS/Backup` nombres de la sección de métricas de la consola. CloudWatch

Registrar las llamadas a AWS Backup la API con CloudTrail

AWS Backup está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS servicio. CloudTrail captura todas las llamadas a la API AWS Backup como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Backup consola y llamadas en código a las operaciones de la AWS Backup API. Con la información recopilada por CloudTrail, puede determinar a qué solicitud se realizó AWS Backup, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu cuenta Cuenta de AWS al crear la cuenta y automáticamente tienes acceso al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

AWS Backup eventos en CloudTrail

AWS Backup genera estos CloudTrail eventos cuando realiza copias de seguridad, restauraciones, copias o notificaciones. Estos eventos no se generan necesariamente mediante el uso de las API AWS Backup públicas. Para obtener más información, consulte Servicio de AWS los eventos en la Guía AWS CloudTrail del usuario.

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

Descripción de las entradas de los archivos de AWS Backup registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra las `DeleteRecoveryPoint` acciones y `StartBackupJobStartRestoreJob`, además, el `BackupJobCompleted` evento.

```
{
    "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"
    }
}
```


Registro de eventos de administración entre cuentas

Con AWS Backupél, puede administrar sus copias de seguridad en todo Cuentas de AWS el interior de su AWS Organizationsestructura. AWS Backup genera estos CloudTrail eventos cuando creas, actualizas o eliminas una política de AWS Organizations copias de seguridad (que aplica los planes de copia de seguridad a las cuentas de tus miembros) o cuando hay un plan de respaldo organizacional no válido:

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

Ejemplo: entradas de archivos de AWS Backup registro para la administración de varias cuentas

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o

más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateOrganizationalBackupPlan` acción.


```
{
    "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"
    }
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `DeleteOrganizationalBackupPlan` acción.

```
{
    "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"
    }
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra el eventoInvalidOrganizationBackupPlan, que se envía cuando se AWS Backup recibe un plan de respaldo no válido de 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"
}
```

Opciones de notificación con AWS Backup

Hay dos formas de recibir notificaciones sobre AWS Backup:

- AWS Las notificaciones de usuario pueden enviar notificaciones, incluidas CloudWatch las alarmas de Amazon y las notificaciones de otros servicios. AWS Support
- Amazon Simple Notification Service puede notificarle los AWS Backup eventos.

AWS Notificaciones de usuario y AWS Backup

AWS Backup admite la gestión de las notificaciones de respaldo desde la consola AWS de notificaciones de usuario. Con las Notificaciones de usuario de AWS, puede ver el progreso de

los trabajos de copia de seguridad, copia y restauración y los cambios en las políticas de copia de seguridad, los almacenes, los puntos de recuperación y la configuración desde el Centro de notificaciones de usuario.

Amazon CloudWatch, EventBridge las alarmas de Amazon y las actualizaciones de AWS Support casos son otros tipos de notificaciones que puedes gestionar desde la consola. Además, puedes configurar varias opciones de entrega, como el correo electrónico, AWS Chatbot las notificaciones y las notificaciones AWS Console Mobile Application push.

Amazon SNS y eventos AWS Backup

AWS Backup aprovecha las sólidas notificaciones que ofrece Amazon Simple Notification Service (Amazon SNS). Puede configurar Amazon SNS para que le notifique los AWS Backup eventos desde la consola de Amazon SNS.

Limitaciones

- Si bien el servicio Amazon SNS permite notificaciones entre cuentas, actualmente AWS Backup no admite esta función. Debe especificar su propio ID de AWS cuenta y el ARN de recurso de su tema.
- AWS Backup admite los temas estándar para la deduplicación óptima de SNS, pero actualmente no AWS Backup admite los temas de FIFO de SNS para la deduplicación estricta.

Casos de uso comunes

- Para configurar las notificaciones de los trabajos de copia de seguridad fallidos, siga los pasos que se indican en ¿Cómo puedo recibir notificaciones de los trabajos fallidos? AWS Backup de AWS Premium Support.
- Consulte ejemplos de JSON de notificaciones de Amazon SNS para ver trabajos de copia de seguridad completados, que produjeron errores o vencidos en la tabla Ejemplos de eventos que aparece más adelante.

Para obtener más información sobre Amazon SNS en general, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

AWS Backup API de notificación

Tras crear los temas con la consola de Amazon SNS o AWS Command Line Interface (AWS CLI), puede utilizar las siguientes operaciones de AWS Backup API para gestionar las notificaciones de respaldo.

- DeleteBackupVaultNotifications: elimina las notificaciones de eventos para el almacén de copias de seguridad especificado.
- GetBackupVaultNotifications: enumera todas las notificaciones de eventos para el almacén de copias de seguridad especificado.
- PutBackupVaultNotifications: activa las notificaciones para el tema y los eventos especificados.

AWS Backup admite los siguientes eventos:

Tipo de trabajo	Evento
Trabajo de copia de seguridad	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED` | `CONTINUOUS_BACKUP_INTERRUPTED`
Trabajo de copia	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
Trabajo de restauración	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
Punto de recuperación	`RECOVERY_POINT_MODIFIED`

AWS Backup para S3 admite dos eventos adicionales:

- `S3_BACKUP_OBJECT_FAILED` le notifica cualquier objeto de S3 del que AWS Backup no haya podido realizar una copia de seguridad durante un trabajo de copia de seguridad.
- `S3_RESTORE_OBJECT_FAILED` le notifica cualquier objeto de S3 que AWS Backup no haya podido restaurar durante un trabajo de restauración.

Ejemplos de eventos

Example Ejemplo: trabajo de Backup completado

```
{
    "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 Ejemplo: error en el trabajo de Backup

```
{
    "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 Ejemplo: El trabajo de backup no pudo completarse durante la ventana de backup

```
{
    "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 ejemplos de comandos de notificación

Puede usar AWS CLI comandos para suscribirse a las notificaciones de Amazon SNS de sus AWS Backup eventos, enumerarlas y eliminarlas.

Ejemplo de activación de notificaciones del almacén de copias de seguridad

El siguiente comando se suscribe a un tema de Amazon SNS del almacén de copias de seguridad especificado que le notifica cuando se inicia o finaliza un trabajo de restauración o cuando se modifica un punto de recuperación.

```
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
```

Ejemplo de obtención de notificaciones del almacén de copias de seguridad

El siguiente comando enumera todos los eventos suscritos actualmente a un tema de Amazon SNS para el almacén de copias de seguridad especificado.

```
aws backup get-backup-vault-notifications
    --backup-vault-name myVault
```

El resultado del ejemplo es el siguiente:

```
{
    "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"
}
```

Ejemplo de eliminación de notificaciones del almacén de copias de seguridad

El siguiente comando cancela la suscripción a un tema de Amazon SNS para el almacén de copias de seguridad especificado.

```
aws backup delete-backup-vault-notifications
    --backup-vault-name myVault
```

Especificar AWS Backup como principal de servicio

> **Note**
>
> AWS Backup Para permitir la publicación de temas de SNS en su nombre, debe especificarlo AWS Backup como principal de servicio.

Incluya el siguiente JSON en la política de acceso del tema Amazon SNS que utiliza para realizar un seguimiento AWS Backup de los eventos. Debe especificar el Nombre de recurso de Amazon (ARN) del tema.

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

Para obtener más información sobre cómo especificar un principal de servicio en una política de acceso a Amazon SNS, consulte Permitir que cualquier AWS recurso se publique en un tema en la Guía para desarrolladores de Amazon Simple Notification Service.

> **Note**
>
> Si su tema está cifrado, debe incluir permisos adicionales en su política AWS Backup para poder publicar en él. Para obtener más información sobre cómo permitir que los servicios publiquen en temas cifrados, consulte Habilitar la compatibilidad entre las fuentes de eventos de AWS los servicios y los temas cifrados en la Guía para desarrolladores de Amazon Simple Notification Service.

Solución de problemas AWS Backup

Cuando lo usas AWS Backup, es posible que encuentres problemas. Las siguientes secciones pueden ayudarle a solucionar algunos problemas habituales que puede encontrarse.

Si tienes preguntas generales al respecto AWS Backup, consulta las AWS Backup preguntas frecuentes. También puede buscar respuestas y publicar preguntas en el foro de AWS Backup.

Temas

Solución de problemas generales

Al realizar copias de seguridad de los recursos y restaurarlos, debe tener permiso para usar AWS Backup y acceder a los recursos que desea proteger. La forma más sencilla de tener los permisos adecuados es elegir el rol predeterminado al asignar recursos a un plan de copia de seguridad. Para obtener más información sobre el control de acceso mediante AWS Identity and Access Management (IAM) con AWS Backup, consulteControl de acceso.

Si recibe un `AccessDenied` error al intentar acceder a un AWS Backup recurso, como una bóveda de respaldo, significa que el recurso no existe o que no tiene permisos para acceder al recurso.

Si tiene problemas con la copia de seguridad y la restauración de un tipo de recurso concreto, puede resultar útil revisar el tema sobre solución de problemas de copia de seguridad y restauración de ese recurso. Para obtener más información, consulte los enlaces de la sección Cómo AWS Backup funciona con AWS los servicios compatibles.

Si AWS Backup no puede crear o eliminar un recurso, puede obtener más información sobre el problema utilizando AWS CloudTrail para ver los mensajes de error o los registros. Para obtener más información sobre el uso CloudTrail con AWS Backup, consulteRegistrar las llamadas a AWS Backup la API con CloudTrail.

Solución de problemas de creación de recursos

La siguiente información puede ayudarle a solucionar problemas con la creación de copias de seguridad.

- En general, los servicios de bases de datos de AWS no pueden iniciar las copias de seguridad una hora antes o durante el intervalo de mantenimiento o el intervalo de copia de seguridad automática. Amazon FSx no puede iniciar copias de seguridad 4 horas antes o durante el intervalo de mantenimiento o el intervalo de copia de seguridad automática (Amazon Aurora está exento de esta restricción del intervalo de mantenimiento). Las copias de seguridad instantáneas programadas durante esos periodos producirán un error. Una excepción: si opta por utilizar un servicio compatible AWS Backup para copias de seguridad instantáneas y continuas, ya no tendrá que preocuparse por esas ventanas, ya no tendrá que preocuparse por esas ventanas, ya que las AWS Backup programará automáticamente. Consulte Point-in-Time Recovery para obtener una lista de los servicios compatibles e instrucciones sobre cómo utilizarlos AWS Backup para realizar copias de seguridad continuas.
- La creación de copias de seguridad para tablas de DynamoDB producirá un error mientras se crean las tablas. La creación de una tabla de DynamoDB suele tardar un par de minutos.
- La copia de seguridad de los sistemas de archivos de Amazon EFS puede tardar hasta 7 días si los sistemas de archivos son muy grandes. Solo se puede poner en cola una copia de seguridad simultánea a la vez para un sistema de archivos de Amazon EFS. Si se pone en cola una copia de seguridad posterior mientras la anterior sigue en curso, la ventana de copia de seguridad puede caducar y no se crea ninguna copia de seguridad.
- Amazon EBS tiene una cuota flexible de 100 000 copias de seguridad Región de AWS por cuenta y las copias de seguridad adicionales fallan cuando se alcanza esta cuota. Si alcanza esta cuota, puede eliminar las copias de seguridad que sobran o solicitar un aumento. Para obtener más información acerca de cómo solicitar un aumento de cuotas, consulte Cuotas de servicio de AWS.
- Al crear copias de seguridad de de Amazon Relational Database Service (RDS), tenga en cuenta lo siguiente:
  - Si no lo utiliza AWS Backup para gestionar tanto las instantáneas de Amazon RDS como las copias de seguridad continuas con point-in-time recuperación, las copias de seguridad fallarán si se inician si están programadas o si se realizan bajo demanda durante el período de copia de seguridad diario de 30 minutos configurable por el usuario. Para obtener más información sobre las copias de seguridad automatizadas de Amazon RDS, consulte Trabajo con copias de seguridad en la Guía del usuario de Amazon RDS. Puede evitar esta limitación si lo utiliza AWS

Backup para gestionar tanto las instantáneas de Amazon RDS como las copias de seguridad continuas con point-in-time recuperación.

- Si inicia un trabajo de copia de seguridad desde la consola de Amazon RDS, esto puede entrar en conflicto con un trabajo de copia de seguridad de clústeres Aurora y provocar el error `Backup job expired before completion.`. Si ocurre esto, configure un intervalo de copias de seguridad más largo en AWS Backup.
- AWS Backup actualmente no transfiere el grupo de opciones de TDE cuando se crea un trabajo de copia. Si piensa utilizar este grupo de opciones para la creación de trabajos de copia, debe utilizar la consola de Amazon RDS o la API de Amazon RDS en lugar de las herramientas de AWS Backup . Consulte Copia de un grupo de opciones en la Guía del usuario de Amazon Relational Database Service para obtener más información.
- ERROR: las copias de seguridad bajo demanda se completan, pero las copias de seguridad programadas no se completan y dan el error "The source snapshot KMS key does not exist, is not enabled or you do not have permissions to access it". El trabajo bajo demanda se completa porque utiliza la llamada a la API `CopyDBSnapshot`, que no requiere acceso a KMS.

  SOLUCIÓN: agregue el rol de IAM a su clave de KMS. Para hacer esto, permita el rol en su política de claves de KMS.

  Para editar su política,

  1. Abra la consola de KMS.
  2. En la barra de navegación izquierda, elija claves administradas por el cliente.
  3. Haga clic en la clave administrada por el cliente que deseas editar.
  4. En Política de claves, haga clic en Cambiar a vista de política.
  5. Haga clic en Edit.
  6. Agregue el rol.

Solución de problemas de eliminación de recursos

Los puntos de recuperación creados por el recurso protegido AWS Backup no se pueden eliminar en la ventana de consola del recurso protegido. Puede eliminarlos en la AWS Backup consola seleccionándolos en el almacén donde están almacenados y, a continuación, seleccionando Eliminar.

Para eliminar un punto de recuperación o un almacén de copia de seguridad, necesita los permisos adecuados. Para obtener más información sobre el control de acceso mediante IAM with AWS Backup, consulteControl de acceso.

Solución de problemas de restauración de recursos

Restauración mediante la API

Para restaurar una copia de seguridad mediante programación, utilice la operación de API StartRestoreJob.

Para obtener los metadatos de configuración con los que se creó la copia de seguridad, puede llamar a GetRecoveryPointRestoreMetadata.

Para obtener más información, consulte Restauración de una copia de seguridad.

Restauración mediante la consola

- Restauración de datos de Amazon S3
- Restauración de una máquina virtual
- Restauración de un sistema de archivos de Amazon FSx
- Restauración de un volumen de Amazon EBS
- Restauración de un sistema de archivos de Amazon EFS
- Restauración de una tabla de Amazon DynamoDB
- Restauración de una base de datos de Amazon RDS
- Restauración de un clúster de Aurora
- Restauración de una instancia de Amazon EC2
- Restauración de un volumen de Storage Gateway
- Restauración de un clúster de Amazon DocumentDB
- Restauración de un clúster de Neptune

Solución de problemas de formato

Cuando se incluye un comodín (*) para el valor de un parámetro, el comodín se procesa para incluir valores distintos de los espacios en blanco. Los valores de un par clave-valor que contengan espacios en blanco no se incluirán como parte del comodín.

API de AWS Backup

Además de utilizar la consola, puede utilizar los tipos de datos y las acciones de la API de AWS Backup para configurar y administrar AWS Backup y sus recursos mediante programación. En esta sección se describen los tipos de datos y las acciones de AWS Backup. Contiene la referencia de la API para AWS Backup.

API de AWS Backup

- Acciones de AWS Backup
- Tipos de datos de AWS Backup

Acciones

AWS Backup admiten las siguientes acciones:

- 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

AWS Backup gateway admiten las siguientes acciones:

- 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

AWS Backup admiten las siguientes acciones:

- 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

Servicio: AWS Backup

Elimina la retención legal especificada en un punto de recuperación. Solo puede realizar esta acción un usuario con permisos suficientes.

Sintaxis de la solicitud

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

CancelDescription

Cadena que describe el motivo de la eliminación de la retención legal.

Obligatorio: sí

legalHoldId

El identificador de la retención legal.

Obligatorio: sí

RetainRecordInDays

El importe entero, en días, tras el que se eliminará la retención legal.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 201
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidResourceStateException

AWS Backup ya está realizando una acción en este punto de recuperación. No es posible realizar la acción que ha solicitado hasta que finalice la primera acción. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateBackupPlan

Servicio: AWS Backup

Crea un plan de copia de seguridad con el nombre del plan y las reglas de copia de seguridad. Un plan de respaldo es un documento que contiene información que se AWS Backup utiliza para programar tareas que crean puntos de recuperación para los recursos.

Si llama a `CreateBackupPlan` con un plan que ya existe, recibirá una excepción `AlreadyExistsException`.

Sintaxis de la solicitud

```
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"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupPlan

El cuerpo de un plan de respaldo. Incluye un `BackupPlanName` y uno o más conjuntos de `Rules`.

Tipo: objeto BackupPlanInput

Obligatorio: sí

BackupPlanTags

Las etiquetas que se van a asignar al plan de respaldo.

Tipo: mapa de cadena a cadena

Obligatorio: no

CreatorRequestId

Identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si la solicitud incluye un `CreatorRequestId` que coincide con un plan de copia de seguridad existente, se devuelve ese plan. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AdvancedBackupSettings

La configuración de un tipo de recurso. Esta opción solo está disponible para los trabajos de copia de seguridad de Volume Shadow Copy Service (VSS) de Windows.

Tipo: matriz de objetos AdvancedBackupSetting

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

BackupPlanId

El identificador del plan de respaldo.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. No es posible editarlos.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateBackupSelection

Servicio: AWS Backup

Crea un documento JSON que especifica un conjunto de recursos que se asignarán a un plan de copia de seguridad. Para ver ejemplos, consulte Asignación de recursos mediante programación.

Sintaxis de la solicitud

```
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"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

El identificador del plan de respaldo.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupSelection

El cuerpo de una solicitud para asignar un conjunto de recursos a un plan de respaldo.

Tipo: objeto BackupSelection

Obligatorio: sí

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlanId

El ID del plan de respaldo.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó la selección de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

SelectionId

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateBackupVault

Servicio: AWS Backup

Crea un contenedor lógico donde se almacenan las copias de seguridad. Una solicitud `CreateBackupVault` incluye un nombre, opcionalmente una o varias etiquetas de recursos, una clave de cifrado y un ID de solicitud.

> **Note**
>
> No incluya datos confidenciales, como los números de pasaporte, en el nombre de un almacén de copia de seguridad.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon. Constan de letras minúsculas, números y guiones.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupVaultTags

Las etiquetas que se van a asignar al almacén de copias de seguridad.

Tipo: mapa de cadena a cadena

Obligatorio: no

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

EncryptionKeyArn

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de donde se crearon. Constan de letras minúsculas, números y guiones.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

La fecha y la hora en que se creó el almacén, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateFramework

Servicio: AWS Backup

Crea un marco con uno o más controles. Un marco es un conjunto de controles que puede usar para evaluar sus prácticas de copia de seguridad. Mediante el uso de controles personalizables prediseñados para definir sus políticas, puede evaluar si sus prácticas de copia de seguridad cumplen con sus políticas y qué recursos aún no.

Sintaxis de la solicitud

```
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"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

FrameworkControls

Los controles que componen el marco. Cada control de la lista tiene un nombre, parámetros de entrada y alcance.

Tipo: matriz de objetos FrameworkControl

Obligatorio: sí

FrameworkDescription

Una descripción opcional del marco con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

FrameworkName

El nombre único del marco. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

FrameworkTags

Las etiquetas que se van a asignar al marco.

Tipo: mapa de cadena a cadena

Obligatorio: no

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `CreateFrameworkInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

FrameworkArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

FrameworkName

El nombre único del marco. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateLegalHold

Servicio: AWS Backup

Crea una retención legal en un punto de recuperación (copia de seguridad). Una retención legal es una restricción a la modificación o eliminación de una copia de seguridad hasta que un usuario autorizado cancele la retención legal. Toda acción que se lleve a cabo para eliminar o disociar un punto de recuperación dará lugar a un error si hay una o más retenciones legales activas en el punto de recuperación.

Sintaxis de la solicitud

```
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"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Description

La descripción de la retención legal.

Tipo: cadena

Obligatorio: sí

IdempotencyToken

Se trata de una cadena elegida por el usuario que se utiliza para distinguir entre llamadas que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

RecoveryPointSelection

Los criterios para asignar un conjunto de recursos, como los tipos de recursos o las bóvedas de respaldo.

Tipo: objeto RecoveryPointSelection

Obligatorio: no

Tags

Etiquetas opcionales que se incluirán. Una etiqueta es un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos. Los caracteres permitidos incluyen espacios, números y letras en UTF-8, además de los siguientes caracteres especiales: + - = . _ : /.

Tipo: mapa de cadena a cadena

Obligatorio: no

Title

El título de la retención legal.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationDate

El momento en que se creó la retención legal.

Tipo: marca temporal

Description

La descripción de la retención legal.

Tipo: cadena

LegalHoldArn

El nombre del recurso de Amazon (ARN) de la retención legal.

Tipo: cadena

LegalHoldId

El identificador de la retención legal.

Tipo: cadena

RecoveryPointSelection

Los criterios que se van a asignar a un conjunto de recursos, como los tipos de recursos o las bóvedas de respaldo.

Tipo: objeto RecoveryPointSelection

Status

El estado de la retención legal.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

El título de la retención legal.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateLogicallyAirGappedBackupVault

Servicio: AWS Backup

Crea un contenedor lógico en el que se pueden copiar las copias de seguridad.

Esta solicitud incluye un nombre, la región, el número máximo de días de retención y el número mínimo de días de retención y, opcionalmente, puede incluir etiquetas y un identificador de solicitud del creador.

> **Note**
>
> No incluya datos confidenciales, como los números de pasaporte, en el nombre de un almacén de copia de seguridad.

Sintaxis de la solicitud

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad independientes lógicamente se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región en la que se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupVaultTags

Las etiquetas que se van a asignar al almacén.

Tipo: mapa de cadena a cadena

Obligatorio: no

CreatorRequestId

El ID de la solicitud de creación.

Este parámetro es opcional. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

MaxRetentionDays

El período máximo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, AWS Backup no impone un periodo de retención máximo en los puntos de recuperación del almacén (lo que permite un almacenamiento indefinido).

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o inferior al periodo de retención máximo. Si el periodo de retención del trabajo es más largo que ese periodo de retención máximo, el almacén no podrá realizar el trabajo de copia de seguridad o de copia, y deberá modificar la configuración del ciclo de vida o utilizar un almacén diferente.

Tipo: largo

Obligatorio: sí

MinRetentionDays

Esta configuración especifica el periodo mínimo de retención durante el cual el almacén retiene sus puntos de recuperación. Si no se especifica este parámetro, no se impondrá un periodo mínimo de retención.

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o superior al periodo de retención mínimo. Si el periodo de retención del trabajo es más corto que ese periodo de retención mínimo, el almacén no podrá realizar ese trabajo de copia de seguridad o de copia, y deberá modificar la configuración del ciclo de vida o utilizar un almacén diferente.

Tipo: largo

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

El ARN (Amazon Resource Name) del almacén.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad independientes lógicamente se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región en la que se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

Fecha y hora en que se creó el almacén.

Este valor está en formato Unix, horario universal coordinado (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

VaultState

El estado actual del almacén.

Tipo: cadena

Valores válidos: `CREATING | AVAILABLE | FAILED`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateReportPlan

Servicio: AWS Backup

Crea un plan de informe. Un plan de informes es un documento que contiene información sobre el contenido del informe y dónde AWS Backup se entregará.

Si llama a `CreateReportPlan` con un plan que ya existe, recibirá una excepción `AlreadyExistsException`.

Sintaxis de la solicitud

```
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"
   }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `CreateReportPlanInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

ReportDeliveryChannel

Una estructura que contiene información sobre dónde y cómo entregar sus informes, específicamente el nombre del bucket de Amazon S3, el prefijo de clave de S3 y los formatos de sus informes.

Tipo: objeto ReportDeliveryChannel

Obligatorio: sí

ReportPlanDescription

Una descripción opcional del plan de informes con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

ReportPlanName

El nombre único del plan de informes. El nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

ReportPlanTags

Las etiquetas que se van a asignar al plan de informes.

Tipo: mapa de cadena a cadena

Obligatorio: no

ReportSetting

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Si la plantilla del informe es `RESOURCE_COMPLIANCE_REPORT` o`CONTROL_COMPLIANCE_REPORT`, este recurso de API también describe la cobertura del informe por marcos Regiones de AWS y marcos.

Tipo: objeto ReportSetting

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La fecha y la hora en que se creó la lista de dominios, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

ReportPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

ReportPlanName

El nombre único del plan de informes.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateRestoreTestingPlan

Servicio: AWS Backup

Crea un plan de pruebas de restauración.

El primero de los dos pasos para crear un plan de pruebas de restauración. Una vez que la solicitud se haya realizado correctamente, finalice el procedimiento utilizando CreateRestoreTestingSelection.

Sintaxis de la solicitud

```
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"
   }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

CreatorRequestId

Es una cadena única que identifica la solicitud y permite que se reintenten las solicitudes con un error sin riesgo de ejecutar la operación dos veces. Este parámetro es opcional. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

RestoreTestingPlan

Un plan de prueba de restauración debe contener una cadena `RestoreTestingPlanName` única que usted crea y debe contener un cron de `ScheduleExpression`. Puede incluir opcionalmente un entero de `StartWindowHours` y una cadena de `CreatorRequestId`.

`RestoreTestingPlanName` es una cadena única que es el nombre del plan de prueba de restauración. No se puede cambiar después de la creación y debe constar únicamente de caracteres alfanuméricos y guiones bajos.

Tipo: objeto RestoreTestingPlanForCreate

Obligatorio: sí

Tags

Las etiquetas que se van a asignar al plan de pruebas de restauración.

Tipo: mapa de cadena a cadena

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La fecha y la hora en que se creó el plan de informes, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

RestoreTestingPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el plan de prueba de restauración creado.

Tipo: cadena

RestoreTestingPlanName

Esta cadena única es el nombre del plan de prueba de restauración.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python

- AWS SDK para Ruby V3

CreateRestoreTestingSelection

Servicio: AWS Backup

Esta solicitud se puede enviar después de que la CreateRestoreTestingPlan solicitud se devuelva correctamente. Es la segunda parte de la creación de un plan de prueba de recursos y debe completarse secuencialmente.

Consta de `RestoreTestingSelectionName`, `ProtectedResourceType` y uno de los siguientes elementos:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Cada tipo de recurso protegido puede tener un único valor.

Una selección de pruebas de restauración puede incluir un valor comodín ("*") como `ProtectedResourceArns` junto con `ProtectedResourceConditions`. También puede incluir hasta 30 ARN de recursos protegidos específicos en `ProtectedResourceArns`.

No se puede seleccionar por tipos de recursos protegidos y al mismo tiempo por ARN específicos. La solicitud producirá error si se incluyen ambos.

Sintaxis de la solicitud

```
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
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Introduzca el nombre del plan de pruebas de restauración devuelto por la CreateRestoreTestingPlan solicitud relacionada.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

CreatorRequestId

Es una cadena única opcional que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

RestoreTestingSelection

Consta de `RestoreTestingSelectionName`, `ProtectedResourceType` y uno de los siguientes elementos:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Cada tipo de recurso protegido puede tener un único valor.

Una selección de pruebas de restauración puede incluir un valor comodín ("*") como `ProtectedResourceArns` junto con `ProtectedResourceConditions`. También puede incluir hasta 30 ARN de recursos protegidos específicos en `ProtectedResourceArns`.

Tipo: objeto RestoreTestingSelectionForCreate

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La hora en que se creó la selección de pruebas de recursos.

Tipo: marca temporal

RestoreTestingPlanArn

El ARN del plan de pruebas de restauración al que está asociada la selección de pruebas de restauración.

Tipo: cadena

RestoreTestingPlanName

El nombre del plan de pruebas de restauración.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

RestoreTestingSelectionName

El nombre de la selección de pruebas de restauración para el plan de pruebas de restauración correspondiente.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteBackupPlan

Servicio: AWS Backup

Elimina un plan de copia de seguridad. Solo puede eliminar un plan de copia de seguridad después de haber eliminado todas las selecciones de recursos asociadas. La eliminación de un plan de copia de seguridad elimina la versión actual del plan. Las versiones anteriores, si las hay, seguirán existiendo.

Sintaxis de la solicitud

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

DeletionDate

La fecha y la hora en que se eliminó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `DeletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteBackupSelection

Servicio: AWS Backup

Elimina la selección de recursos asociada a un plan de copia de seguridad especificado por `SelectionId`.

Sintaxis de la solicitud

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

selectionId

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteBackupVault

Servicio: AWS Backup

Elimina el almacén de copias de seguridad identificado por su nombre. Un almacén solo se puede eliminar si está vacío.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteBackupVaultAccessPolicy

Servicio: AWS Backup

Elimina el documento de política que administra los permisos en un almacén de copias de seguridad.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon. Constan de letras minúsculas, números y guiones.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteBackupVaultLockConfiguration

Servicio: AWS Backup

Elimina AWS Backup Vault Lock de un almacén de respaldo especificado por un nombre de almacén de respaldo.

Si la configuración del bloqueo de almacenes es inmutable, no podrá eliminar el bloqueo de almacenes mediante operaciones de API y recibirá una `InvalidRequestException` si lo intenta. Para obtener más información, consulte Vault Lock en la Guía para AWS Backup desarrolladores.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre del almacén de respaldo del que se va a eliminar AWS Backup Vault Lock.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteBackupVaultNotifications

Servicio: AWS Backup

Elimina las notificaciones de eventos para el almacén de copias de seguridad especificado.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteFramework

Servicio: AWS Backup

Elimina el marco especificado por un nombre de marco.

Sintaxis de la solicitud

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

frameworkName

El nombre único de un marco.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteRecoveryPoint

Servicio: AWS Backup

Elimina el punto de recuperación especificado por un ID de punto de recuperación.

Si el ID del punto de recuperación pertenece a una copia de seguridad continua, al llamar a este punto de conexión se elimina la copia de seguridad continua existente y se detiene la copia de seguridad continua futura.

Cuando los permisos de un rol de IAM no son suficientes para llamar a esta API, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío, pero el punto de recuperación no se elimina. En su lugar, entra en un estado `EXPIRED`.

Los puntos de recuperación `EXPIRED` se pueden eliminar con esta API una vez que el rol de IAM tenga la acción `iam:CreateServiceLinkedRole`. Para obtener más información acerca de cómo agregar este rol, consulte Solución de problemas de eliminaciones manuales.

Si se elimina el usuario o el rol o se quita el permiso del rol, la eliminación no se realizará correctamente y pasará a un estado `EXPIRED`.

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

InvalidResourceStateException

AWS Backup ya está realizando una acción en este punto de recuperación. No es posible realizar la acción que ha solicitado hasta que finalice la primera acción. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteReportPlan

Servicio: AWS Backup

Elimina el plan de informes especificado por un nombre de plan de informes.

Sintaxis de la solicitud

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único de un plan de informes.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteRestoreTestingPlan

Servicio: AWS Backup

Esta solicitud elimina el plan de prueba de restauración especificado.

La eliminación solo se puede realizar correctamente si se eliminan primero todas las selecciones de pruebas de restauración asociadas.

Sintaxis de la solicitud

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Nombre único obligatorio del plan de prueba de restauración que desea eliminar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteRestoreTestingSelection

Servicio: AWS Backup

Introduzca el nombre del plan de prueba de restauración y el nombre de la selección de pruebas de restauración.

Todas las selecciones de pruebas asociadas a un plan de prueba de restauración deben eliminarse para poder eliminar el plan de prueba de restauración.

Sintaxis de la solicitud

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Nombre único obligatorio del plan de prueba de restauración que contiene la selección de pruebas de restauración que desea eliminar.

Obligatorio: sí

RestoreTestingSelectionName

Nombre único obligatorio de la selección de pruebas de restauración que desea eliminar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeBackupJob

Servicio: AWS Backup

Devuelve los detalles del trabajo de copia de seguridad para el `BackupJobId` especificado.

Sintaxis de la solicitud

```
GET /backup-jobs/backupJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupJobId

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccountId

Devuelve el ID de la cuenta a la que pertenece el trabajo de copia de seguridad.

Tipo: String

Patrón: `^[0-9]{12}$`

BackupJobId

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Tipo: cadena

BackupOptions

Representa las opciones especificadas como parte del plan de copia de seguridad o del trabajo de copia de seguridad bajo demanda.

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.]{1,50}$`

BackupSizeInBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

BackupType

Representa el tipo de copia de seguridad real seleccionado para un trabajo de copia de seguridad. Por ejemplo, si se realizó una copia de seguridad correcta de Volume Shadow Copy Service (VSS) de Windows, `BackupType` devuelve `"WindowsVSS"`. Si `BackupType` está vacío, significa que el tipo de copia de seguridad era una copia de seguridad normal.

Tipo: cadena

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

BytesTransferred

El tamaño en bytes transferido a un almacén de copias de seguridad en el momento en que se consultó el estado del trabajo.

Tipo: largo

ChildJobsInState

Devuelve las estadísticas de los trabajos de copia de seguridad secundarios (anidados) incluidos.

Tipo: mapa de cadena a largo

Claves válidas: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

CompletionDate

La fecha y la hora en que se completó un trabajo para crear un trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de copia de seguridad, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad utilizado para crearlo.

Tipo: objeto RecoveryPointCreator

CreationDate

La fecha y la hora en que se creó el trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

ExpectedCompletionDate

La fecha y la hora en que se espera completar un trabajo de copia de seguridad de recursos, en formato Unix y horario universal coordinado (UTC). El valor de `ExpectedCompletionDate`

tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

InitiationDate

La fecha en que se inició un trabajo de copia de seguridad.

Tipo: marca temporal

IsParent

Esto devuelve el valor booleano de que un trabajo de copia de seguridad es un trabajo principal (compuesto).

Tipo: Booleano

MessageCategory

El recuento de trabajos para la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `INVALIDPARAMETERS`. Consulte Monitoring para ver una lista de MessageCategory cadenas aceptadas.

Tipo: cadena

NumberOfChildJobs

Esto devuelve el número de trabajos de copia de seguridad secundarios (anidados).

Tipo: largo

ParentJobId

Esto devuelve el ID del trabajo de copia de seguridad del recurso principal (compuesto).

Tipo: cadena

PercentDone

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

ResourceArn

Un ARN que identifica de forma exclusiva un recurso guardado. El formato del ARN depende del tipo de recurso.

Tipo: cadena

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

ResourceType

El tipo de AWS recurso del que se va a hacer una copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

Especifica la hora en formato Unix y horario universal coordinado (UTC) en la que se debe iniciar un trabajo de copia de seguridad antes de que se cancele. El valor se calcula agregando el periodo de inicio a la hora programada. Por lo tanto, si la hora programada fueran las 18:00 h y el periodo de inicio fuera de 2 horas, la hora `StartBy` sería las 20:00 h en la fecha especificada.

El valor de `StartBy` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

State

El estado actual de un trabajo de copia de seguridad.

Tipo: cadena

Valores válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

Un mensaje detallado que explica el estado del trabajo de copia de seguridad de un recurso.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DependencyFailureException

Un AWS servicio o recurso dependiente devolvió un error al AWS Backup servicio y no se pudo completar la acción.

Código de estado HTTP: 500

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeBackupVault

Servicio: AWS Backup

Devuelve los metadatos de un almacén de copias de seguridad especificado por su nombre.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

El ID de cuenta del almacén de copias de seguridad especificado.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de donde se crearon.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el almacén, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional. Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

EncryptionKeyArn

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

LockDate

La fecha y la hora en las que no se puede cambiar ni eliminar la configuración de AWS Backup Vault Lock.

Si ha aplicado el bloqueo de almacenes a su almacén sin especificar una fecha de bloqueo, puede cambiar cualquier configuración del bloqueo de almacenes o eliminarlo del almacén por completo en cualquier momento.

Este valor está en formato Unix, horario universal coordinado (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Locked

Un valor booleano que indica si AWS Backup Vault Lock protege actualmente el almacén de respaldo. `True`significa que Vault Lock provoca un error en las operaciones de eliminación o actualización de los puntos de recuperación almacenados en el almacén.

Tipo: Booleano

MaxRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período máximo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo de almacenes no impone un periodo de retención máximo en los puntos de recuperación del almacén (lo que permite un almacenamiento indefinido).

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o inferior al periodo de retención máximo. Si el periodo de retención del trabajo es superior a ese periodo de retención máximo, el almacén falla el trabajo de copia de seguridad o de copia de seguridad, y deberá modificar

la configuración del ciclo de vida o utilizar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

MinRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período mínimo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo del almacén no impondrá un periodo mínimo de retención.

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o superior al periodo de retención mínimo. Si el periodo de retención del trabajo es más breve que ese periodo de retención mínimo, el almacén dará error en el trabajo de copia de seguridad o copia, y deberá modificar la configuración del ciclo de vida o usar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

NumberOfRecoveryPoints

El número de puntos de recuperación que se almacenan en un almacén de copias de seguridad.

Tipo: largo

VaultType

El tipo de depósito descrito.

Tipo: cadena

Valores válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeCopyJob

Servicio: AWS Backup

Devuelve los metadatos asociados a la creación de una copia de un recurso.

Sintaxis de la solicitud

```
GET /copy-jobs/copyJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

copyJobId

Identifica de forma exclusiva un trabajo de copia.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
    }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CopyJob

Contiene información detallada acerca de un trabajo de copia.

Tipo: objeto CopyJob

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeFramework

Servicio: AWS Backup

Devuelve los detalles del marco para el `FrameworkName` especificado.

Sintaxis de la solicitud

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

frameworkName

El nombre único de un marco.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

Es la fecha y la hora en que se creó un marco con la norma ISO 8601. El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, 2020-07-10T15:00:00.000-08:00 representa el 10 de julio de 2020 a las 15:00 h, 8 horas menos que UTC.

Tipo: marca temporal

DeploymentStatus

El estado de implementación de un marco. Los estados son:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Tipo: cadena

FrameworkArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

FrameworkControls

Los controles que componen el marco. Cada control de la lista tiene un nombre, parámetros de entrada y alcance.

Tipo: matriz de objetos FrameworkControl

FrameworkDescription

Una descripción opcional del marco.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

FrameworkName

El nombre único de un marco.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

Un marco consta de uno o varios controles. Cada control rige un recurso, como los planes de copia de seguridad, las selecciones de copia de seguridad, los almacenes de copia de seguridad o los puntos de recuperación. También puede activar o desactivar la grabación de AWS Config para cada recurso. Los estados son:

- `ACTIVE` cuando la grabación está activada para todos los recursos regidos por el marco.
- `PARTIALLY_ACTIVE` cuando la grabación está desactivada para al menos un recurso regido por el marco.
- `INACTIVE` cuando la grabación está desactivada para todos los recursos regidos por el marco.
- `UNAVAILABLE`cuando AWS Backup no puede validar el estado de la grabación en este momento.

Tipo: cadena

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `DescribeFrameworkOutput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeGlobalSettings

Servicio: AWS Backup

Describe si la AWS cuenta está habilitada para la copia de seguridad multicuenta. Devuelve un error si la cuenta no forma parte de una organización de Organizations. Ejemplo: `describe-global-settings --region us-west-2`

Sintaxis de la solicitud

```
GET /global-settings HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GlobalSettings

El estado del indicador `isCrossAccountBackupEnabled`.

Tipo: mapa de cadena a cadena

LastUpdateTime

La fecha y hora en que se actualizó por última vez el indicador `isCrossAccountBackupEnabled`. Esta actualización está en formato Unix y horario universal coordinado (UTC). El valor de `LastUpdateTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeProtectedResource

Servicio: AWS Backup

Devuelve información sobre un recurso guardado, incluida la última vez que se realizó una copia de seguridad, su nombre de recurso de Amazon (ARN) y el tipo de AWS servicio del recurso guardado.

Sintaxis de la solicitud

```
GET /resources/resourceArn HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LastBackupTime

La fecha y la hora en que se realizó la última una copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de `LastBackupTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

LastBackupVaultArn

El ARN (Amazon Resource Name) del almacén de copias de seguridad que contiene el punto de recuperación de copias de seguridad más reciente.

Tipo: cadena

LastRecoveryPointArn

El ARN (Amazon Resource Name) del punto de recuperación más reciente.

Tipo: cadena

LatestRestoreExecutionTimeMinutes

El tiempo, en minutos, que tardó en completarse el trabajo de restauración más reciente.

Tipo: largo

LatestRestoreJobCreationDate

La fecha de creación del trabajo de restauración más reciente.

Tipo: marca temporal

LatestRestoreRecoveryPointCreationDate

La fecha en que se creó el punto de recuperación más reciente.

Tipo: marca temporal

ResourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

ResourceName

El nombre del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

ResourceType

El tipo de AWS recurso guardado como punto de recuperación; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeRecoveryPoint

Servicio: AWS Backup

Devuelve los metadatos asociados a un punto de recuperación, incluidos el ID, el estado, el cifrado y el ciclo de vida.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

El ID de cuenta del almacén de copias de seguridad especificado.

Patrón: `^[0-9]{12}$`

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupSizeInBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

BackupVaultArn

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

Un objeto `CalculatedLifecycle` que contiene las marcas temporales `MoveToColdStorageAt` y `DeleteAt`.

Tipo: objeto CalculatedLifecycle

CompletionDate

La fecha y la hora en que se completó un trabajo para crear un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CompositeMemberIdentifier

El identificador de un recurso dentro de un grupo compuesto, como un punto de recuperación anidado (secundario) que pertenece a una pila compuesta (principal). El ID se transfiere desde el ID lógico de una pila.

Tipo: cadena

CreatedBy

Contiene información de identificación sobre la creación de un punto de recuperación, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad utilizado para crearlo.

Tipo: objeto RecoveryPointCreator

CreationDate

La fecha y la hora en que se creó un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

EncryptionKeyArn

La clave de cifrado en el servidor utilizada para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

IsEncrypted

Un valor booleano que se devuelve como `TRUE` si el punto de recuperación especificado está cifrado o como `FALSE` si el punto de recuperación no está cifrado.

Tipo: Booleano

IsParent

Esto devuelve el valor booleano de que un punto de recuperación es un trabajo principal (compuesto).

Tipo: Booleano

LastRestoreTime

La fecha y hora en que se restauró por última vez un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `LastRestoreTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto Lifecycle

ParentRecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación principal (compuesto); por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

ResourceArn

Un ARN que identifica de forma exclusiva un recurso guardado. El formato del ARN depende del tipo de recurso.

Tipo: cadena

ResourceName

El nombre del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

ResourceType

El tipo de AWS recurso que se va a guardar como punto de recuperación; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

SourceBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el almacén de origen en el que se realizó la copia de seguridad original del recurso; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`. Si la recuperación se restaura en la misma AWS cuenta o región, este valor será. `null`

Tipo: cadena

Status

Un código de estado que especifica el estado del punto de recuperación.

`PARTIAL`el estado indica que no se AWS Backup pudo crear el punto de recuperación antes de que se cerrara la ventana de respaldo. Para aumentar el plazo de su plan de respaldo mediante

la API, consulte UpdateBackupPlan. También puede seleccionar y editar el plan de copia de seguridad mediante la consola para aumentar el periodo del plan de copia de seguridad.

`EXPIRED`El estado indica que el punto de recuperación ha superado su período de retención, pero AWS Backup carece de permiso o no puede eliminarlo por algún motivo. Para eliminar estos puntos de recuperación manualmente, consulte el Paso 3: elimine los puntos de recuperación en la sección Depuración de recursos de la Introducción.

El estado `STOPPED` se produce en una copia de seguridad continua cuando un usuario ha realizado alguna acción que provoca la desactivación de la copia de seguridad continua. Esto puede deberse a la eliminación de los permisos, a la desactivación del control de versiones, a la desactivación de los eventos a EventBridge los que se envían o a la desactivación de EventBridge las reglas establecidas por. AWS Backup

Para resolver el estado `STOPPED`, asegúrese de que todos los permisos solicitados estén en vigor y de que el control de versiones esté activado en el bucket de S3. Una vez que se cumplan estas condiciones, la siguiente instancia de una regla de copia de seguridad que se ejecute provocará la creación de un nuevo punto de recuperación continuo. No es necesario eliminar los puntos de recuperación con el estado STOPPED.

En el caso de SAP HANA en Amazon EC2, el estado `STOPPED` se debe a una acción del usuario, un error de configuración de la aplicación o a un error en la copia de seguridad. Para garantizar que las futuras copias de seguridad continuas se realicen correctamente, consulte el estado del punto de recuperación y consulte SAP HANA para obtener más información.

Tipo: cadena

Valores válidos: `COMPLETED | PARTIAL | DELETING | EXPIRED`

StatusMessage

Un mensaje de estado que explica el estado del punto de recuperación.

Tipo: cadena

StorageClass

Especifica la clase de almacenamiento del punto de recuperación. Los valores válidos son `WARM` o `COLD`.

Tipo: cadena

Valores válidos: `WARM | COLD | DELETED`

VaultType

El tipo de almacén en el que se almacena el punto de recuperación descrito.

Tipo: cadena

Valores válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeRegionSettings

Servicio: AWS Backup

Devuelve la configuración actual de suscripción del servicio para la región. Si la opción de servicio está habilitada para un servicio, AWS Backup intenta proteger los recursos de ese servicio en esta región cuando el recurso esté incluido en un plan de respaldo bajo demanda o programado. De no ser así, AWS Backup no intenta proteger los recursos de ese servicio en esta región.

Sintaxis de la solicitud

```
GET /account-settings HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ResourceTypeManagementPreference

Devuelve si administra AWS Backup completamente las copias de seguridad de un tipo de recurso.

Para conocer las ventajas de una AWS Backup administración completa, consulte AWS Backup Administración completa.

Para obtener una lista de los tipos de recursos y saber si cada uno de ellos admite una AWS Backup administración completa, consulte la tabla Disponibilidad de funciones por recurso.

Si`"DynamoDB":false`, puede habilitar la AWS Backup administración completa de las copias de seguridad de DynamoDB habilitando las funciones avanzadas de copia de seguridad AWS Backup de DynamoDB.

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

Los servicios junto con las preferencias de suscripción de la región.

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeReportJob

Servicio: AWS Backup

Devuelve los detalles asociados a la creación de un informe especificado por su `ReportJobId`.

Sintaxis de la solicitud

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportJobId

El identificador del trabajo de informes. Una única cadena cifrada en UTF-8, Unicode, generada aleatoriamente que tiene como máximo una longitud de 1024 bytes. El ID del trabajo de informes no se puede editar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
```

```
    }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ReportJob

La información sobre un trabajo de informe, incluidos sus tiempos de finalización y creación, el destino del informe, el identificador único del trabajo de informe, el nombre del recurso de Amazon (ARN), la plantilla del informe, el estado y el mensaje de estado.

Tipo: objeto ReportJob

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeReportPlan

Servicio: AWS Backup

Devuelve una lista de todos los planes de informes de un Cuenta de AWS y Región de AWS.

Sintaxis de la solicitud

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único de un plan de informes.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
         }
      }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ReportPlan

Devuelve detalles sobre el plan de informes especificado por su nombre. Estos detalles incluyen el nombre de recurso de Amazon (ARN) del plan de informes, la descripción, la configuración, el canal de entrega, el estado de implementación, la hora de creación y las últimas veces que se intentó ejecutar y se ejecutó correctamente.

Tipo: objeto ReportPlan

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DescribeRestoreJob

Servicio: AWS Backup

Devuelve los metadatos asociados a un trabajo de restauración especificado mediante un ID de trabajo.

Sintaxis de la solicitud

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

restoreJobId

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AccountId

Devuelve el ID de la cuenta a la que pertenece el trabajo de restauración.

Tipo: String

Patrón: `^[0-9]{12}$`

BackupSizeInBytes

El tamaño del recurso restaurado, en bytes.

Tipo: largo

CompletionDate

La fecha y la hora en que se completó un trabajo para restaurar un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de restauración.

Tipo: objeto RestoreJobCreator

CreatedResourceArn

El nombre de recurso de Amazon (ARN) del recurso creado por el trabajo de restauración.

El formato del ARN depende del tipo de recurso del que se ha hecho copia de seguridad.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó un trabajo de restauración, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

DeletionStatus

El estado de los datos generados por la prueba de restauración.

Tipo: cadena

Valores válidos: `DELETING | FAILED | SUCCESSFUL`

DeletionStatusMessage

Describe el estado de eliminación del trabajo de restauración.

Tipo: cadena

ExpectedCompletionTimeMinutes

La cantidad de tiempo en minutos que se espera que tarde un trabajo de restauración de un punto de recuperación.

Tipo: largo

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

PercentDone

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

RecoveryPointCreationDate

La fecha de creación del punto de recuperación creado por el trabajo de restauración especificado.

Tipo: marca temporal

ResourceType

Devuelve los metadatos asociados a un trabajo de restauración enumerados por tipo de recurso.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Tipo: cadena

Status

Código de estado que especifica el estado del trabajo que se inicia AWS Backup para restaurar un punto de recuperación.

Tipo: cadena

Valores válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

Un mensaje que muestra el estado de un trabajo para restaurar un punto de recuperación.

Tipo: cadena

ValidationStatus

El estado de la validación se ejecuta en el trabajo de restauración indicado.

Tipo: cadena

Valores válidos: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

Mensaje del estado.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

DependencyFailureException

Un AWS servicio o recurso dependiente devolvió un error al AWS Backup servicio y la acción no se pudo completar.

Código de estado HTTP: 500

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DisassociateRecoveryPoint

Servicio: AWS Backup

Elimina el punto de recuperación de copias de seguridad continuas especificado AWS Backup y transfiere el control de esa copia de seguridad continua al servicio de origen, como Amazon RDS. El servicio de origen seguirá creando y reteniendo copias de seguridad continuas según el ciclo de vida que haya especificado en su plan de copia de seguridad original.

No admite puntos de recuperación de copias de seguridad instantáneas.

Sintaxis de la solicitud

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre exclusivo de un AWS Backup almacén.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de AWS Backup recuperación.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

InvalidResourceStateException

AWS Backup ya está realizando una acción en este punto de recuperación. No es posible realizar la acción que ha solicitado hasta que finalice la primera acción. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DisassociateRecoveryPointFromParent

Servicio: AWS Backup

Esta acción dirigida a un punto de recuperación secundario (anidado) específico elimina la relación entre el punto de recuperación especificado y su punto de recuperación principal (compuesto).

Sintaxis de la solicitud

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico en el que se almacena el punto de recuperación secundario (anidado). Los almacenes de Backup se identifican con nombres que son exclusivos de la cuenta utilizada para crearlos y de la AWS región en la que se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

recoveryPointArn

El nombre del recurso de Amazon (ARN) que identifica de forma exclusiva el punto de recuperación secundario (anidado); por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ExportBackupPlanTemplate

Servicio: AWS Backup

Devuelve el plan de copia de seguridad especificado por el ID del plan como plantilla de copia de seguridad.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlanTemplateJson

El cuerpo de una plantilla de plan de copia de seguridad en formato JSON.

> **Note**
>
> Se trata de un documento JSON firmado que no se puede modificar antes de pasarlo a `GetBackupPlanFromJSON`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetBackupPlan

Servicio: AWS Backup

Devuelve los detalles del `BackupPlan` para el `BackupPlanId` especificado. Los detalles son el cuerpo de un plan de copia de seguridad en formato JSON, además de los metadatos del plan.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AdvancedBackupSettings

Contiene una lista de `BackupOptions` para cada tipo de recurso. La lista se rellena solo si se ha configurado la opción avanzada para el plan de copia de seguridad.

Tipo: matriz de objetos AdvancedBackupSetting

BackupPlan

Especifica el cuerpo de un plan de copia de seguridad. Incluye un `BackupPlanName` y uno o más conjuntos de `Rules`.

Tipo: objeto BackupPlan

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces.

Tipo: cadena

DeletionDate

La fecha y la hora en que se eliminó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `DeletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

LastExecutionDate

La última vez que se ejecutó este plan de respaldo. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de `LastExecutionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetBackupPlanFromJSON

Servicio: AWS Backup

Devuelve un documento JSON válido que especifica un plan de copia de seguridad o un error.

Sintaxis de la solicitud

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupPlanTemplateJson

Un documento del plan de copia de seguridad proporcionado por el cliente en formato JSON.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
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"
         }
      ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlan

Especifica el cuerpo de un plan de copia de seguridad. Incluye un `BackupPlanName` y uno o más conjuntos de `Rules`.

Tipo: objeto BackupPlan

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetBackupPlanFromTemplate

Servicio: AWS Backup

Devuelve la plantilla especificada por su `templateId` como plan de copia de seguridad.

Sintaxis de la solicitud

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

templateId

Identifica de forma exclusiva una plantilla de plan de copia de seguridad almacenada.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
         }
      ]
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlanDocument

Devuelve el cuerpo de un plan de copia de seguridad en función de la plantilla de destino, incluidos el nombre, las reglas y el almacén de copias de seguridad del plan.

Tipo: objeto BackupPlan

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

GetBackupSelection

Servicio: AWS Backup

Devuelve los metadatos de selección y un documento en formato JSON que especifica una lista de recursos asociados a un plan de copia de seguridad.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

selectionId

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

BackupSelection

Especifica el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: objeto BackupSelection

CreationDate

La fecha y la hora en que se creó la selección de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces.

Tipo: cadena

SelectionId

Identifica de forma única el cuerpo de una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetBackupVaultAccessPolicy

Servicio: AWS Backup

Devuelve el documento de política de acceso asociado al almacén de copias de seguridad indicado.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Policy

El documento de política de acceso al almacén de copias de seguridad en formato JSON.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetBackupVaultNotifications

Servicio: AWS Backup

Devuelve notificaciones de eventos para el almacén de copias de seguridad especificado.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

BackupVaultEvents

Una matriz de eventos que indica el estado de los trabajos para realizar copias de seguridad de recursos en el almacén de copia de seguridad.

Tipo: matriz de cadenas

Valores válidos: `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

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

Un ARN que identifica de forma exclusiva un tema de Amazon Simple Notification Service (Amazon SNS); por ejemplo, `arn:aws:sns:us-west-2:111122223333:MyTopic`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

GetLegalHold

Servicio: AWS Backup

Esta acción devuelve los detalles de una retención legal concreta. Los detalles son el cuerpo de una retención legal en formato JSON, además de los metadatos.

Sintaxis de la solicitud

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

legalHoldId

El identificador de la retención legal.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CancelDescription

El motivo de la eliminación de la retención legal.

Tipo: cadena

CancellationDate

La hora en que se canceló la suspensión legal.

Tipo: marca temporal

CreationDate

El momento en que se creó la retención legal.

Tipo: marca temporal

Description

La descripción de la retención legal.

Tipo: cadena

LegalHoldArn

El ARN marco para la retención legal especificada. El formato del ARN depende del tipo de recurso.

Tipo: cadena

LegalHoldId

El identificador de la retención legal.

Tipo: cadena

RecoveryPointSelection

Los criterios para asignar un conjunto de recursos, como los tipos de recursos o las bóvedas de respaldo.

Tipo: objeto RecoveryPointSelection

RetainRecordUntil

La fecha y la hora hasta las que se conserva el registro de retenciones legales.

Tipo: marca temporal

Status

El estado de la retención legal.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | CANCELING | CANCELED`

Title

El título de la retención legal.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetRecoveryPointRestoreMetadata

Servicio: AWS Backup

Devuelve un conjunto de pares clave-valor de metadatos que se utilizaron para crear la copia de seguridad.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

El ID de cuenta del almacén de copias de seguridad especificado.

Patrón: `^[0-9]{12}$`

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

ResourceType

El tipo de recurso del punto de recuperación.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreMetadata

El conjunto de pares clave-valor de metadatos que describen la configuración original del recurso del que se ha hecho una copia de seguridad. Estos valores varían en función del servicio que se esté restaurando.

Tipo: mapa de cadena a cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetRestoreJobMetadata

Servicio: AWS Backup

Esta solicitud devuelve los metadatos del trabajo de restauración especificado.

Sintaxis de la solicitud

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

restoreJobId

Se trata de un identificador único de un trabajo de restauración interno AWS Backup.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Metadata

Contiene los metadatos del trabajo de copia de seguridad especificado.

Tipo: mapa de cadena a cadena

RestoreJobId

Se trata de un identificador único de un trabajo de restauración interno AWS Backup.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetRestoreTestingInferredMetadata

Servicio: AWS Backup

Esta solicitud devuelve el conjunto mínimo de metadatos necesario para iniciar un trabajo de restauración con una configuración predeterminada segura. `BackupVaultName` y `RecoveryPointArn` son parámetros obligatorios. `BackupVaultAccountId` es un parámetro opcional.

Sintaxis de la solicitud

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

El ID de cuenta del almacén de copias de seguridad especificado.

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de Backup se identifican con nombres que son exclusivos de la cuenta utilizada para crearlos y de la AWS región en la que se crearon. Constan de letras minúsculas, números y guiones.

Obligatorio: sí

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

InferredMetadata

Es un mapa de cadenas de los metadatos inferidos de la solicitud.

Tipo: mapa de cadena a cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetRestoreTestingPlan

Servicio: AWS Backup

Devuelve los detalles del `RestoreTestingPlan` para el `RestoreTestingPlanName` especificado. Los detalles son el cuerpo de un plan de prueba de restauración en formato JSON, además de los metadatos del plan.

Sintaxis de la solicitud

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Nombre único obligatorio del plan de prueba de restauración.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

RestoreTestingPlan

Especifica el cuerpo de un plan de prueba de restauración. Incluye `RestoreTestingPlanName`.

Tipo: objeto RestoreTestingPlanForGet

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetRestoreTestingSelection

Servicio: AWS Backup

Devuelve RestoreTestingSelection, que muestra los recursos y elementos del plan de pruebas de restauración.

Sintaxis de la solicitud

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

Nombre único obligatorio del plan de prueba de restauración.

Obligatorio: sí

RestoreTestingSelectionName

Nombre único obligatorio de la selección de pruebas de restauración.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

RestoreTestingSelection

Nombre único de la selección de pruebas de restauración.

Tipo: objeto RestoreTestingSelectionForGet

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetSupportedResourceTypes

Servicio: AWS Backup

Devuelve los tipos AWS de recursos admitidos por AWS Backup.

Sintaxis de la solicitud

```
GET /supported-resource-types HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ResourceTypes

Contiene una cadena con los tipos de AWS recursos admitidos:

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (con compatibilidad con MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store (EBS)

- `EC2` para Amazon Elastic Compute Cloud
- `EFS` para Amazon Elastic File System
- `FSX` para Amazon FSx
- `Neptune` para Amazon Neptune
- `RDS` para Amazon Relational Database Service
- `Redshift` para Amazon Redshift
- `SAP HANA on Amazon EC2`para bases de datos SAP HANA en instancias de Amazon Elastic Compute Cloud
- `S3`para Amazon Simple Storage Service (Amazon S3)
- `Storage Gateway`para AWS Storage Gateway
- `Timestream` para Amazon Timestream
- `VirtualMachine`para máquinas virtuales VMware

Tipo: matriz de cadenas

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++

- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListBackupJobs

Servicio: AWS Backup

Devuelve una lista de los trabajos de copia de seguridad existentes para una cuenta autenticada durante los últimos 30 días. Para un periodo de tiempo más prolongado, considere la posibilidad de utilizar estas herramientas de monitorización.

Sintaxis de la solicitud

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ByAccountId

El ID de la cuenta desde la que se van a enumerar los trabajos. Devuelve solo los trabajos de copia de seguridad asociados al ID de cuenta especificado.

Si se usa desde una cuenta AWS Organizations de administración, la * transferencia devuelve todos los trabajos de la organización.

Patrón: `^[0-9]{12}$`

ByBackupVaultName

Devuelve solo los trabajos de copia de seguridad que se almacenarán en el almacén de copias de seguridad especificado. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

Devuelve solo los trabajos de copia de seguridad completados después de una fecha expresada en formato Unix y horario universal coordinado (UTC).

ByCompleteBefore

Devuelve solo los trabajos de copia de seguridad completados antes de una fecha expresada en formato Unix y horario universal coordinado (UTC).

ByCreatedAfter

Devuelve solo los trabajos de copia de seguridad que se crearon después de la fecha especificada.

ByCreatedBefore

Devuelve solo los trabajos de copia de seguridad que se crearon antes de la fecha especificada.

ByMessageCategory

Se trata de un parámetro opcional que se puede utilizar para filtrar los trabajos con un valor MessageCategory que coincida con el valor introducido.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `InvalidParameters`.

Vista Monitorización

El comodín (*) devuelve el recuento de todas las categorías de mensajes.

`AGGREGATE_ALL` suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

ByParentJobId

Se trata de un filtro para enumerar los trabajos secundarios (anidados) en función del ID del trabajo principal.

ByResourceArn

Devuelve solo los trabajos de copia de seguridad que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

ByResourceType

Devuelve únicamente los trabajos de copia de seguridad de los recursos especificados:

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (con compatibilidad con MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store (EBS)

- `EC2` para Amazon Elastic Compute Cloud
- `EFS` para Amazon Elastic File System
- `FSx` para Amazon FSx
- `Neptune` para Amazon Neptune
- `Redshift` para Amazon Redshift
- `RDS` para Amazon Relational Database Service
- `SAP HANA on Amazon EC2` para bases de datos de SAP HANA
- `Storage Gateway`para AWS Storage Gateway
- `S3` para Amazon S3
- `Timestream` para Amazon Timestream
- `VirtualMachine` para máquinas virtuales

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Devuelve solo los trabajos de copia de seguridad que se encuentran en el estado especificado.

`Completed with issues` es un estado que solo se encuentra en la consola de AWS Backup . En el caso de la API, este estado se refiere a los trabajos con un estado de `MessageCategory` y una `SUCCESS` con un valor distinto de `COMPLETED`; es decir, el estado se ha completado pero genera un mensaje de estado.

Para obtener el recuento de trabajos de `Completed with issues`, ejecute dos solicitudes GET y reste el segundo número, más pequeño:

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

Valores válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupJobs

Una matriz de estructuras que contiene metadatos sobre trabajos de copia de seguridad devueltos en formato JSON.

Tipo: matriz de objetos BackupJob

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListBackupJobSummaries

Servicio: AWS Backup

Es una solicitud de resumen de trabajos de copia de seguridad creados o en ejecución en los 30 últimos días. Puede incluir los parámetros AccountID, State,,, ResourceType MessageCategory AggregationPeriod MaxResults, NextToken o para filtrar los resultados.

Esta solicitud devuelve un resumen que contiene la región, la cuenta, el estado, ResourceType, MessageCategory StartTime EndTime, y el recuento de los trabajos incluidos.

Sintaxis de la solicitud

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccountId

Devuelve el recuento de trabajos de la cuenta especificada.

Si la solicitud se envía desde una cuenta de miembro o desde una cuenta que no forma parte de AWS Organizations, se devolverán los trabajos de la cuenta del solicitante.

Las cuentas raíz, de administrador y de administrador delegado pueden utilizar el valor ANY para devolver recuentos de trabajos de todas las cuentas de la organización.

AGGREGATE_ALL suma los recuentos de trabajos de todas las cuentas de la organización autenticada y, a continuación, devuelve la suma.

Patrón: ^[0-9]{12}$

AggregationPeriod

El período de entrega de los resultados devueltos.

- ONE_DAY- El recuento diario de trabajos de los 14 días anteriores.
- SEVEN_DAYS- El recuento total de trabajos de los 7 días anteriores.
- FOURTEEN_DAYS- El recuento total de trabajos de los 14 días anteriores.

Valores válidos: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Número máximo de elementos que se van a devolver.

El valor es un entero. El rango de valores aceptados está entre 1 y 500.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

MessageCategory

Este parámetro devuelve el recuento de trabajos de la categoría de mensajes especificada.

Ejemplos de cadenas aceptadas son `AccessDenied`, `Success` y `InvalidParameters`. Consulte Supervisión para ver una lista de MessageCategory las cadenas aceptadas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

`AGGREGATE_ALL` suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

ResourceType

Devuelve el recuento de trabajos del tipo de recurso especificado. Utilice `GetSupportedResourceTypes` de solicitud para obtener cadenas para los tipos de recursos compatibles.

El valor ANY devuelve el recuento de todos los tipos de recursos.

`AGGREGATE_ALL` suma los recuentos de trabajos de todos los tipos de recursos y devuelve la suma.

El tipo de AWS recurso del que se va a hacer una copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Este parámetro devuelve el recuento de los trabajos con el estado especificado.

El valor ANY devuelve el recuento de todos los estados.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de estados y devuelve la suma.

Completed with issues es un estado que solo se encuentra en la consola de AWS Backup . En el caso de la API, este estado se refiere a los trabajos con un estado de MessageCategory y una SUCCESS con un valor distinto de COMPLETED; es decir, el estado se ha completado pero genera un mensaje de estado. Para obtener el recuento de trabajos de Completed with issues, ejecute dos solicitudes GET y reste el segundo número, más pequeño:

¿OBTENER /audit/? backup-job-summaries AggregationPeriod=Catorce días&STATE=Completado

¿OBTENER /audit/? backup-job-summaries AggregationPeriodMessageCategory=CATORCEEN_DÍAS& =ÉXITO&ESTADO=Completado

Valores válidos: CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AggregationPeriod

El período de los resultados devueltos.

- ONE_DAY- El recuento diario de trabajos de los 14 días anteriores.
- SEVEN_DAYS- El recuento total de trabajos de los 7 días anteriores.
- FOURTEEN_DAYS- El recuento total de trabajos de los 14 días anteriores.

Tipo: cadena

BackupJobSummaries

La información resumida.

Tipo: matriz de objetos BackupJobSummary

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListBackupPlans

Servicio: AWS Backup

Muestra los planes de respaldo activos de la cuenta.

Sintaxis de la solicitud

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

IncludeDeleted

Un valor booleano con un valor predeterminado de `FALSE` que devuelve los planes de copia de seguridad eliminados si se establece en `TRUE`.

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlansList

Información sobre los planes de respaldo.

Tipo: matriz de objetos BackupPlansListMember

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListBackupPlanTemplates

Servicio: AWS Backup

Muestra las plantillas del plan de respaldo.

Sintaxis de la solicitud

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

El número máximo de artículos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlanTemplatesList

Una matriz de elementos de la lista de plantillas que contiene metadatos sobre las plantillas guardadas.

Tipo: matriz de objetos BackupPlanTemplatesListMember

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListBackupPlanVersions

Servicio: AWS Backup

Devuelve los metadatos de las versiones de sus planes de copia de seguridad, incluidos los nombres de recursos de Amazon (ARN), los ID de los planes de copia de seguridad, las fechas de creación y eliminación, los nombres de los planes y los ID de versión.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupPlanVersionsList

Una matriz de elementos de la lista de versiones que contiene metadatos sobre sus planes de copia de seguridad.

Tipo: matriz de objetos BackupPlansListMember

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

ListBackupSelections

Servicio: AWS Backup

Devuelve una matriz que contiene los metadatos de los recursos asociados al plan de copia de seguridad de destino.

Sintaxis de la solicitud

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

Identifica de forma única un plan de copia de seguridad.

Obligatorio: sí

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "BackupSelectionsList": [
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupSelectionsList

Una matriz de elementos de la lista de selección de copias de seguridad que contiene metadatos sobre cada recurso de la lista.

Tipo: matriz de objetos BackupSelectionsListMember

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListBackupVaults

Servicio: AWS Backup

Devuelve una lista de contenedores de almacenamiento de puntos de recuperación junto con información sobre ellos.

Sintaxis de la solicitud

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ByShared

Este parámetro ordenará la lista de almacenes por almacenes compartidos.

ByVaultType

Este parámetro ordenará la lista de almacenes por tipo de almacén.

Valores válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultList

Una matriz de miembros de la lista del almacén de copias de seguridad que contiene metadatos del almacén, como el nombre de recurso de Amazon (ARN), el nombre de visualización, la fecha de creación, el número de puntos de recuperación guardados y la información de cifrado si los recursos guardados en el almacén de copias de seguridad están cifrados.

Tipo: matriz de objetos BackupVaultListMember

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2

- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListCopyJobs

Servicio: AWS Backup

Devuelve los metadatos de los trabajos de copia.

Sintaxis de la solicitud

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ByAccountId

El ID de la cuenta desde la que se van a enumerar los trabajos. Devuelve solo los trabajos de copia asociados al ID de cuenta especificado.

Patrón: `^[0-9]{12}$`

ByCompleteAfter

Devuelve solo los trabajos de copia completados después de una fecha expresada en formato Unix y horario universal coordinado (UTC).

ByCompleteBefore

Devuelve solo los trabajos de copia completados antes de una fecha expresada en formato Unix y horario universal coordinado (UTC).

ByCreatedAfter

Devuelve solo los trabajos de copia que se crearon después de la fecha especificada.

ByCreatedBefore

Devuelve solo los trabajos de copia que se crearon antes de la fecha especificada.

ByDestinationVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de seguridad de origen desde el que realizar copias; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

ByMessageCategory

Se trata de un parámetro opcional que se puede utilizar para filtrar los trabajos con un valor MessageCategory que coincida con el valor introducido.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `INVALIDPARAMETERS`.

Consulte en Monitorización una lista de cadenas aceptadas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

`AGGREGATE_ALL` suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

ByParentJobId

Se trata de un filtro para enumerar los trabajos secundarios (anidados) en función del ID del trabajo principal.

ByResourceArn

Devuelve solo los trabajos de copia que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

ByResourceType

Devuelve únicamente los trabajos de copia de seguridad de los recursos especificados:

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (con compatibilidad con MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store (EBS)
- `EC2` para Amazon Elastic Compute Cloud
- `EFS` para Amazon Elastic File System
- `FSx` para Amazon FSx
- `Neptune` para Amazon Neptune
- `Redshift` para Amazon Redshift

- `RDS` para Amazon Relational Database Service
- `SAP HANA on Amazon EC2` para bases de datos de SAP HANA
- `Storage Gateway`para AWS Storage Gateway
- `S3` para Amazon S3
- `Timestream` para Amazon Timestream
- `VirtualMachine` para máquinas virtuales

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByState

Devuelve solo los trabajos de copia que se encuentran en el estado especificado.

Valores válidos: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva un MaxResults número de NextToken artículos, podrás devolver más artículos de tu lista empezando por la ubicación que indique el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CopyJobs

Una matriz de estructuras que contiene metadatos sobre trabajos de copia devueltos en formato JSON.

Tipo: matriz de objetos CopyJob

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el MaxResults número de NextToken artículos, podrás devolver más artículos de la lista empezando por la ubicación que indique el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python

- AWS SDK para Ruby V3

ListCopyJobSummaries

Servicio: AWS Backup

Esta solicitud obtiene una lista de trabajos de copia creados o en ejecución en los 30 últimos días. Puede incluir los parámetros AccountID, State,,, ResourceType MessageCategory AggregationPeriod MaxResults, NextToken o para filtrar los resultados.

Esta solicitud devuelve un resumen que contiene la región, la cuenta, el estado, RestourceType, MessageCategory StartTime EndTime, y el recuento de los trabajos incluidos.

Sintaxis de la solicitud

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccountId

Devuelve el recuento de trabajos de la cuenta especificada.

Si la solicitud se envía desde una cuenta de miembro o desde una cuenta que no forma parte de AWS Organizations, se devolverán los trabajos de la cuenta del solicitante.

Las cuentas raíz, de administrador y de administrador delegado pueden utilizar el valor ANY para devolver recuentos de trabajos de todas las cuentas de la organización.

AGGREGATE_ALL suma los recuentos de trabajos de todas las cuentas de la organización autenticada y, a continuación, devuelve la suma.

Patrón: `^[0-9]{12}$`

AggregationPeriod

El período para los resultados devueltos.

- ONE_DAY- El recuento diario de trabajos de los 14 días anteriores.
- SEVEN_DAYS- El recuento total de trabajos de los 7 días anteriores.

- FOURTEEN_DAYS- El recuento total de trabajos de los 14 días anteriores.

Valores válidos: ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

Este parámetro establece el número máximo de elementos que se van a devolver.

El valor es un entero. El rango de valores aceptados está entre 1 y 500.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

MessageCategory

Este parámetro devuelve el recuento de trabajos de la categoría de mensajes especificada.

Ejemplos de cadenas aceptadas son AccessDenied, Success y InvalidParameters. Consulte Supervisión para ver una lista de MessageCategory las cadenas aceptadas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos MaxResults, NextToken permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

ResourceType

Devuelve el recuento de trabajos del tipo de recurso especificado. Utilice GetSupportedResourceTypes de solicitud para obtener cadenas para los tipos de recursos compatibles.

El valor ANY devuelve el recuento de todos los tipos de recursos.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de recursos y devuelve la suma.

El tipo de AWS recurso del que se va a hacer una copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Este parámetro devuelve el recuento de los trabajos con el estado especificado.

El valor ANY devuelve el recuento de todos los estados.

AGGREGATE_ALL suma los recuentos de trabajos de todos los tipos de estados y devuelve la suma.

Valores válidos: `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AggregationPeriod

El período de los resultados devueltos.

- `ONE_DAY`- El recuento diario de trabajos de los 14 días anteriores.
- `SEVEN_DAYS`- El recuento total de trabajos de los 7 días anteriores.
- `FOURTEEN_DAYS`- El recuento total de trabajos de los 14 días anteriores.

Tipo: cadena

CopyJobSummaries

Esta declaración muestra un resumen que contiene la región, la cuenta, el estado ResourceType, MessageCategory, StartTime EndTime, y el recuento de los trabajos incluidos.

Tipo: matriz de objetos CopyJobSummary

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListFrameworks

Servicio: AWS Backup

Devuelve una lista de todos los marcos de un Cuenta de AWS y Región de AWS.

Sintaxis de la solicitud

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

El número de resultados deseados va de 1 a 1000. Opcional. Si no se especifica, la consulta devolverá 1 MB de datos.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
         "FrameworkName": "string",
```

```
            "NumberOfControls": number
        }
    ],
    "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Frameworks

Los marcos con detalles de cada marco, incluidos el nombre del marco, el nombre del recurso de Amazon (ARN), la descripción, el número de controles, la hora de creación y el estado de la implementación.

Tipo: matriz de objetos Framework

NextToken

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListLegalHolds

Servicio: AWS Backup

Esta acción devuelve metadatos sobre las retenciones legales activas y anteriores.

Sintaxis de la solicitud

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

LegalHolds

Se trata de una matriz de retenciones legales devueltas, tanto activas como anteriores.

Tipo: matriz de objetos LegalHold

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListProtectedResources

Servicio: AWS Backup

Devuelve una matriz de recursos de la que se realizó una copia de seguridad correcta AWS Backup, incluida la hora en que se guardó el recurso, el nombre de recurso de Amazon (ARN) del recurso y el tipo de recurso.

Sintaxis de la solicitud

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
```

```
            "LastBackupVaultArn": "string",
            "LastRecoveryPointArn": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string"
        }
    ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Results

Un conjunto de recursos del que se ha hecho una copia de seguridad correcta, AWS Backup incluyendo la hora en que se guardó el recurso, el nombre de recurso de Amazon (ARN) del recurso y el tipo de recurso.

Tipo: matriz de objetos ProtectedResource

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListProtectedResourcesByBackupVault

Servicio: AWS Backup

En esta solicitud se enumeran los recursos protegidos correspondientes a cada almacén de copias de seguridad.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

La lista de recursos protegidos por almacén de respaldo dentro de los almacenes que especifique por ID de cuenta.

Patrón: `^[0-9]{12}$`

backupVaultName

La lista de recursos protegidos por almacén de respaldo dentro de los almacenes que especifique por nombre.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Results

Estos son los resultados devueltos para la solicitud ListProtectedResourcesByBackupVault.

Tipo: matriz de objetos ProtectedResource

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRecoveryPointsByBackupVault

Servicio: AWS Backup

Devuelve información detallada sobre los puntos de recuperación almacenados en un almacén de copias de seguridad.

Sintaxis de la solicitud

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

BackupVaultAccountId

Este parámetro ordenará la lista de puntos de recuperación por ID de cuenta.

Patrón: `^[0-9]{12}$`

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

> **Note**
>
> Es posible que el nombre del almacén de copias de seguridad no esté disponible cuando un servicio compatible cree la copia de seguridad.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

ByBackupPlanId

Devuelve solo los puntos de recuperación que coinciden con el identificador del plan de copia de seguridad especificado.

ByCreatedAfter

Devuelve solo los puntos de recuperación que se crearon después de la marca de tiempo especificada.

ByCreatedBefore

Devuelve solo los puntos de recuperación que se crearon antes de la marca de tiempo especificada.

ByParentRecoveryPointArn

Devuelve solo los puntos de recuperación que coinciden con el nombre de recurso de Amazon (ARN) del punto de recuperación principal (compuesto) especificado.

ByResourceArn

Devuelve solo los puntos de recuperación que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

ByResourceType

Devuelve solo los puntos de recuperación que coinciden con el tipo o los tipos de recurso especificados.

- `Aurora` para Amazon Aurora
- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (con compatibilidad con MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store (EBS)
- `EC2` para Amazon Elastic Compute Cloud
- `EFS` para Amazon Elastic File System
- `FSx` para Amazon FSx
- `Neptune` para Amazon Neptune
- `Redshift` para Amazon Redshift
- `RDS` para Amazon Relational Database Service
- `SAP HANA on Amazon EC2` para bases de datos de SAP HANA
- `Storage Gateway`para AWS Storage Gateway
- `S3` para Amazon S3

- `Timestream` para Amazon Timestream
- `VirtualMachine` para máquinas virtuales

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

RecoveryPoints

Una matriz de objetos que contiene información detallada sobre los puntos de recuperación guardados en un almacén de copias de seguridad.

Tipo: matriz de objetos RecoveryPointByBackupVault

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2

- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRecoveryPointsByLegalHold

Servicio: AWS Backup

Esta acción devuelve los ARN (nombres de recursos de Amazon) de los puntos de recuperación de la retención legal especificada.

Sintaxis de la solicitud

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

legalHoldId

El identificador de la retención legal.

Obligatorio: sí

MaxResults

Número máximo de elementos de la lista de recursos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos.

Tipo: cadena

RecoveryPoints

Los puntos de recuperación.

Tipo: matriz de objetos RecoveryPointMember

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRecoveryPointsByResource

Servicio: AWS Backup

La información sobre los puntos de recuperación del tipo especificado por un Amazon Resource Name (ARN) de un recurso.

> **Note**
>
> Para Amazon EFS y Amazon EC2, esta acción solo muestra los puntos de recuperación creados por AWS Backup.

Sintaxis de la solicitud

```
GET /resources/resourceArn/recovery-points/?
managedByAWSBackupOnly=ManagedByAWSBackupOnly&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ManagedByAWSBackupOnly

Este atributo filtra los puntos de recuperación en función de su propiedad.

Si se establece en`TRUE`, la respuesta contendrá los puntos de recuperación asociados a los recursos seleccionados gestionados por AWS Backup.

Si se establece en`FALSE`, la respuesta contendrá todos los puntos de recuperación asociados al recurso seleccionado.

Tipo: Booleano

MaxResults

Número máximo de elementos que se van a devolver.

> **Note**
>
> Amazon RDS requiere un valor mínimo de 20.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

resourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

RecoveryPoints

Una matriz de objetos que contiene información detallada sobre los puntos de recuperación del tipo de recurso especificado.

> **Note**
>
> Solo se devuelven los puntos de recuperación de Amazon EFS y Amazon EC2. BackupVaultName

Tipo: matriz de objetos RecoveryPointByResource

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListReportJobs

Servicio: AWS Backup

Devuelve detalles sobre sus trabajos de informes.

Sintaxis de la solicitud

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ByCreationAfter

Devuelve solo los trabajos de informes que se crearon después de la fecha y la hora especificadas en formato Unix y horario universal coordinado (UTC). Por ejemplo, el valor 1516925490 representa el viernes 26 de enero de 2018 a las 12:11:30 h

ByCreationBefore

Devuelve solo los trabajos de informes que se crearon antes de la fecha y la hora especificadas en formato Unix y horario universal coordinado (UTC). Por ejemplo, el valor 1516925490 representa el viernes 26 de enero de 2018 a las 12:11:30 h

ByReportPlanName

Devuelve solo los trabajos de informe con el nombre del plan de informes especificado.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

Devuelve solo los trabajos de informes que se encuentran en el estado especificado. Los estados son:

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

El número de resultados deseados va de 1 a 1000. Opcional. Si no se especifica, la consulta devolverá 1 MB de datos.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Tipo: cadena

ReportJobs

Detalles sobre sus trabajos de informes en formato JSON.

Tipo: matriz de objetos ReportJob

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListReportPlans

Servicio: AWS Backup

Devuelve una lista de los planes de informes. Para obtener información detallada sobre un plan de informes único, utilice `DescribeReportPlan`.

Sintaxis de la solicitud

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

El número de resultados deseados va de 1 a 1000. Opcional. Si no se especifica, la consulta devolverá 1 MB de datos.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
         }
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

Un identificador que se devolvió de la llamada anterior a esta operación, que se puede usar para devolver el siguiente conjunto de elementos de la lista.

Tipo: cadena

ReportPlans

El informe planifica con información detallada para cada plan. Esta información incluye el nombre de recurso de Amazon (ARN), el nombre del plan de informes, la descripción, la configuración, el canal de entrega, el estado de implementación, la hora de creación y las últimas veces que el plan de informes se intentó ejecutar y se ejecutó correctamente.

Tipo: matriz de objetos ReportPlan

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRestoreJobs

Servicio: AWS Backup

Devuelve una lista de los trabajos que AWS Backup se iniciaron para restaurar un recurso guardado, incluidos los detalles del proceso de recuperación.

Sintaxis de la solicitud

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ByAccountId

El ID de la cuenta desde la que se van a enumerar los trabajos. Devuelve solo los trabajos de restauración asociados al ID de cuenta especificado.

Patrón: `^[0-9]{12}$`

ByCompleteAfter

Devuelve solo los trabajos de copia completados después de una fecha expresada en formato Unix y horario universal coordinado (UTC).

ByCompleteBefore

Devuelve solo los trabajos de copia completados antes de una fecha expresada en formato Unix y horario universal coordinado (UTC).

ByCreatedAfter

Devuelve solo los trabajos de restauración que se crearon después de la fecha especificada.

ByCreatedBefore

Devuelve solo los trabajos de restauración que se crearon antes de la fecha especificada.

ByResourceType

Incluya este parámetro para devolver únicamente los trabajos de restauración de los recursos especificados:

- `Aurora` para Amazon Aurora

- `CloudFormation`para AWS CloudFormation
- `DocumentDB` para Amazon DocumentDB (con compatibilidad con MongoDB)
- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store (EBS)
- `EC2` para Amazon Elastic Compute Cloud
- `EFS` para Amazon Elastic File System
- `FSx` para Amazon FSx
- `Neptune` para Amazon Neptune
- `Redshift` para Amazon Redshift
- `RDS` para Amazon Relational Database Service
- `SAP HANA on Amazon EC2` para bases de datos de SAP HANA
- `Storage Gateway`para AWS Storage Gateway
- `S3` para Amazon S3
- `Timestream` para Amazon Timestream
- `VirtualMachine` para máquinas virtuales

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

ByRestoreTestingPlanArn

Devuelve solo los trabajos de restauración que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

ByStatus

Devuelve solo los trabajos de restauración asociados al estado de trabajo especificado.

Valores válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

RestoreJobs

Una matriz de objetos que contiene información detallada sobre los trabajos para restaurar los recursos guardados.

Tipo: matriz de objetos RestoreJobsListMember

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRestoreJobsByProtectedResource

Servicio: AWS Backup

Devuelve los trabajos de restauración que contienen el recurso protegido especificado.

Debe incluir `ResourceArn`. Opcionalmente, puede incluir `NextToken`, `ByStatus`, `MaxResults`, `ByRecoveryPointCreationDateAfter` y `ByRecoveryPointCreationDateBefore`.

Sintaxis de la solicitud

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

ByRecoveryPointCreationDateAfter

Devuelve solo los trabajos de restauración de puntos de recuperación que se crearon después de la fecha especificada.

ByRecoveryPointCreationDateBefore

Devuelve solo los trabajos de restauración de puntos de recuperación que se crearon antes de la fecha especificada.

ByStatus

Devuelve solo los trabajos de restauración asociados al estado de trabajo especificado.

Valores válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

resourceArn

Devuelve solo los trabajos de restauración que coinciden con el nombre de recurso de Amazon (ARN) del recurso especificado.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
      }
   ]
```

```
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token

Tipo: cadena

RestoreJobs

Una matriz de objetos que contiene información detallada sobre los trabajos para restaurar los recursos guardados.>

Tipo: matriz de objetos RestoreJobsListMember

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRestoreJobSummaries

Servicio: AWS Backup

Esta solicitud obtiene un resumen de los trabajos de restauración creados o en ejecución en los 30 últimos días. Puede incluir los parámetros AccountID, State,, ResourceType AggregationPeriod MaxResults, NextToken o para filtrar los resultados.

Esta solicitud devuelve un resumen que contiene la región, la cuenta, el estado, RestourceType, MessageCategory StartTime EndTime, y el recuento de los trabajos incluidos.

Sintaxis de la solicitud

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

AccountId

Devuelve el recuento de trabajos de la cuenta especificada.

Si la solicitud se envía desde una cuenta de miembro o una cuenta que no forma parte de AWS Organizations, se devolverán los trabajos de la cuenta del solicitante.

Las cuentas raíz, de administrador y de administrador delegado pueden utilizar el valor ANY para devolver recuentos de trabajos de todas las cuentas de la organización.

AGGREGATE_ALL suma los recuentos de trabajos de todas las cuentas de la organización autenticada y, a continuación, devuelve la suma.

Patrón: ^[0-9]{12}$

AggregationPeriod

El período para los resultados devueltos.

- ONE_DAY- El recuento diario de trabajos de los 14 días anteriores.
- SEVEN_DAYS- El recuento total de trabajos de los 7 días anteriores.

- `FOURTEEN_DAYS`- El recuento total de trabajos de los 14 días anteriores.

Valores válidos: `ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS`

MaxResults

Este parámetro establece el número máximo de elementos que se van a devolver.

El valor es un entero. El rango de valores aceptados está entre 1 y 500.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

ResourceType

Devuelve el recuento de trabajos del tipo de recurso especificado. Utilice `GetSupportedResourceTypes` de solicitud para obtener cadenas para los tipos de recursos compatibles.

El valor ANY devuelve el recuento de todos los tipos de recursos.

`AGGREGATE_ALL` suma los recuentos de trabajos de todos los tipos de recursos y devuelve la suma.

El tipo de AWS recurso del que se va a hacer una copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

State

Este parámetro devuelve el recuento de los trabajos con el estado especificado.

El valor ANY devuelve el recuento de todos los estados.

`AGGREGATE_ALL` suma los recuentos de trabajos de todos los tipos de estados y devuelve la suma.

Valores válidos: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AggregationPeriod

El período de los resultados devueltos.

- `ONE_DAY`- El recuento diario de trabajos de los 14 días anteriores.
- `SEVEN_DAYS`- El recuento total de trabajos de los 7 días anteriores.
- `FOURTEEN_DAYS`- El recuento total de trabajos de los 14 días anteriores.

Tipo: cadena

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

RestoreJobSummaries

Esta declaración contiene un resumen que incluye la región, la cuenta, el estado ResourceType, MessageCategory, StartTime EndTime, y el recuento de los trabajos incluidos.

Tipo: matriz de objetos RestoreJobSummary

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRestoreTestingPlans

Servicio: AWS Backup

Devuelve una lista de los planes de prueba de restauración.

Sintaxis de la solicitud

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
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
        }
    ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

RestoreTestingPlans

Es una lista devuelta de planes de prueba de restauración.

Tipo: matriz de objetos RestoreTestingPlanForList

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListRestoreTestingSelections

Servicio: AWS Backup

Devuelve una lista de selecciones de pruebas de restauración. Se puede filtrar por `MaxResults` y `RestoreTestingPlanName`.

Sintaxis de la solicitud

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

RestoreTestingPlanName

Devuelve las selecciones de pruebas de restauración por el nombre del plan de prueba de restauración especificado.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "NextToken": "string",
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

RestoreTestingSelections

Las selecciones de pruebas de restauración devueltas asociadas al plan de prueba de restauración.

Tipo: matriz de objetos RestoreTestingSelectionForList

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListTags

Servicio: AWS Backup

Devuelve las etiquetas asignadas al recurso, como un punto de recuperación de destino, un plan de respaldo o un almacén de respaldo.

`ListTags` solo funciona para los tipos de recursos que admiten la administración completa de AWS Backup de sus copias de seguridad. Estos tipos de recursos se muestran en la tabla Disponibilidad de funciones por recurso.

Sintaxis de la solicitud

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

MaxResults

Número máximo de elementos que se van a devolver.

Rango válido: valor mínimo de 1. Valor máximo de 1000.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

resourceArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso. Los objetivos válidos `ListTags` son los puntos de recuperación, los planes de copia de seguridad y los almacenes de copia de seguridad.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de elementos devueltos. Por ejemplo, si se solicita que se devuelva el número de elementos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: cadena

Tags

Información sobre las etiquetas.

Tipo: mapa de cadena a cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutBackupVaultAccessPolicy

Servicio: AWS Backup

Establece una política basada en recursos que se utiliza para administrar los permisos de acceso en el almacén de copias de seguridad de destino. Requiere un nombre de almacén de copias de seguridad y un documento de política de acceso en formato JSON.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Policy

El documento de política de acceso al almacén de copias de seguridad en formato JSON.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutBackupVaultLockConfiguration

Servicio: AWS Backup

Aplica AWS Backup Vault Lock a una bóveda de copias de seguridad, lo que impide los intentos de eliminar cualquier punto de recuperación almacenado o creado en una bóveda de copias de seguridad. El bloqueo de almacenes también impide los intentos de actualizar la política de ciclo de vida que controla el periodo de retención de cualquier punto de recuperación almacenado actualmente en un almacén de copias de seguridad. Si se especifica, el bloqueo de almacenes impone un periodo de retención mínimo y máximo a los futuros trabajos de copia y copia de seguridad que tengan como destino un almacén de copias de seguridad.

> **Note**
>
> AWS Backup Cohasset Associates ha evaluado el uso de Vault Lock en entornos sujetos a las normas SEC 17a-4, la CFTC y la FINRA. Para obtener más información sobre la relación de AWS Backup Vault Lock con estas normas, consulte la evaluación de conformidad de Cohasset Associates.

Para obtener más información, consulte Bloqueo de almacenes de AWS Backup.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

La configuración de AWS Backup Vault Lock que especifica el nombre de la bóveda de respaldo que protege.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

ChangeableForDays

La configuración de AWS Backup Vault Lock que especifica el número de días antes de la fecha de bloqueo. Por ejemplo, si se fija `ChangeableForDays` en 30 el 1 de enero de 2022 a las 20:00 UTC, la fecha de bloqueo será el 31 de enero de 2022 a las 20:00 UTC.

AWS Backup impone un período de reflexión de 72 horas antes de que Vault Lock entre en vigor y pase a ser inmutable. Por tanto, debe establecer `ChangeableForDays` a 3 o mayor.

Antes de la fecha de bloqueo, puede eliminar el bloqueo de almacenes mediante `DeleteBackupVaultLockConfiguration` o cambiar la configuración de este mediante `PutBackupVaultLockConfiguration`. A partir de la fecha de bloqueo, el bloqueo de almacenes pasa a ser inmutable y no se puede cambiar ni eliminar.

Si no se especifica este parámetro, puede eliminar el bloqueo de almacenes mediante `DeleteBackupVaultLockConfiguration` o cambiar la configuración del bloqueo de almacenes mediante `PutBackupVaultLockConfiguration` en cualquier momento.

Tipo: largo

Obligatorio: no

MaxRetentionDays

La configuración de AWS Backup Vault Lock que especifica el período máximo de retención durante el que el almacén conserva sus puntos de recuperación. Esta configuración puede resultar útil si, por ejemplo, las políticas de su organización requieren que destruya ciertos datos después de retenerlos durante cuatro años (1460 días).

Si no se incluye este parámetro, el bloqueo de almacenes no impone un periodo de retención máximo en los puntos de recuperación del almacén. Si este parámetro se incluye sin un valor, el bloqueo de almacenes no aplicará un periodo de retención máximo.

Si se especifica este parámetro, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o inferior al periodo de retención máximo. Si el periodo de retención del trabajo es superior a ese periodo de retención máximo, el almacén falla el trabajo de copia de seguridad o de copia de seguridad, y deberá modificar la configuración del ciclo de vida o utilizar un almacén diferente. El periodo de retención máximo más largo que puede especificar es de 36 500 días (aproximadamente 100 años). Los puntos de recuperación ya guardados en el almacén antes del bloqueo del almacén de no se ven afectados.

Tipo: largo

Obligatorio: no

MinRetentionDays

La configuración de AWS Backup Vault Lock que especifica el período mínimo de retención durante el que el almacén conserva sus puntos de recuperación. Esta configuración puede ser útil si, por ejemplo, las políticas de su organización requieren que se retengan ciertos datos durante al menos siete años (2555 días).

Este parámetro es obligatorio cuando se crea un bloqueo de almacén AWS CloudFormation; de lo contrario, este parámetro es opcional. Si no se especifica este parámetro, el bloqueo del almacén no impondrá un periodo mínimo de retención.

Si se especifica este parámetro, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o superior al periodo de retención mínimo. Si el periodo de retención del trabajo es más corto que ese periodo de retención mínimo, el almacén no supera ese trabajo de copia o copia, y debe modificar la configuración del ciclo de vida o usar un almacén diferente. El periodo de retención mínimo más corto que puede especificar es de 1 día. Los puntos de recuperación ya guardados en el almacén antes del bloqueo del almacén de no se ven afectados.

Tipo: largo

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutBackupVaultNotifications

Servicio: AWS Backup

Activa las notificaciones en un almacén de copias de seguridad para el tema y los eventos especificados.

Sintaxis de la solicitud

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupVaultEvents

Una matriz de eventos que indica el estado de los trabajos para realizar copias de seguridad de recursos en el almacén de copia de seguridad.

Para ver ejemplos de código y casos de uso comunes, consulte Uso de Amazon SNS para realizar un seguimiento AWS Backup de eventos.

Se admiten los siguientes eventos:

- `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 siguiente lista incluye tanto los eventos compatibles como los eventos obsoletos que ya no se utilizan (como referencia). Los eventos obsoletos no devuelven estados ni notificaciones. Consulte la lista anterior para ver los eventos compatibles.

Tipo: matriz de cadenas

Valores válidos: `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`

Obligatorio: sí

SNSTopicArn

El nombre de recurso de Amazon (ARN) que especifica el tema de los eventos de un almacén de copias de seguridad; por ejemplo, `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`.

Tipo: cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++

- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutRestoreValidationResult

Servicio: AWS Backup

Esta solicitud permite enviar los resultados de validación de pruebas de restauración independientes que se ejecutan automáticamente. `RestoreJobId` y `ValidationStatus` son obligatorios. Si lo desea, puede introducir un `ValidationStatusMessage`.

Sintaxis de la solicitud

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

restoreJobId

Se trata de un identificador único de un trabajo de restauración interno AWS Backup.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

ValidationStatus

El estado de la validación de la restauración.

Tipo: cadena

Valores válidos: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Obligatorio: sí

ValidationStatusMessage

Es una cadena de mensaje opcional que puede introducir para describir el estado de validación de la prueba de restauración.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 204
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StartBackupJob

Servicio: AWS Backup

Inicia un trabajo de copia de seguridad bajo demanda para el recurso especificado.

Sintaxis de la solicitud

```
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
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupOptions

La opción de copia de seguridad de un recurso seleccionado. Esta opción solo está disponible para los trabajos de copia de seguridad de Windows Volume Shadow Copy Service (VSS).

Valores válidos: configure `"WindowsVSS":"enabled"` para habilitar la opción de copia de seguridad de `WindowsVSS` y crear una copia de seguridad de Windows VSS. Configure `"WindowsVSS""disabled"` para crear una copia de seguridad normal. La opción `WindowsVSS` no está habilitada de forma predeterminada.

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

CompleteWindowMinutes

Un valor en minutos durante el cual debe completarse una copia de seguridad que se haya iniciado correctamente o, de lo contrario, AWS Backup cancelará el trabajo. Este valor es opcional. Este valor comienza la cuenta regresiva a partir del momento en que se programó la copia de seguridad. No agrega tiempo adicional para `StartWindowMinutes` o si la copia de seguridad se inició más tarde de lo programado.

Como `StartWindowMinutes`, este parámetro tiene un valor máximo de 100 años (52 560 000 minutos).

Tipo: largo

Obligatorio: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartBackupJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup realizará la transición y caducará las copias de seguridad automáticamente según el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Este parámetro tiene un valor máximo de 100 años (36 500 días).

Tipo: objeto Lifecycle

Obligatorio: no

RecoveryPointTags

Las etiquetas que se van a asignar a los recursos.

Tipo: mapa de cadena a cadena

Obligatorio: no

ResourceArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Obligatorio: sí

StartWindowMinutes

Un valor en minutos después del que una copia de seguridad está programada antes de que se cancele el trabajo si no se ha iniciado correctamente. El valor es opcional y el valor predeterminado es 8 horas. Si se incluye este valor, debe ser de al menos 60 minutos para evitar errores.

Este parámetro tiene un valor máximo de 100 años (52 560 000 minutos).

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado `CREATED` hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia a`RUNNING`) o hasta que el estado del trabajo cambie a `EXPIRED` (lo que se espera que ocurra cuando termine el tiempo de la ventana de inicio).

Tipo: largo

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupJobId

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

IsParent

Se trata de un valor booleano devuelto que indica que es un trabajo de copia de seguridad principal (compuesto).

Tipo: Booleano

RecoveryPointArn

Nota: Este campo solo se devuelve para los recursos avanzados de DynamoDB y Amazon EFS.

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StartCopyJob

Servicio: AWS Backup

Inicia un trabajo para crear una copia única del recurso especificado.

No admite copias de seguridad continuas.

Sintaxis de la solicitud

```
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"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

DestinationBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de seguridad de destino al que copiar; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Obligatorio: sí

IamRoleArn

Especifica el ARN del rol de IAM utilizado para copiar el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartCopyJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Lifecycle

Especifica el período de tiempo, en días, antes de que un punto de recuperación pase a almacenamiento en frío o se elimine.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, en la consola, la configuración de retención debe ser 90 días superior a la de transición a la configuración «frío después de días». La configuración de transición a frío después de varios días no se puede cambiar después de que una copia de seguridad haya pasado a estar fría.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y. `DeleteAfterDays`

Tipo: objeto Lifecycle

Obligatorio: no

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación que se usará en el trabajo de copia; por ejemplo, arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.

Tipo: cadena

Obligatorio: sí

SourceBackupVaultName

El nombre de un contenedor de origen lógico donde se almacenan las copias de seguridad. Los almacenes de Backup se identifican con nombres exclusivos de la cuenta utilizada para crearlos y de la AWS región en la que se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CopyJobId

Identifica de forma exclusiva un trabajo de copia.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el trabajo de copia, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

IsParent

Se trata de un valor booleano devuelto que indica que es un trabajo de copia principal (compuesto).

Tipo: Booleano

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StartReportJob

Servicio: AWS Backup

Inicia un trabajo de informes bajo demanda para el plan de informes especificado.

Sintaxis de la solicitud

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único de un plan de informes.

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartReportJobInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ReportJobId

El identificador del trabajo de informes. Una única cadena cifrada en UTF-8, Unicode, generada aleatoriamente que tiene como máximo una longitud de 1024 bytes. El ID del trabajo de informes no se puede editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StartRestoreJob

Servicio: AWS Backup

Recupera el recurso guardado identificado por un nombre de recurso de Amazon (ARN).

Sintaxis de la solicitud

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

CopySourceTagsToRestoredResource

Se trata de un parámetro opcional. Si es igual a `True`, las etiquetas incluidas en la copia de seguridad se copiarán en el recurso restaurado.

Esto solo se puede aplicar a las copias de seguridad creadas mediante AWS Backup.

Tipo: Booleano

Obligatorio: no

IamRoleArn

El nombre del recurso de Amazon (ARN) de la función de IAM que se AWS Backup utiliza para crear el recurso de destino; por ejemplo:. `arn:aws:iam::123456789012:role/S3Access`

Tipo: cadena

Requerido: no

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `StartRestoreJob` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Metadata

Un conjunto de pares clave-valor de metadatos.

Para obtener los metadatos de configuración de un recurso en el momento en que se realizó la copia de seguridad, solo tiene que llamar a `GetRecoveryPointRestoreMetadata`. Sin embargo, es posible que para restaurar un recurso se necesiten valores adicionales a los proporcionados por el recurso `GetRecoveryPointRestoreMetadata`. Por ejemplo, puede que tenga que proporcionar un nombre de recurso nuevo si el original ya existe.

Para obtener más información sobre los metadatos de cada recurso, consulte lo siguiente:

- Metadatos de Amazon Aurora
- Metadatos de Amazon DocumentDB
- Metadatos de AWS CloudFormation
- Metadatos de Amazon DynamoDB
- Metadatos para Amazon EBS
- Metadatos para Amazon EC2
- Metadatos para Amazon EFS
- Metadatos de Amazon FSx
- Metadatos de Amazon Neptune
- Metadatos para Amazon RDS
- Metadatos de Amazon Redshift
- Metadatos de AWS Storage Gateway

- Metadatos para Amazon S3
- Metadatos de Amazon Timestream
- Metadatos para máquinas virtuales

Tipo: mapa de cadena a cadena

Obligatorio: sí

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Obligatorio: sí

ResourceType

Inicia un trabajo para restaurar un punto de recuperación para uno de los siguientes recursos:

- `Aurora`- Amazon Aurora
- `DocumentDB`- Amazon DocumentDB
- `CloudFormation` - AWS CloudFormation
- `DynamoDB`- Amazon DynamoDB
- `EBS`- Tienda 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`- Máquinas virtuales

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

RestoreJobId

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StopBackupJob

Servicio: AWS Backup

Intenta cancelar un trabajo para crear una copia de seguridad única de un recurso.

Esta acción no es compatible con los siguientes servicios: Amazon FSx para Windows File Server, Amazon FSx para Lustre, Amazon FSx para ONTAP, Amazon NetApp FSx para OpenZFS, Amazon DocumentDB (compatible con MongoDB), Amazon RDS, Amazon Aurora y Amazon Neptune.

Sintaxis de la solicitud

```
POST /backup-jobs/backupJobId HTTP/1.1
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupJobId

AWS Backup Identifica de forma exclusiva una solicitud para hacer una copia de seguridad de un recurso.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud no tiene un cuerpo de la solicitud.

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

TagResource

Servicio: AWS Backup

Asigna un conjunto de pares clave-valor a un punto de recuperación, plan de copia de seguridad o almacén de copias de seguridad identificado por un nombre de recurso de Amazon (ARN).

Esta API es compatible con los puntos de recuperación de tipos de recursos, incluidos Aurora y Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune y Amazon RDS.

Sintaxis de la solicitud

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso etiquetado.

Los ARN que no lo incluyan son `backup` incompatibles con el etiquetado. `TagResource`y si `UntagResource` los ARN no son válidos, se producirá un error. El contenido de ARN aceptable puede incluir. `arn:aws:backup:us-east` El contenido del ARN no válido puede tener este aspecto. `arn:aws:ec2:us-east`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Tags

Pares clave-valor que se utiliza para ayudar a organizar los recursos. Puede asignar sus propios metadatos a los recursos que cree. Para mayor claridad, esta es la estructura para asignar etiquetas: `[{"Key":"string","Value":"string"}]`.

Tipo: mapa de cadena a cadena

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UntagResource

Servicio: AWS Backup

Elimina un conjunto de pares clave-valor de un punto de recuperación, plan de copia de seguridad o almacén de copias de seguridad identificado por un nombre de recurso de Amazon (ARN).

Esta API no es compatible con los puntos de recuperación de tipos de recursos, incluidos Aurora y Amazon DocumentDB. Amazon EBS, Amazon FSx, Neptune y Amazon RDS.

Sintaxis de la solicitud

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

resourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso etiquetado.

Los ARN que no lo incluyan son `backup` incompatibles con el etiquetado. `TagResource`y si `UntagResource` los ARN no son válidos, se producirá un error. El contenido de ARN aceptable puede incluir. `arn:aws:backup:us-east` El contenido del ARN no válido puede tener este aspecto. `arn:aws:ec2:us-east`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

TagKeyList

Las claves para identificar qué etiquetas clave-valor se deben eliminar de un recurso.

Tipo: matriz de cadenas

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateBackupPlan

Servicio: AWS Backup

Actualiza el plan de respaldo especificado. La nueva versión se identifica de forma exclusiva por su ID.

Sintaxis de la solicitud

```
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"
         }
      ]
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupPlanId

El ID del plan de respaldo.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

BackupPlan

El cuerpo de un plan de respaldo. Incluye un `BackupPlanName` y uno o más conjuntos de `Rules`.

Tipo: objeto BackupPlanInput

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
```

```
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

AdvancedBackupSettings

Contiene una lista de `BackupOptions` para cada tipo de recurso.

Tipo: matriz de objetos AdvancedBackupSetting

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

CreationDate

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateFramework

Servicio: AWS Backup

Actualiza el marco especificado.

Sintaxis de la solicitud

```
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"
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

frameworkName

El nombre único de un marco. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

FrameworkControls

Los controles que componen el marco. Cada control de la lista tiene un nombre, parámetros de entrada y alcance.

Tipo: matriz de objetos FrameworkControl

Obligatorio: no

FrameworkDescription

Una descripción opcional del marco con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `UpdateFrameworkInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "CreationTime": number,
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

Es la fecha y la hora en que se creó un marco con la norma ISO 8601. El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, 2020-07-10T15:00:00.000-08:00 representa el 10 de julio de 2020 a las 15:00 h, 8 horas menos que UTC.

Tipo: marca temporal

FrameworkArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

FrameworkName

El nombre único de un marco. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AlreadyExistsException

El recurso ya existe.

Código de estado HTTP: 400

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

LimitExceededException

Se ha superado un límite en la solicitud; por ejemplo, el número máximo de elementos permitidos en una solicitud.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateGlobalSettings

Servicio: AWS Backup

Actualiza si la AWS cuenta está habilitada para la copia de seguridad multicuenta. Devuelve un error si la cuenta no es una cuenta de administración de Organizations. Utilice la API `DescribeGlobalSettings` para determinar la configuración actual.

Sintaxis de la solicitud

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

GlobalSettings

Un valor para `isCrossAccountBackupEnabled` y una región. Ejemplo:`update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2`.

Tipo: mapa de cadena a cadena

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateRecoveryPointLifecycle

Servicio: AWS Backup

Establece el ciclo de vida de transferencia de un punto de recuperación.

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Esta operación no admite copias de seguridad continuas.

Sintaxis de la solicitud

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

backupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

recoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa al almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Tipo: objeto Lifecycle

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BackupVaultArn

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

CalculatedLifecycle

Un objeto `CalculatedLifecycle` que contiene las marcas temporales `MoveToColdStorageAt` y `DeleteAt`.

Tipo: objeto CalculatedLifecycle

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que

el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto Lifecycle

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

InvalidRequestException

Indica que hay algún problema con la entrada de la solicitud. Por ejemplo, un parámetro es del tipo incorrecto.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateRegionSettings

Servicio: AWS Backup

Actualiza la configuración actual de suscripción del servicio para la región.

Utilice la API `DescribeRegionSettings` para determinar los tipos de recursos compatibles.

Sintaxis de la solicitud

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

Parámetros de solicitud del URI

La solicitud no utiliza ningún parámetro de URI.

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

ResourceTypeManagementPreference

Habilita o deshabilita la AWS Backup administración completa de las copias de seguridad para un tipo de recurso. Para habilitar la AWS Backup administración completa de DynamoDB junto con las funciones avanzadas de copia de seguridad AWS Backup de DynamoDB, siga el procedimiento para habilitar la copia de seguridad avanzada de DynamoDB mediante programación.

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

ResourceTypeOptInPreference

Actualiza la lista de servicios junto con las preferencias de suscripción de la región.

Si las asignaciones de recursos se basan únicamente en etiquetas, se aplica la configuración de suscripción al servicio. Si un tipo de recurso se asigna explícitamente a un plan de copia de seguridad, como Amazon S3, Amazon EC2 o Amazon RDS, se incluirá en la copia de seguridad incluso si la suscripción no está habilitada para ese servicio en particular. Si en una asignación de recursos se especifican tanto el tipo de recurso como las etiquetas, el tipo de recurso especificado en el plan de copia de seguridad tiene prioridad sobre la condición de la etiqueta. En esta situación no se tiene en cuenta la configuración de suscripción al servicio.

Tipo: mapa de cadena a booleano

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los SDK específicos del idioma, consulte lo siguiente: AWS

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateReportPlan

Servicio: AWS Backup

Actualiza el plan de informes especificado.

Sintaxis de la solicitud

```
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"
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

reportPlanName

El nombre único del plan de informes. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

IdempotencyToken

Una cadena elegida por el cliente que puede utilizar para distinguir entre llamadas a `UpdateReportPlanInput` que, de otro modo, serían idénticas. Si se vuelve a intentar una solicitud correcta con el mismo token de idempotencia, aparece un mensaje de confirmación y no se realiza ninguna acción.

Tipo: cadena

Requerido: no

ReportDeliveryChannel

La información sobre dónde entregar los informes, específicamente el nombre del bucket de Amazon S3, el key prefijo de S3 y los formatos de los informes.

Tipo: objeto ReportDeliveryChannel

Obligatorio: no

ReportPlanDescription

Una descripción opcional del plan de informes con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

ReportSetting

La plantilla de informe para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

```
RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT |
BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT
```

Si la plantilla del informe es `RESOURCE_COMPLIANCE_REPORT` o`CONTROL_COMPLIANCE_REPORT`, este recurso de API también describe la cobertura del informe por marcos Regiones de AWS y marcos.

Tipo: objeto ReportSetting

Obligatorio: no

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La fecha y la hora en que se creó el plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

ReportPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

ReportPlanName

El nombre único del plan de informes.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateRestoreTestingPlan

Servicio: AWS Backup

Esta solicitud enviará los cambios al plan de prueba de restauración especificado. `RestoreTestingPlanName` no se puede actualizar después de crearlo.

`RecoveryPointSelection` puede contener:

- `Algorithm`
- `ExcludeVaults`
- `IncludeVaults`
- `RecoveryPointTypes`
- `SelectionWindowDays`

Sintaxis de la solicitud

```
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
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

El nombre del plan de pruebas de restauración.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

RestoreTestingPlan

Especifica el cuerpo de un plan de prueba de restauración.

Tipo: objeto RestoreTestingPlanForUpdate

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

Hora en que se creó el plan de pruebas de recursos.

Tipo: marca temporal

RestoreTestingPlanArn

ARN (Amazon Resource Name) único del plan de prueba de restauración.

Tipo: cadena

RestoreTestingPlanName

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

UpdateTime

La hora a la que se completó la actualización del plan de pruebas de restauración.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateRestoreTestingSelection

Servicio: AWS Backup

Actualiza la selección de pruebas de restauración especificada.

La mayoría de los elementos, salvo el `RestoreTestingSelectionName`, se pueden actualizar con esta solicitud.

Puede utilizar los ARN o las condiciones de los recursos protegidos, pero no ambos.

Sintaxis de la solicitud

```
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
   }
}
```

Parámetros de solicitud del URI

La solicitud utiliza los siguientes parámetros URI.

RestoreTestingPlanName

El nombre del plan de prueba de restauración es obligatorio para actualizar el plan de prueba indicado.

Obligatorio: sí

RestoreTestingSelectionName

El nombre de la selección de pruebas de restauración requerida de la selección de pruebas de restauración que desea actualizar.

Obligatorio: sí

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

RestoreTestingSelection

Para actualizar la selección de pruebas de restauración puede utilizar ARN de recursos protegidos o condiciones, pero no ambos. Es decir, si su selección tiene `ProtectedResourceArns`, no podrá solicitar una actualización con el parámetro `ProtectedResourceConditions`.

Tipo: objeto RestoreTestingSelectionForUpdate

Obligatorio: sí

Sintaxis de la respuesta

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
```

```
    "RestoreTestingSelectionName": "string",
    "UpdateTime": number
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

CreationTime

La hora en que la selección de pruebas de recursos se actualizó correctamente.

Tipo: marca temporal

RestoreTestingPlanArn

Cadena única que es el nombre del plan de prueba de restauración.

Tipo: cadena

RestoreTestingPlanName

El plan de pruebas de restauración al que está asociada la selección de pruebas de restauración actualizada.

Tipo: cadena

RestoreTestingSelectionName

El nombre de la selección de pruebas de restauración devuelta.

Tipo: cadena

UpdateTime

La hora a la que se completó la actualización de la selección de pruebas de restauración.

Tipo: marca temporal

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

AWS Backup no puede realizar la acción que ha solicitado hasta que termine de realizar una acción anterior. Inténtelo de nuevo más tarde.

Código de estado HTTP: 400

InvalidParameterValueException

Indica que hay algún problema con el valor de un parámetro. Por ejemplo, el valor está fuera del rango.

Código de estado HTTP: 400

MissingParameterValueException

Indica que falta un parámetro obligatorio.

Código de estado HTTP: 400

ResourceNotFoundException

No existe un recurso necesario para la acción.

Código de estado HTTP: 400

ServiceUnavailableException

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 500

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3

- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

AWS Backup gateway

AWS Backup gateway admiten las siguientes acciones:

- 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

Servicio: AWS Backup gateway

Asocia una puerta de enlace de copia de seguridad a su servidor. Tras completar el proceso de asociación, puede realizar copias de seguridad de sus máquinas virtuales y restaurarlas a través de la puerta de enlace.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la `ListGateways` operación para devolver una lista de pasarelas para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

ServerArn

El nombre de recurso de Amazon (ARN) del servidor que aloja la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de una puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

CreateGateway

Servicio: AWS Backup gateway

Crea una puerta de enlace de copia de seguridad. Después de crear una puerta de enlace, puede asociarla a un servidor mediante la operación `AssociateGatewayToServer`.

Sintaxis de la solicitud

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ActivationKey

La clave de activación de la puerta de enlace creada.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 50 caracteres.

Patrón: `^[0-9a-zA-Z\-]+$`

Obligatorio: sí

GatewayDisplayName

El nombre de visualización de la puerta de enlace creada.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: sí

GatewayType

El tipo de puerta de enlace creada.

Tipo: cadena

Valores válidos: `BACKUP_VM`

Obligatorio: sí

Tags

Una lista de hasta 50 etiquetas que se asignarán a la puerta de enlace. Cada etiqueta es un par clave-valor.

Tipo: matriz de objetos Tag

Obligatorio: no

Sintaxis de la respuesta

```
{
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que crea.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3

- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteGateway

Servicio: AWS Backup gateway

Elimina una puerta de enlace de copia de seguridad.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha eliminado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DeleteHypervisor

Servicio: AWS Backup gateway

Elimina un hipervisor.

Sintaxis de la solicitud

```
{
   "HypervisorArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor que se va a eliminar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "HypervisorArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor que ha eliminado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

DisassociateGatewayFromServer

Servicio: AWS Backup gateway

Disocia una puerta de enlace de copia de seguridad del servidor especificado. Una vez finalizado el proceso de disociación, la puerta de enlace ya no podrá acceder a las máquinas virtuales del servidor.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a disociar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha disociado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetBandwidthRateLimitSchedule

Servicio: AWS Backup gateway

Recupera la programación de límite de velocidad de ancho de banda de una puerta de enlace especificada. De forma predeterminada, las puertas de enlace no tienen una programación de límite de velocidad de ancho de banda, lo que significa que no hay ningún límite de velocidad de ancho de banda en vigor. Use esto para obtener la programación de límite de velocidad de ancho de banda de una puerta de enlace.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la ListGatewaysoperación para devolver una lista de pasarelas para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "BandwidthRateLimitIntervals": [
      {
```

```
            "AverageUploadRateLimitInBitsPerSec": number,
            "DaysOfWeek": [ number ],
            "EndHourOfDay": number,
            "EndMinuteOfHour": number,
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
        }
    ],
    "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

BandwidthRateLimitIntervals

Una matriz que contiene los intervalos de programación de límite de velocidad de ancho de banda para una puerta de enlace. Cuando no se ha programado ningún intervalo de límite de velocidad de ancho de banda, la matriz está vacía.

Tipo: matriz de objetos BandwidthRateLimitInterval

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 20 artículos.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la ListGatewaysoperación para devolver una lista de pasarelas para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetGateway

Servicio: AWS Backup gateway

Al proporcionar el ARN (nombre de recurso de Amazon), esta API devuelve la puerta de enlace.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
```

```
            "DayOfWeek": number,
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Gateway

Al proporcionar el ARN (nombre de recurso de Amazon), esta API devuelve la puerta de enlace.

Tipo: objeto GatewayDetails

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetHypervisor

Servicio: AWS Backup gateway

Esta acción solicita información sobre el hipervisor especificado al que se conectará la puerta de enlace. Un hipervisor es un hardware, software o firmware que crea y administra máquinas virtuales y les asigna recursos.

Sintaxis de la solicitud

```
{
   "HypervisorArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
```

```
        "LatestMetadataSyncStatus": "string",
        "LatestMetadataSyncStatusMessage": "string",
        "LogGroupArn": "string",
        "Name": "string",
        "State": "string"
    }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Hypervisor

Detalles sobre el hipervisor solicitado.

Tipo: objeto HypervisorDetails

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetHypervisorPropertyMappings

Servicio: AWS Backup gateway

Esta acción recupera las asignaciones de propiedades del hipervisor especificado. Un mapeo de propiedades de hipervisor muestra la relación entre las propiedades de la entidad disponibles en el hipervisor y las propiedades disponibles en. AWS

Sintaxis de la solicitud

```
{
   "HypervisorArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
```

```
            "VmwareCategory": "string",
            "VmwareTagName": "string"
        }
    ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

Esta es una visualización de las asignaciones de las etiquetas de VMware a las etiquetas de AWS .

Tipo: matriz de objetos VmwareToAwsTagMapping

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

GetVirtualMachine

Servicio: AWS Backup gateway

Al proporcionar el ARN (nombre de recurso de Amazon), esta API devuelve la máquina virtual.

Sintaxis de la solicitud

```
{
   "ResourceArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ResourceArn

El nombre de recurso de Amazon (ARN) de la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
```

```
            {
               "VmwareCategory": "string",
               "VmwareTagDescription": "string",
               "VmwareTagName": "string"
            }
         ]
      }
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

VirtualMachine

Este objeto contiene los atributos básicos de las `VirtualMachine` contenidas en el resultado de `GetVirtualMachine`

Tipo: objeto VirtualMachineDetails

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ImportHypervisorConfiguration

Servicio: AWS Backup gateway

Conéctese a un hipervisor importando su configuración.

Sintaxis de la solicitud

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Host

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: `^.+$`

Obligatorio: sí

KmsKeyArn

El AWS Key Management Service para el hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obligatorio: no

Name

El nombre del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: sí

Password

La contraseña del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[ -~]+$`

Obligatorio: no

Tags

Las etiquetas de configuración del hipervisor que se van a importar.

Tipo: matriz de objetos Tag

Obligatorio: no

Username

El nombre de usuario del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "HypervisorArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor que ha disociado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListGateways

Servicio: AWS Backup gateway

Enumera las puertas de enlace de respaldo propiedad de un Cuenta de AWS en un Región de AWS. La lista obtenida se ordena por el nombre de recurso de Amazon (ARN) de la gateway.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

El número máximo de puertas de enlace que se van a enumerar.

Tipo: entero

Rango válido: valor mínimo de 1.

Obligatorio: no

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `MaxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `^.+$`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Gateways

Una lista de sus puertas de enlace.

Tipo: matriz de objetos Gateway

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `^.+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListHypervisors

Servicio: AWS Backup gateway

Enumera los hipervisores.

Sintaxis de la solicitud

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

MaxResults

El número máximo de hipervisores que se van a enumerar.

Tipo: entero

Rango válido: valor mínimo de 1.

Obligatorio: no

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `^.+$`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Hypervisors

Una lista de sus objetos `Hypervisor`, ordenados por sus nombres de recurso de Amazon (ARN).

Tipo: matriz de objetos Hypervisor

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `^.+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListTagsForResource

Servicio: AWS Backup gateway

Enumera las etiquetas aplicadas al recurso identificado por su nombre de recurso de Amazon (ARN).

Sintaxis de la solicitud

```
{
   "ResourceArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ResourceArn

El nombre de recurso de Amazon (ARN) de las etiquetas del recurso a enumerar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ResourceArn

El nombre de recurso de Amazon (ARN) de las etiquetas del recurso que ha enumerado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

Una lista de las etiquetas del recurso.

Tipo: matriz de objetos Tag

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

ListVirtualMachines

Servicio: AWS Backup gateway

Enumera sus máquinas virtuales.

Sintaxis de la solicitud

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor conectado a la máquina virtual.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: no

MaxResults

El número máximo de máquinas virtuales que se van a enumerar.

Tipo: entero

Rango válido: valor mínimo de 1.

Obligatorio: no

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `^.+$`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

NextToken

El siguiente elemento que sigue a una lista parcial de recursos devueltos. Por ejemplo, si se solicita que se devuelva el número de recursos `maxResults`, `NextToken` permite devolver más elementos de la lista empezando por la ubicación indicada por el siguiente token.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1000 caracteres.

Patrón: `^.+$`

VirtualMachines

Una lista de sus objetos `VirtualMachine`, ordenados por sus nombres de recurso de Amazon (ARN).

Tipo: matriz de objetos VirtualMachine

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS

- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutBandwidthRateLimitSchedule

Servicio: AWS Backup gateway

Esta acción establece la programación de límite de velocidad de ancho de banda para una puerta de enlace especificada. De forma predeterminada, las puertas de enlace no tienen una programación de límite de velocidad de ancho de banda, lo que significa que no hay ningún límite de velocidad de ancho de banda en vigor. Use esto para iniciar la programación de límite de velocidad de ancho de banda de una puerta de enlace.

Sintaxis de la solicitud

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

BandwidthRateLimitIntervals

Una matriz que contiene los intervalos de programación de límite de velocidad de ancho de banda para una puerta de enlace. Cuando no se ha programado ningún intervalo de límite de velocidad de ancho de banda, la matriz está vacía.

Tipo: matriz de objetos BandwidthRateLimitInterval

Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 20 artículos.

Obligatorio: sí

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la ListGatewaysoperación para devolver una lista de pasarelas para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la ListGatewaysoperación para devolver una lista de pasarelas para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutHypervisorPropertyMappings

Servicio: AWS Backup gateway

Esta acción establece las asignaciones de propiedades del hipervisor especificado. Un mapeo de propiedades de hipervisor muestra la relación entre las propiedades de la entidad disponibles en el hipervisor y las propiedades disponibles en. AWS

Sintaxis de la solicitud

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 20. La longitud máxima es de 2048 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

Obligatorio: sí

VmwareToAwsTagMappings

Esta acción solicita la asignación de las etiquetas de VMware a las etiquetas de AWS .

Tipo: matriz de objetos VmwareToAwsTagMapping

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "HypervisorArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

PutMaintenanceStartTime

Servicio: AWS Backup gateway

Establece la hora de inicio del mantenimiento de una puerta de enlace.

Sintaxis de la solicitud

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

DayOfMonth

El día del mes de inicio del mantenimiento de una puerta de enlace.

Los valores válidos van de `Sunday` a `Saturday`.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 31.

Obligatorio: no

DayOfWeek

El día de la semana de inicio del mantenimiento de una puerta de enlace.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 6.

Obligatorio: no

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace, que se utiliza para especificar la hora de inicio del mantenimiento.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

HourOfDay

La hora del día de inicio del mantenimiento de una puerta de enlace.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

MinuteOfHour

El minuto de la hora de inicio del mantenimiento de una puerta de enlace.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de una puerta de enlace para la que haya establecido la hora de inicio del mantenimiento.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

StartVirtualMachinesMetadataSync

Servicio: AWS Backup gateway

Esta acción envía una solicitud para sincronizar los metadatos en las máquinas virtuales especificadas.

Sintaxis de la solicitud

```
{
   "HypervisorArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "HypervisorArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

TagResource

Servicio: AWS Backup gateway

Etiqueta el recurso.

Sintaxis de la solicitud

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ResourceARN

El nombre de recurso de Amazon (ARN) del recurso que se va a etiquetar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Tags

Una lista de etiquetas que se asignarán al recurso.

Tipo: matriz de objetos Tag

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ResourceARN": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ResourceARN

El nombre de recurso de Amazon (ARN) del recurso que ha etiquetado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

TestHypervisorConfiguration

Servicio: AWS Backup gateway

Prueba la configuración del hipervisor para validar que la puerta de enlace de copia de seguridad pueda conectarse con el hipervisor y sus recursos.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace al hipervisor que se va a probar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Host

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: `^.+$`

Obligatorio: sí

Password

La contraseña del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[ -~]+$`

Obligatorio: no

Username

El nombre de usuario del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200 con un cuerpo HTTP vacío.

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UntagResource

Servicio: AWS Backup gateway

Elimina etiquetas del recurso.

Sintaxis de la solicitud

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

ResourceARN

El nombre de recurso de Amazon (ARN) del recurso del que se van a eliminar etiquetas.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

TagKeys

La lista de claves de etiquetas que especifica las etiquetas que se van a eliminar.

Tipo: matriz de cadenas

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
   "ResourceARN": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

ResourceARN

El nombre de recurso de Amazon (ARN) del recurso del que ha eliminado etiquetas.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateGatewayInformation

Servicio: AWS Backup gateway

Actualiza el nombre de una puerta de enlace. Especifique la puerta de enlace que desea actualizar mediante el nombre de recurso de Amazon (ARN) de la puerta de enlace en su solicitud.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

GatewayDisplayName

El nombre de visualización actualizado de la puerta de enlace.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha actualizado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateGatewaySoftwareNow

Servicio: AWS Backup gateway

Esta operación actualiza el software de máquina virtual (VM) de la puerta de enlace. La solicitud activa inmediatamente la actualización del software.

> **Note**
>
> Al realizar esta solicitud, se obtiene inmediatamente una respuesta `200 OK` de confirmación. Sin embargo, es posible que la actualización tarde algún tiempo en completarse.

Sintaxis de la solicitud

```
{
   "GatewayArn": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que se va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

Sintaxis de la respuesta

```
{
```

```
   "GatewayArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace que ha actualizado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET
- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

UpdateHypervisor

Servicio: AWS Backup gateway

Actualiza los metadatos de un hipervisor, lo que incluye el host, el nombre de usuario y la contraseña. Especifique el hipervisor que desea actualizar mediante el nombre de recurso de Amazon (ARN) del hipervisor en su solicitud.

Sintaxis de la solicitud

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

Parámetros de la solicitud

Para obtener información sobre los parámetros comunes a todas las acciones, consulte Parámetros comunes.

La solicitud acepta los siguientes datos en formato JSON.

Host

El host actualizado del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: `^.+$`

Obligatorio: no

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor que se va a actualizar.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: sí

LogGroupArn

El nombre de recurso de Amazon (ARN) de grupo de puertas de enlace dentro del registro solicitado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Patrón: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Obligatorio: no

Name

El nombre actualizado del hipervisor

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

Password

La contraseña actualizada del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[ -~]+$`

Obligatorio: no

Username

El nombre de usuario actualizado del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[ -\.0-\[\]-~]*[!-\.0-\[\]-~][ -\.0-\[\]-~]*$`

Obligatorio: no

Sintaxis de la respuesta

```
{
   "HypervisorArn": "string"
}
```

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor que ha actualizado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Errores

Para obtener información acerca de los errores comunes a todas las acciones, consulte Errores comunes.

AccessDeniedException

La operación no puede continuar porque no tiene permisos suficientes.

Código de estado HTTP: 400

ConflictException

La operación no puede continuar porque no se admite.

Código de estado HTTP: 400

InternalServerException

La operación no se realizó correctamente porque se produjo un error interno. Inténtelo de nuevo más tarde.

Código de estado HTTP: 500

ResourceNotFoundException

No se encontró un recurso necesario para la acción.

Código de estado HTTP: 400

ThrottlingException

Las TPS se han limitado para proteger frente a altos volúmenes de solicitudes, intencionados o no.

Código de estado HTTP: 400

ValidationException

La operación no se realizó correctamente porque se produjo un error de validación.

Código de estado HTTP: 400

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- Interfaz de la línea de comandos de AWS
- AWS SDK para .NET

- AWS SDK para C++
- AWS SDK para Go v2
- AWS SDK para Java V2
- AWS SDK para JavaScript V3
- AWS SDK para PHP V3
- AWS SDK para Python
- AWS SDK para Ruby V3

Data Types

AWS Backup admite los siguientes tipos de datos:

- 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

AWS Backup gateway admite los siguientes tipos de datos:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

AWS Backup admite los siguientes tipos de datos:

- 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

Servicio: AWS Backup

Las opciones de copia de seguridad para cada tipo de recurso.

Contenido

BackupOptions

Especifica la opción de copia de seguridad para un recurso seleccionado. Esta opción solo está disponible para los trabajos de copia de seguridad de Windows VSS.

Valores válidos:

Configure `"WindowsVSS":"enabled"` para habilitar la opción de copia de seguridad de `WindowsVSS` y crear una copia de seguridad de Windows VSS.

Configure `"WindowsVSS":"disabled"` para crear una copia de seguridad normal. La opción `WindowsVSS` no está habilitada de forma predeterminada.

Si especifica una opción no válida, obtendrá una excepción `InvalidParameterValueException`.

Para obtener más información acerca de las copias de seguridad de Windows VSS, consulte Creación de una copia de seguridad de Windows habilitada para VSS.

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

ResourceType

Especifica un objeto que contiene diferentes opciones de tipos de recursos y copias de seguridad. El único tipo de recurso compatible son las instancias de Amazon EC2 con Windows Volume Shadow Copy Service (VSS). Para ver un CloudFormation ejemplo, consulte la CloudFormation plantilla de ejemplo para habilitar Windows VSS en la Guía del AWS Backup usuario.

Valores válidos: `EC2`.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupJob

Servicio: AWS Backup

Contiene información detallada acerca de un trabajo de copia de seguridad.

Contenido

AccountId

El ID de la cuenta a la que pertenece el trabajo de copia de seguridad.

Tipo: String

Patrón: `^[0-9]{12}$`

Obligatorio: no

BackupJobId

Identifica de forma exclusiva una solicitud para AWS Backup hacer una copia de seguridad de un recurso.

Tipo: cadena

Requerido: no

BackupOptions

Especifica la opción de copia de seguridad para un recurso seleccionado. Esta opción solo está disponible para los trabajos de copia de seguridad de Windows Volume Shadow Copy Service (VSS).

Valores válidos: configure `"WindowsVSS":"enabled"` para habilitar la opción de copia de seguridad de `WindowsVSS` y crear una copia de seguridad de Windows VSS. Configure `"WindowsVSS":"disabled"` para crear una copia de seguridad normal. Si especifica una opción no válida, obtendrá una excepción `InvalidParameterValueException`.

Tipo: mapa de cadena a cadena

Patrón de clave: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Patrón de valores: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

BackupSizeInBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

Obligatorio: no

BackupType

Representa el tipo de copia de seguridad de un trabajo de copia de seguridad.

Tipo: cadena

Requerido: no

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: no

BytesTransferred

El tamaño en bytes transferido a un almacén de copias de seguridad en el momento en que se consultó el estado del trabajo.

Tipo: largo

Obligatorio: no

CompletionDate

La fecha y la hora en que se completó un trabajo para crear un trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de copia de seguridad, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad utilizado para crearlo.

Tipo: objeto RecoveryPointCreator

Obligatorio: no

CreationDate

La fecha y la hora en que se creó el trabajo de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ExpectedCompletionDate

La fecha y la hora en que se espera completar un trabajo de copia de seguridad de recursos, en formato Unix y horario universal coordinado (UTC). El valor de `ExpectedCompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino. Los roles de IAM distintos del rol predeterminado deben incluir `AWSBackup` o `AwsBackup` en el nombre del rol. Por ejemplo, `arn:aws:iam::123456789012:role/AWSBackupRDSAccess`. Los nombres de los roles sin esas cadenas carecen de permisos para realizar trabajos de copia de seguridad.

Tipo: cadena

Requerido: no

InitiationDate

La fecha en la que se inició el trabajo de copia de seguridad.

Tipo: marca temporal

Obligatorio: no

IsParent

Se trata de un valor booleano que indica que es un trabajo de copia de seguridad principal (compuesto).

Tipo: Booleano

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `INVALIDPARAMETERS`. Consulte Supervisión para ver una lista de MessageCategory cadenas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

`AGGREGATE_ALL` suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

Tipo: cadena

Requerido: no

ParentJobId

Identifica de forma exclusiva una solicitud de AWS Backup para hacer una copia de seguridad de un recurso. Se devolverá el ID del trabajo principal (compuesto).

Tipo: cadena

Requerido: no

PercentDone

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

Requerido: no

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

ResourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso del que se va a hacer una copia de seguridad; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso admitido es Amazon EC2.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

StartBy

Especifica la hora en formato Unix y horario universal coordinado (UTC) en la que se debe iniciar un trabajo de copia de seguridad antes de que se cancele. El valor se calcula agregando el periodo de inicio a la hora programada. Por lo tanto, si la hora programada fueran las 18:00 h y el periodo de inicio fuera de 2 horas, la hora `StartBy` sería las 20:00 h en la fecha especificada. El valor de `StartBy` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

El estado actual de un trabajo de copia de seguridad.

Tipo: cadena

Valores válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

Obligatorio: no

StatusMessage

Un mensaje detallado que explica el estado del trabajo de copia de seguridad de un recurso.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupJobSummary

Servicio: AWS Backup

Es un resumen de los trabajos creados o en ejecución en los 30 últimos días.

El resumen devuelto puede contener lo siguiente: región, cuenta, estado RestourceType, MessageCategory, StartTime EndTime, y recuento de trabajos incluidos.

Contenido

AccountId

El ID de la cuenta propietaria de los trabajos del resumen.

Tipo: String

Patrón: `^[0-9]{12}$`

Obligatorio: no

Count

El valor expresado como número de trabajos en un resumen de trabajos.

Tipo: entero

Obligatorio: no

EndTime

El valor de hora en formato numérico de la hora de finalización de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser `AccessDenied`, `Success` y `InvalidParameters`. Consulte Supervisión para ver una lista de MessageCategory cadenas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

Tipo: cadena

Requerido: no

Region

Las AWS regiones incluidas en el resumen del trabajo.

Tipo: cadena

Requerido: no

ResourceType

Este valor es el recuento de trabajos para el tipo de recurso especificado. La solicitud GetSupportedResourceTypes devuelve cadenas para los tipos de recursos compatibles.

Tipo: String

Patrón: ^[a-zA-Z0-9\-_\.]{1,50}$

Obligatorio: no

StartTime

El valor de hora en formato numérico de la hora de inicio de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

Este valor es el recuento de trabajos con el estado especificado.

Tipo: cadena

Valores válidos: `CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupPlan

Servicio: AWS Backup

Contiene un nombre de visualización de plan de copia de seguridad opcional y una matriz de objetos `BackupRule`, cada uno de los cuales especifica una regla de copia de seguridad. Cada regla de un plan de copia de seguridad es una tarea programada independiente y puede hacer una copia de seguridad de una selección diferente de recursos de AWS .

Contenido

BackupPlanName

El nombre de visualización del plan de copia de seguridad. Debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Obligatorio: sí

Rules

Una matriz de objetos `BackupRule`, cada uno de los cuales especifica una tarea programada que se utiliza para realizar una copia de seguridad de una selección de recursos.

Tipo: matriz de objetos BackupRule

Obligatorio: sí

AdvancedBackupSettings

Contiene una lista de `BackupOptions` para cada tipo de recurso.

Tipo: matriz de objetos AdvancedBackupSetting

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

BackupPlanInput

Servicio: AWS Backup

Contiene un nombre de visualización de plan de copia de seguridad opcional y una matriz de objetos `BackupRule`, cada uno de los cuales especifica una regla de copia de seguridad. Cada regla de un plan de copia de seguridad es una tarea programada independiente.

Contenido

BackupPlanName

El nombre de visualización del plan de copia de seguridad. Debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Obligatorio: sí

Rules

Una matriz de objetos `BackupRule`, cada uno de los cuales especifica una tarea programada que se utiliza para realizar una copia de seguridad de una selección de recursos.

Tipo: matriz de objetos BackupRuleInput

Obligatorio: sí

AdvancedBackupSettings

Especifica una lista de `BackupOptions` para cada tipo de recurso. Esta configuración solo está disponible para los trabajos de copia de seguridad de Windows Volume Shadow Copy Service (VSS).

Tipo: matriz de objetos AdvancedBackupSetting

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupPlansListMember

Servicio: AWS Backup

Contiene metadatos sobre un plan de copia de seguridad.

Contenido

AdvancedBackupSettings

Contiene una lista de `BackupOptions` para un tipo de recurso.

Tipo: matriz de objetos AdvancedBackupSetting

Obligatorio: no

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

Requerido: no

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

Requerido: no

BackupPlanName

El nombre de visualización del plan de copia de seguridad guardado.

Tipo: cadena

Requerido: no

CreationDate

La fecha y la hora en que se creó el plan de copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de

milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

DeletionDate

La fecha y la hora en que se eliminó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `DeletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastExecutionDate

La última vez que se ejecutó este plan de respaldo. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de `LastExecutionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

VersionId

Cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. Los ID de versión no se pueden editar.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupPlanTemplatesListMember

Servicio: AWS Backup

Un objeto que especifica los metadatos asociados a una plantilla de plan de copia de seguridad.

Contenido

BackupPlanTemplateId

Identifica de forma exclusiva una plantilla de plan de copia de seguridad almacenada.

Tipo: cadena

Requerido: no

BackupPlanTemplateName

El nombre de visualización opcional de la plantilla de copia de seguridad.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupRule

Servicio: AWS Backup

Especifica una tarea programada utilizada para hacer una copia de seguridad de una selección de recursos.

Contenido

RuleName

Un nombre de visualización para una regla de copia de seguridad. Debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: sí

TargetBackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

CompletionWindowMinutes

Un valor en minutos después de que un trabajo de copia de seguridad se haya iniciado correctamente antes que AWS Backup deba completarlo o cancelarlo. Este valor es opcional.

Tipo: largo

Obligatorio: no

CopyActions

Una matriz de objetos `CopyAction`, que contiene los detalles de la operación de copia.

Tipo: matriz de objetos CopyAction

Obligatorio: no

EnableContinuousBackup

Especifica si AWS Backup crea copias de seguridad continuas. True hace AWS Backup que se creen copias de seguridad continuas con capacidad de point-in-time restauración (PITR). Si es falso (o no se ha especificado), AWS Backup se crean copias de seguridad instantáneas.

Tipo: Booleano

Obligatorio: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a un almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente de acuerdo con el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto Lifecycle

Obligatorio: no

RecoveryPointTags

Las etiquetas que se asignan a los recursos que están asociados a esta regla cuando se restauran desde una copia de seguridad.

Tipo: mapa de cadena a cadena

Obligatorio: no

RuleId

Identifica de forma exclusiva una regla que se utiliza para programar la copia de seguridad de una selección de recursos.

Tipo: cadena

Requerido: no

ScheduleExpression

Expresión cron en UTC que especifica cuándo se AWS Backup inicia un trabajo de copia de seguridad. Para obtener más información sobre las expresiones AWS cron, consulte Programar expresiones para reglas en la Guía del usuario de Amazon CloudWatch Events. . Dos ejemplos de expresiones AWS cron son `15 * ? * * *` (realizar una copia de seguridad cada hora 15 minutos después de la hora) y `0 12 * * ? *` (realizar una copia de seguridad todos los días a las 12 del mediodía UTC). Para ver una tabla de ejemplos, haga clic en el enlace anterior y desplácese hacia abajo en la página.

Tipo: cadena

Requerido: no

ScheduleExpressionTimezone

La zona horaria en la que se establece la expresión de programación. De forma predeterminada, ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowMinutes

Un valor en minutos después del que una copia de seguridad está programada antes de que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, debe ser de al menos 60 minutos para evitar errores.

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado `CREATED` hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia

aRUNNING) o hasta que el estado del trabajo cambie a EXPIRED (lo que se espera que ocurra cuando finalice el tiempo de la ventana de inicio).

Tipo: largo

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupRuleInput

Servicio: AWS Backup

Especifica una tarea programada utilizada para hacer una copia de seguridad de una selección de recursos.

Contenido

RuleName

Un nombre de visualización para una regla de copia de seguridad. Debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: sí

TargetBackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: sí

CompletionWindowMinutes

Un valor en minutos después de que un trabajo de copia de seguridad se haya iniciado correctamente antes que AWS Backup deba completarlo o cancelarlo. Este valor es opcional.

Tipo: largo

Obligatorio: no

CopyActions

Una matriz de objetos `CopyAction`, que contiene los detalles de la operación de copia.

Tipo: matriz de objetos CopyAction

Obligatorio: no

EnableContinuousBackup

Especifica si AWS Backup crea copias de seguridad continuas. True hace AWS Backup que se creen copias de seguridad continuas con capacidad de point-in-time restauración (PITR). Si es falso (o no se ha especificado), AWS Backup se crean copias de seguridad instantáneas.

Tipo: Booleano

Obligatorio: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a un almacenamiento en frío y cuándo caduca. AWS Backup realizará la transición y caducará las copias de seguridad automáticamente según el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. La configuración de «transición al almacenamiento en frío después de varios días» no se puede cambiar una vez que una copia de seguridad se haya transferido a almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Este parámetro tiene un valor máximo de 100 años (36 500 días).

Tipo: objeto Lifecycle

Obligatorio: no

RecoveryPointTags

Las etiquetas que se van a asignar a los recursos.

Tipo: mapa de cadena a cadena

Obligatorio: no

ScheduleExpression

Expresión CRON en UTC que especifica cuándo se AWS Backup inicia un trabajo de copia de seguridad.

Tipo: cadena

Requerido: no

ScheduleExpressionTimezone

La zona horaria en la que se establece la expresión de programación. De forma predeterminada, ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowMinutes

Un valor en minutos después del que una copia de seguridad está programada antes de que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, debe ser de al menos 60 minutos para evitar errores.

Este parámetro tiene un valor máximo de 100 años (52 560 000 minutos).

Durante el intervalo de inicio, el estado del trabajo de copia de seguridad permanece en ese estado `CREATED` hasta que comience correctamente o hasta que se agote el tiempo del intervalo de inicio. Si dentro de la ventana de inicio, Time AWS Backup recibe un error que permite volver a intentar el trabajo, AWS Backup volverá a intentarlo automáticamente al menos cada 10 minutos hasta que la copia de seguridad comience correctamente (el estado del trabajo cambia a`RUNNING`) o hasta que el estado del trabajo cambie a `EXPIRED` (lo que se espera que ocurra cuando finalice el tiempo de la ventana de inicio).

Tipo: largo

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupSelection

Servicio: AWS Backup

Se usa para especificar un conjunto de recursos para un plan de copia de seguridad.

Le recomendamos que especifique las condiciones, etiquetas o recursos que desee incluir o excluir. De lo contrario, Backup intentará seleccionar todos los recursos de almacenamiento admitidos y habilitados, lo que podría tener implicaciones de costos imprevistas.

Para obtener más información, consulte Asignación de recursos mediante programación.

Contenido

IamRoleArn

El ARN de la función de IAM que se AWS Backup utiliza para autenticarse al realizar una copia de seguridad del recurso de destino; por ejemplo,. `arn:aws:iam::123456789012:role/S3Access`

Tipo: cadena

Obligatorio: sí

SelectionName

El nombre de visualización de un documento de selección de recursos. Debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: sí

Conditions

Las condiciones que defina para asignar recursos a sus planes de respaldo mediante etiquetas. Por ejemplo, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true" }`.

`Conditions`admite `StringEquals``StringLike`,`StringNotEquals`, y`StringNotLike`. Los operadores de condición distinguen entre mayúsculas y minúsculas.

Si especifica varias condiciones, los recursos deben coincidir con todas las condiciones (lógica AND).

Tipo: objeto Conditions

Obligatorio: no

ListOfTags

Las condiciones que defina para asignar recursos a sus planes de respaldo mediante etiquetas. Por ejemplo, `"StringEquals": { "ConditionKey": "aws:ResourceTag/CreatedByCryo", "ConditionValue": "true"}`.

`ListOfTags`solo admite`StringEquals`. Los operadores de condición distinguen entre mayúsculas y minúsculas.

Si especifica varias condiciones, los recursos deben coincidir con cualquiera de las condiciones (lógica OR).

Tipo: matriz de objetos Condition

Obligatorio: no

NotResources

Los nombres de recursos de Amazon (ARN) de los recursos que se van a excluir de un plan de respaldo. El número máximo de ARN es 500 sin caracteres comodín o 30 ARN con caracteres comodín.

Si necesita excluir muchos recursos de un plan de copia de seguridad, considere una estrategia de selección de recursos diferente, como asignar solo uno o unos pocos tipos de recursos o refinar su selección de recursos utilizando etiquetas.

Tipo: matriz de cadenas

Obligatorio: no

Resources

Los nombres de recursos de Amazon (ARN) de los recursos que se van a asignar a un plan de respaldo. El número máximo de ARN es 500 sin caracteres comodín o 30 ARN con caracteres comodín.

Si necesita asignar muchos recursos a un plan de copia de seguridad, considere una estrategia de selección de recursos diferente, como asignar todos los recursos de un tipo de recurso o ajustar su selección de recursos mediante etiquetas.

Si especifica varios ARN, los recursos coinciden con creces con cualquiera de los ARN (lógica OR).

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupSelectionsListMember

Servicio: AWS Backup

Contiene metadatos sobre un objeto `BackupSelection`.

Contenido

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

Requerido: no

CreationDate

La fecha y la hora en que se creó el plan de copia de seguridad, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

IamRoleArn

Especifica el nombre de recurso de Amazon (ARN) del rol de IAM para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

SelectionId

Identifica de forma única una solicitud para asignar un conjunto de recursos a un plan de copia de seguridad.

Tipo: cadena

Requerido: no

SelectionName

El nombre de visualización de un documento de selección de recursos.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

BackupVaultListMember

Servicio: AWS Backup

Contiene metadatos sobre un almacén de copias de seguridad.

Contenido

BackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: no

CreationDate

La fecha y la hora en que se creó la copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatorRequestId

Una cadena única que identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

EncryptionKeyArn

Una clave de cifrado del lado del servidor que puede especificar para cifrar las copias de seguridad de los servicios que admiten la AWS Backup administración completa; por ejemplo,. `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` Si especifica una clave, debe especificar su ARN, no su alias. Si no especifica ninguna clave, AWS Backup crea una clave de KMS para usted de forma predeterminada.

Para saber qué AWS Backup servicios admiten la AWS Backup administración completa y cómo se AWS Backup gestiona el cifrado de las copias de seguridad de los servicios que aún no lo son AWS Backup, consulte Cifrado de copias de seguridad en AWS Backup

Tipo: cadena

Requerido: no

LockDate

La fecha y la hora en que la configuración de AWS Backup Vault Lock pasa a ser inmutable, lo que significa que no se puede cambiar ni eliminar.

Si ha aplicado el bloqueo de almacenes a su almacén sin especificar una fecha de bloqueo, puede cambiar la configuración del bloqueo de almacenes o eliminarlo del almacén por completo en cualquier momento.

Este valor está en formato Unix, horario universal coordinado (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

Locked

Un valor booleano que indica si AWS Backup Vault Lock se aplica al almacén de respaldo seleccionado. Si `true`, el bloqueo de almacenes impide las operaciones de eliminación y actualización en los puntos de recuperación del almacén seleccionado.

Tipo: Booleano

Obligatorio: no

MaxRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período máximo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo de almacenes no impone un periodo de retención máximo en los puntos de recuperación del almacén (lo que permite un almacenamiento indefinido).

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o inferior al periodo de retención máximo. Si el periodo de retención del trabajo es superior a ese periodo de retención máximo, el almacén falla el trabajo de copia de seguridad o de copia de seguridad, y deberá modificar la configuración del ciclo de vida o utilizar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

Obligatorio: no

MinRetentionDays

La configuración de bloqueo del AWS Backup almacén que especifica el período mínimo de retención durante el que el almacén conserva sus puntos de recuperación. Si no se especifica este parámetro, el bloqueo del almacén no impondrá un periodo mínimo de retención.

Si se especifica, cualquier trabajo de copia de seguridad o copia en el almacén debe tener una política de ciclo de vida con un periodo de retención igual o superior al periodo de retención mínimo. Si el periodo de retención del trabajo es más breve que ese periodo de retención mínimo, el almacén dará error en el trabajo de copia de seguridad o copia, y deberá modificar la configuración del ciclo de vida o usar un almacén diferente. Los puntos de recuperación ya almacenados en el almacén antes del bloqueo del mismo no se ven afectados.

Tipo: largo

Obligatorio: no

NumberOfRecoveryPoints

El número de puntos de recuperación que se almacenan en un almacén de copias de seguridad.

Tipo: largo

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CalculatedLifecycle

Servicio: AWS Backup

Contiene las marcas de tiempo `MoveToColdStorageAt` y `DeleteAt`, que se utilizan para especificar el ciclo de vida de un punto de recuperación.

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente según el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Contenido

DeleteAt

Una marca de tiempo que especifica cuándo se debe eliminar un punto de recuperación.

Tipo: marca temporal

Obligatorio: no

MoveToColdStorageAt

Una marca de tiempo que especifica cuándo se debe realizar la transferencia de un punto de recuperación al almacenamiento en frío.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Condition

Servicio: AWS Backup

Contiene una matriz de triplos compuesta por un tipo de condición (como `StringEquals`), una clave y un valor. Se utiliza para filtrar los recursos mediante sus etiquetas y asignarlos a un plan de copia de seguridad. Distingue mayúsculas de minúsculas.

Contenido

ConditionKey

La clave en un par de clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, la clave es `Department`.

Tipo: cadena

Obligatorio: sí

ConditionType

Una operación que se aplica a un par clave-valor que se utiliza para asignar recursos a su plan de copia de seguridad. La condición solo es compatible con `StringEquals`. Si desea opciones de asignación más flexibles, incluida `StringLike` y la posibilidad de excluir recursos de su plan de copia de seguridad, utilice `Conditions` (con una “s” al final) para su plan `BackupSelection`.

Tipo: cadena

Valores válidos: `STRINGEQUALS`

Obligatorio: sí

ConditionValue

El valor de un par clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, el valor es `Accounting`.

Tipo: cadena

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ConditionParameter

Servicio: AWS Backup

Incluye información sobre las etiquetas que se definen para asignar recursos etiquetados a un plan de copia de seguridad.

Incluye el prefijo `aws:ResourceTag` en tus etiquetas. Por ejemplo, `"aws:ResourceTag/TagKey1": "Value1"`.

Contenido

ConditionKey

La clave en un par de clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, la clave es `Department`.

Tipo: cadena

Requerido: no

ConditionValue

El valor de un par clave-valor. Por ejemplo, en la etiqueta `Department: Accounting`, el valor es `Accounting`.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Conditions

Servicio: AWS Backup

Contiene información acerca de los recursos que se deben incluir o excluir de un plan de copias de seguridad mediante sus etiquetas. Las condiciones distinguen entre mayúsculas y minúsculas.

Contenido

StringEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron con el mismo valor. También se denomina “coincidencia exacta”.

Tipo: matriz de objetos ConditionParameter

Obligatorio: no

StringLike

Filtra los valores de los recursos etiquetados para que coincidan con los valores de etiqueta mediante el uso de un caracter comodín (*) en cualquier parte de la cadena. Por ejemplo, “prod*” o “*rod*” coinciden con el valor de etiqueta “production”.

Tipo: matriz de objetos ConditionParameter

Obligatorio: no

StringNotEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron y que no tienen el mismo valor. También se denomina “coincidencia negada”.

Tipo: matriz de objetos ConditionParameter

Obligatorio: no

StringNotLike

Filtra los valores de los recursos etiquetados para detectar valores de etiqueta no coincidentes mediante el uso de un carácter comodín (*) en cualquier parte de la cadena.

Tipo: matriz de objetos ConditionParameter

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ControlInputParameter

Servicio: AWS Backup

Los parámetros de un control. Un control puede tener cero, uno o más parámetros. Un ejemplo de un control con dos parámetros es: “La frecuencia del plan de copia de seguridad es de al menos `daily` y el período de retención es de al menos `1 year`“. El primer parámetro es `daily`. El segundo parámetro es `1 year`.

Contenido

ParameterName

El nombre de un parámetro, por ejemplo, `BackupPlanFrequency`.

Tipo: cadena

Requerido: no

ParameterValue

El valor del parámetro, por ejemplo, `hourly`.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ControlScope

Servicio: AWS Backup

Un marco consta de uno o varios controles. Cada control tiene su propio alcance de control. El alcance de control puede incluir uno o varios tipos de recursos, una combinación de un valor y una clave de etiqueta, o una combinación de un tipo de recurso y un ID de recurso. Si no se especifica ningún alcance, las evaluaciones de la regla se activan cuando cambia la configuración de cualquier recurso del grupo de registro.

> **Note**
>
> Para establecer un alcance de control que incluya todo un recurso en particular, deje `ControlScope` vacío o no lo pase cuando llame a `CreateFramework`.

Contenido

ComplianceResourceIds

El ID del único AWS recurso que desea que contenga su ámbito de control.

Tipo: matriz de cadenas

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 100 artículos.

Obligatorio: no

ComplianceResourceTypes

Describe si el alcance de control incluye uno o más tipos de recursos, como `EFS` o `RDS`.

Tipo: matriz de cadenas

Obligatorio: no

Tags

El par clave-valor de etiquetas aplicado a los AWS recursos que desea activar la evaluación de una regla. Se puede proporcionar un máximo de un par de clave-valor. El valor de la etiqueta es opcional, pero no puede ser una cadena vacía si está creando o editando un marco desde la consola (aunque el valor puede ser una cadena vacía cuando se incluye en una CloudFormation plantilla).

La estructura para asignar una etiqueta es `[{"Key":"string","Value":"string"}]`.

Tipo: mapa de cadena a cadena

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CopyAction

Servicio: AWS Backup

Los detalles de la operación de copia.

Contenido

DestinationBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el almacén de copia de seguridad de destino para la copia de seguridad copiada. Por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Obligatorio: sí

Lifecycle

Especifica el período de tiempo, en días, antes de que un punto de recuperación pase a almacenamiento en frío o se elimine.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, en la consola, la configuración de retención debe ser 90 días superior a la de transición a la configuración «frío después de días». La configuración de transición a frío después de varios días no se puede cambiar después de que una copia de seguridad haya pasado a estar fría.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y. `DeleteAfterDays`

Tipo: objeto Lifecycle

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

CopyJob

Servicio: AWS Backup

Contiene información detallada acerca de un trabajo de copia.

Contenido

AccountId

El ID de la cuenta a la que pertenece el trabajo de copia.

Tipo: String

Patrón: `^[0-9]{12}$`

Obligatorio: no

BackupSizeInBytes

El tamaño de un trabajo de copia, en bytes.

Tipo: largo

Obligatorio: no

ChildJobsInState

Devuelve las estadísticas de los trabajos de copia secundarios (anidados) incluidos.

Tipo: mapa de cadena a largo

Claves válidas: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Obligatorio: no

CompletionDate

La fecha y la hora en que se completó el trabajo de copia, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CompositeMemberIdentifier

El identificador de un recurso dentro de un grupo compuesto, como un punto de recuperación anidado (secundario) que pertenece a una pila compuesta (principal). El ID se transfiere desde el ID lógico de una pila.

Tipo: cadena

Requerido: no

CopyJobId

Identifica de forma exclusiva un trabajo de copia.

Tipo: cadena

Requerido: no

CreatedBy

Contiene información sobre el plan de respaldo y la regla que AWS Backup se utilizaron para iniciar la copia de seguridad del punto de recuperación.

Tipo: objeto RecoveryPointCreator

Obligatorio: no

CreationDate

La fecha y la hora en que se creó el trabajo de copia, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

DestinationBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de seguridad de destino al que copiar; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

DestinationRecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación de destino; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para copiar el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

IsParent

Se trata de un valor booleano que indica que es un trabajo de copia principal (compuesto).

Tipo: Booleano

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser `AccessDenied`, `SUCCESS`, `AGGREGATE_ALL` y `InvalidParameters`. Consulte Supervisión para ver una lista de MessageCategory cadenas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

`AGGREGATE_ALL` suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma

Tipo: cadena

Requerido: no

NumberOfChildJobs

El número de trabajos de copia secundarios (anidados).

Tipo: largo

Obligatorio: no

ParentJobId

Identifica de forma exclusiva una solicitud de AWS Backup para hacer una copia de un recurso. Se devolverá el ID del trabajo principal (compuesto).

Tipo: cadena

Requerido: no

ResourceArn

El AWS recurso que se va a copiar; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso que se va a copiar; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS).

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

SourceBackupVaultArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un almacén de copias de origen; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

SourceRecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación de origen; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

State

El estado actual de un trabajo de copia.

Tipo: cadena

Valores válidos: `CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

Obligatorio: no

StatusMessage

Un mensaje detallado que explica el estado del trabajo de copia de un recurso.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

CopyJobSummary

Servicio: AWS Backup

Es un resumen de los trabajos de copia creados o en ejecución en los 30 últimos días.

El resumen devuelto puede contener lo siguiente: región, cuenta, estado RestourceType, MessageCategory, StartTime EndTime, y recuento de trabajos incluidos.

Contenido

AccountId

El ID de la cuenta propietaria de los trabajos del resumen.

Tipo: String

Patrón: `^[0-9]{12}$`

Obligatorio: no

Count

El valor expresado como número de trabajos en un resumen de trabajos.

Tipo: entero

Obligatorio: no

EndTime

El valor de hora en formato numérico de la hora de finalización de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

MessageCategory

Este parámetro es el recuento de trabajos de la categoría de mensajes especificada.

Las cadenas de ejemplo pueden ser `AccessDenied`, `Success` y `InvalidParameters`. Consulte Supervisión para ver una lista de MessageCategory cadenas.

El valor ANY devuelve el recuento de todas las categorías de mensajes.

AGGREGATE_ALL suma los recuentos de trabajos de todas las categorías de mensajes y devuelve la suma.

Tipo: cadena

Requerido: no

Region

Las AWS regiones incluidas en el resumen del trabajo.

Tipo: cadena

Requerido: no

ResourceType

Este valor es el recuento de trabajos para el tipo de recurso especificado. La solicitud GetSupportedResourceTypes devuelve cadenas para los tipos de recursos compatibles

Tipo: String

Patrón: ^[a-zA-Z0-9\-_\.]{1,50}$

Obligatorio: no

StartTime

El valor de hora en formato numérico de la hora de inicio de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

Este valor es el recuento de trabajos con el estado especificado.

Tipo: cadena

Valores válidos: `CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

DateRange

Servicio: AWS Backup

Este es un filtro de recursos que contiene FromDate: DateTime y ToDate: DateTime. Ambos valores son obligatorios. No se permiten DateTime valores futuros.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales). Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Contenido

FromDate

Este valor es la fecha de inicio, inclusive.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales).

Tipo: marca temporal

Obligatorio: sí

ToDate

Este valor es la fecha de finalización, inclusive.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales).

Tipo: marca temporal

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Framework

Servicio: AWS Backup

Contiene información detallada acerca de un marco. Los marcos contienen controles que evalúan e informan sobre sus eventos y recursos de copia de seguridad. Los marcos generan resultados de conformidad diarios.

Contenido

CreationTime

La fecha y la hora en que se creó un marco con la norma ISO 8601. El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, 2020-07-10T15:00:00.000-08:00 representa el 10 de julio de 2020 a las 15:00 h, 8 horas menos que UTC.

Tipo: marca temporal

Obligatorio: no

DeploymentStatus

El estado de implementación de un marco. Los estados son:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED`

Tipo: cadena

Requerido: no

FrameworkArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

FrameworkDescription

Una descripción opcional del marco con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

FrameworkName

El nombre único de un marco. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: no

NumberOfControls

El número de controles que contiene el marco.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

FrameworkControl

Servicio: AWS Backup

Contiene información detallada acerca de todos los controles de un marco. Cada marco debe contener al menos un control.

Contenido

ControlName

El nombre de un control. Este nombre tiene entre 1 y 256 caracteres.

Tipo: cadena

Obligatorio: sí

ControlInputParameters

Los pares nombre/valor.

Tipo: matriz de objetos ControlInputParameter

Obligatorio: no

ControlScope

El alcance de un control. El alcance del control define lo que evaluará el control. Tres ejemplos de alcance de control son: un plan de copia de seguridad específico, todos los planes de copia de seguridad con una etiqueta específica o todos los planes de copia de seguridad.

Para obtener más información, consulte `ControlScope.`

Tipo: objeto ControlScope

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

KeyValue

Servicio: AWS Backup

Par de dos cadenas relacionadas. Los caracteres permitidos son letras, espacios en blanco y números que se pueden representar en UTF-8, y los siguientes caracteres: `+ - = . _ : /`.

Contenido

Key

La clave de la etiqueta (cadena). La clave no pueden comenzar por `aws:`.

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$`

Tipo: cadena

Obligatorio: sí

Value

El valor de la clave.

Limitaciones de longitud: longitud máxima de 256.

Patrón: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Tipo: cadena

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

LegalHold

Servicio: AWS Backup

Una retención legal es una herramienta administrativa que ayuda a evitar que las copias de seguridad se eliminen mientras están retenidas. Mientras la retención esté en vigor, las copias de seguridad retenidas no se pueden eliminar y las políticas de ciclo de vida que podrían alterar el estado de las copias de seguridad (como la transferencia al almacenamiento en frío) se retrasan hasta que se elimine la retención legal. Una copia de seguridad puede tener más de una retención legal. Las retenciones legales se aplican a una o más copias de seguridad (también se conocen como puntos de recuperación). Estas copias de seguridad se pueden filtrar por tipos de recursos y por ID de recursos.

Contenido

CancellationDate

La hora en que se canceló la suspensión legal.

Tipo: marca temporal

Obligatorio: no

CreationDate

El momento en que se creó la retención legal.

Tipo: marca temporal

Obligatorio: no

Description

La descripción de una retención legal.

Tipo: cadena

Requerido: no

LegalHoldArn

El nombre del recurso de Amazon (ARN) de la retención legal; por ejemplo,. `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`

Tipo: cadena

Requerido: no

LegalHoldId

El identificador de la retención legal.

Tipo: cadena

Requerido: no

Status

El estado de la retención legal.

Tipo: cadena

Valores válidos: `CREATING | ACTIVE | CANCELING | CANCELED`

Obligatorio: no

Title

El título de una retención legal.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Lifecycle

Servicio: AWS Backup

Especifica el período de tiempo, en días, antes de que un punto de recuperación pase a almacenamiento en frío o se elimine.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, en la consola, la configuración de retención debe ser 90 días superior a la de transición a la configuración «frío después de días». La configuración de transición a frío después de varios días no se puede cambiar después de que una copia de seguridad haya pasado a estar fría.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Para eliminar el ciclo de vida y los períodos de retención existentes y conservar los puntos de recuperación indefinidamente, especifique -1 para `MoveToColdStorageAfterDays` y. `DeleteAfterDays`

Contenido

DeleteAfterDays

El número de días después de la creación en los que se elimina un punto de recuperación. Este valor debe ser al menos 90 días posterior al número de días especificado en`MoveToColdStorageAfterDays`.

Tipo: largo

Obligatorio: no

MoveToColdStorageAfterDays

El número de días transcurridos desde su creación hasta que un punto de recuperación se traslada a una cámara frigorífica.

Tipo: largo

Obligatorio: no

OptInToArchiveForSupportedResources

Si el valor es verdadero, su plan de respaldo transfiere los recursos compatibles a un nivel de almacenamiento de archivado (frío) de acuerdo con la configuración de su ciclo de vida.

Tipo: Booleano

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ProtectedResource

Servicio: AWS Backup

Estructura que contiene información sobre un recurso del que se ha hecho una copia de seguridad.

Contenido

LastBackupTime

La fecha y la hora en que se realizó la última una copia de seguridad de un recurso, en formato Unix y horario universal coordinado (UTC). El valor de `LastBackupTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastBackupVaultArn

El ARN (Amazon Resource Name) del almacén de copias de seguridad que contiene el punto de recuperación de copias de seguridad más reciente.

Tipo: cadena

Requerido: no

LastRecoveryPointArn

El ARN (Amazon Resource Name) del punto de recuperación más reciente.

Tipo: cadena

Requerido: no

ResourceArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso admitido es Amazon EC2.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ProtectedResourceConditions

Servicio: AWS Backup

Las condiciones que defina para los recursos en su plan de pruebas de restauración mediante etiquetas.

Por ejemplo, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Los operadores de condición distinguen entre mayúsculas y minúsculas.

Contenido

StringEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron con el mismo valor. También se denomina “coincidencia exacta”.

Tipo: matriz de objetos KeyValue

Obligatorio: no

StringNotEquals

Filtra los valores de los recursos etiquetados solo para aquellos recursos que se etiquetaron y que no tienen el mismo valor. También se denomina “coincidencia negada”.

Tipo: matriz de objetos KeyValue

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointByBackupVault

Servicio: AWS Backup

Contiene información detallada sobre los puntos de recuperación almacenados en un almacén de copias de seguridad.

Contenido

BackupSizeInBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

Obligatorio: no

BackupVaultArn

Un ARN que identifica de forma exclusiva un almacén de copias de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:backup-vault:aBackupVault`.

Tipo: cadena

Requerido: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: no

CalculatedLifecycle

Un objeto `CalculatedLifecycle` que contiene las marcas temporales `MoveToColdStorageAt` y `DeleteAt`.

Tipo: objeto CalculatedLifecycle

Obligatorio: no

CompletionDate

La fecha y la hora en que se completó un trabajo para restaurar un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CompositeMemberIdentifier

El identificador de un recurso dentro de un grupo compuesto, como un punto de recuperación anidado (secundario) que pertenece a una pila compuesta (principal). El ID se transfiere desde el ID lógico de una pila.

Tipo: cadena

Requerido: no

CreatedBy

Contiene información de identificación sobre la creación de un punto de recuperación, que incluye los valores de `BackupPlanArn`, `BackupPlanId`, `BackupPlanVersion` y `BackupRuleId` del plan de copia de seguridad que se utilizó para crearlo.

Tipo: objeto RecoveryPointCreator

Obligatorio: no

CreationDate

La fecha y la hora en que se creó un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

EncryptionKeyArn

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

Requerido: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

IsEncrypted

Un valor booleano que se devuelve como `TRUE` si el punto de recuperación especificado está cifrado o como `FALSE` si el punto de recuperación no está cifrado.

Tipo: Booleano

Obligatorio: no

IsParent

Se trata de un valor booleano que indica que es un punto de recuperación principal (compuesto).

Tipo: Booleano

Obligatorio: no

LastRestoreTime

La fecha y hora en que se restauró por última vez un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `LastRestoreTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

Lifecycle

El ciclo de vida define cuándo un recurso protegido pasa a almacenamiento en frío y cuándo caduca. AWS Backup cambia y vence las copias de seguridad automáticamente según el ciclo de vida que usted defina.

Las copias de seguridad que se han migrado al almacenamiento en frío deben permanecer en él durante un mínimo de 90 días. Por lo tanto, el valor de retención debe tener 90 días más que el valor del número de días tras los cuales se transferirá al almacenamiento en frío. El valor de "transition to cold after days" (número de días tras los cuales migrará a almacenamiento en frío) no puede cambiarse una vez que se ha migrado una copia de seguridad al almacenamiento en frío.

Los tipos de recursos que pueden pasar al almacenamiento en frío se muestran en la tabla Disponibilidad de funciones por recurso. AWS Backup omite esta expresión para otros tipos de recursos.

Tipo: objeto Lifecycle

Obligatorio: no

ParentRecoveryPointArn

El nombre del recurso de Amazon (ARN) del punto de recuperación principal (compuesto).

Tipo: cadena

Requerido: no

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

ResourceArn

Un ARN que identifica de forma única a un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso guardado como punto de recuperación; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso admitido es Amazon EC2.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

SourceBackupVaultArn

El almacén de copias de seguridad desde el que se copió originalmente el punto de recuperación. Si el punto de recuperación se restaura en la misma cuenta, este valor será `null`.

Tipo: cadena

Requerido: no

Status

Un código de estado que especifica el estado del punto de recuperación.

Tipo: cadena

Valores válidos: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Obligatorio: no

StatusMessage

Un mensaje que explica el estado actual del punto de recuperación.

Tipo: cadena

Requerido: no

VaultType

El tipo de almacén en el que se almacena el punto de recuperación descrito.

Tipo: cadena

Valores válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointByResource

Servicio: AWS Backup

Contiene información detallada sobre un punto de recuperación guardado.

Contenido

BackupSizeBytes

El tamaño de una copia de seguridad, en bytes.

Tipo: largo

Obligatorio: no

BackupVaultName

El nombre de un contenedor lógico donde se almacenan las copias de seguridad. Los almacenes de copia de seguridad se identifican con nombres que son exclusivos de la cuenta usada para crearlos y de la región de AWS donde se crearon.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: no

CreationDate

La fecha y la hora en que se creó un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

EncryptionKeyArn

La clave de cifrado en el servidor que se utiliza para proteger sus copias de seguridad; por ejemplo, `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.

Tipo: cadena

Requerido: no

IsParent

Se trata de un valor booleano que indica que es un punto de recuperación principal (compuesto).

Tipo: Booleano

Obligatorio: no

ParentRecoveryPointArn

El nombre del recurso de Amazon (ARN) del punto de recuperación principal (compuesto).

Tipo: cadena

Requerido: no

RecoveryPointArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

ResourceName

El nombre no exclusivo del recurso que pertenece a la copia de seguridad especificada.

Tipo: cadena

Requerido: no

Status

Un código de estado que especifica el estado del punto de recuperación.

Tipo: cadena

Valores válidos: `COMPLETED | PARTIAL | DELETING | EXPIRED`

Obligatorio: no

StatusMessage

Un mensaje que explica el estado actual del punto de recuperación.

Tipo: cadena

Requerido: no

VaultType

El tipo de almacén en el que se almacena el punto de recuperación descrito.

Tipo: cadena

Valores válidos: `BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointCreator

Servicio: AWS Backup

Contiene información sobre el plan de respaldo y la regla que AWS Backup se usaron para iniciar la copia de seguridad del punto de recuperación.

Contenido

BackupPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma única un plan de copia de seguridad; por ejemplo, `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`.

Tipo: cadena

Requerido: no

BackupPlanId

Identifica de forma única un plan de copia de seguridad.

Tipo: cadena

Requerido: no

BackupPlanVersion

Los ID de versión son cadenas cifradas en UTF-8, Unicode, únicas, generadas aleatoriamente que tienen como máximo una longitud de 1024 bytes. No es posible editarlos.

Tipo: cadena

Requerido: no

BackupRuleId

Identifica de forma exclusiva una regla utilizada para programar la copia de seguridad de una selección de recursos.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointMember

Servicio: AWS Backup

Se trata de un punto de recuperación que es un punto de recuperación secundario (anidado) de un punto de recuperación principal (compuesto). Estos puntos de recuperación se pueden disociar de su punto de recuperación principal (compuesto), en cuyo caso dejarán de ser miembros.

Contenido

BackupVaultName

El nombre del almacén de copias de seguridad (el contenedor lógico en el que se almacenan las copias de seguridad).

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_]{2,50}$`

Obligatorio: no

RecoveryPointArn

El nombre del recurso de Amazon (ARN) del punto de recuperación principal (compuesto).

Tipo: cadena

Requerido: no

ResourceArn

El nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso guardado.

Tipo: cadena

Requerido: no

ResourceType

El tipo de AWS recurso que se guarda como punto de recuperación.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RecoveryPointSelection

Servicio: AWS Backup

Esto especifica criterios para asignar un conjunto de recursos, como los tipos de recursos o los almacenes de copias de seguridad.

Contenido

DateRange

Este es un filtro de recursos que contiene FromDate: DateTime y ToDate: DateTime. Ambos valores son obligatorios. No se permiten DateTime valores futuros.

La fecha y la hora están en formato Unix y horario universal coordinado (UTC) y tienen una precisión de milisegundos (los milisegundos son opcionales). Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: objeto DateRange

Obligatorio: no

ResourceIdentifiers

Estos son los recursos incluidos en la selección de recursos (incluidos los tipos de recursos y los almacenes).

Tipo: matriz de cadenas

Obligatorio: no

VaultNames

Estos son los nombres de los almacenes en los que se encuentran los puntos de recuperación seleccionados.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportDeliveryChannel

Servicio: AWS Backup

Contiene información del plan de informe sobre dónde entregar los informes, específicamente el nombre del bucket de Amazon S3, el prefijo de clave de S3 y los formatos de los informes.

Contenido

S3BucketName

El nombre único del bucket de S3 que recibe los informes.

Tipo: cadena

Obligatorio: sí

Formats

El formato de sus informes:`CSV`,`JSON`, o ambos. Si no se especifica, el formato predeterminado es `CSV`.

Tipo: matriz de cadenas

Obligatorio: no

S3KeyPrefix

El prefijo del lugar donde AWS Backup Audit Manager envía los informes a Amazon S3. El prefijo es esta parte de la siguiente ruta: s3://your-bucket-name/`prefix`/backup/us-west-2/year/month/day/report-Name. Si no se especifica, no hay prefijo.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los SDK específicos del idioma, consulta lo siguiente: AWS

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

ReportDestination

Servicio: AWS Backup

Contiene información de su trabajo de informe sobre el destino de su informe.

Contenido

S3BucketName

El nombre único del bucket de Amazon S3 que recibe los informes.

Tipo: cadena

Requerido: no

S3Keys

El nombre clave que identifica de forma exclusiva sus informes en el bucket de S3.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportJob

Servicio: AWS Backup

Contiene información detallada acerca de un trabajo de informe. Un trabajo de informe compila un informe en función de un plan de informes y lo publica en Amazon S3.

Contenido

CompletionTime

La fecha y la hora en que se completó el trabajo de informe, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreationTime

La fecha y la hora en que se creó un trabajo de informe, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ReportDestination

El nombre del bucket de S3 y las claves S3 del destino en el que el trabajo de informe publica el informe.

Tipo: objeto ReportDestination

Obligatorio: no

ReportJobId

El identificador de un trabajo de informe. Una única cadena cifrada en UTF-8, Unicode, generada aleatoriamente que tiene como máximo una longitud de 1024 bytes. El ID del trabajo de informe no se puede editar.

Tipo: cadena

Requerido: no

ReportPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ReportTemplate

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Tipo: cadena

Requerido: no

Status

El estado de un trabajo de informe. Los estados son:

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` significa que el informe está disponible para su revisión en el destino designado. Si el estado es `FAILED`, revise el motivo en el `StatusMessage`.

Tipo: cadena

Requerido: no

StatusMessage

Un mensaje que explica el estado del trabajo de informe.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportPlan

Servicio: AWS Backup

Contiene información detallada acerca de un plan de informes.

Contenido

CreationTime

La fecha y la hora en que se creó el plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

DeploymentStatus

Devuelve el estado de una implementación de un plan de informes. Los estados son:

`CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED`

Tipo: cadena

Requerido: no

LastAttemptedExecutionTime

La fecha y la hora en que se intentó ejecutar por última vez un trabajo de informe asociado a este plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `LastAttemptedExecutionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastSuccessfulExecutionTime

La fecha y la hora en que se ejecutó por última vez con éxito un trabajo de informe asociado con este plan de informes, en formato Unix y horario universal coordinado (UTC). El valor de `LastSuccessfulExecutionTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ReportDeliveryChannel

Contiene información sobre dónde y cómo entregar sus informes, específicamente el nombre del bucket de Amazon S3, el prefijo de clave de S3 y los formatos de sus informes.

Tipo: objeto ReportDeliveryChannel

Obligatorio: no

ReportPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

ReportPlanDescription

Una descripción opcional del plan de informes con un máximo de 1024 caracteres.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 1024 caracteres.

Patrón: `.*\S.*`

Obligatorio: no

ReportPlanName

El nombre único del plan de informes. Este nombre debe contener entre 1 y 256 caracteres, comenzando por una letra, y contar con letras (a-z, A-Z), números (0-9) y guiones bajos (_).

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 256 caracteres.

Patrón: `[a-zA-Z][_a-zA-Z0-9]*`

Obligatorio: no

ReportSetting

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Si la plantilla del informe es `RESOURCE_COMPLIANCE_REPORT` o`CONTROL_COMPLIANCE_REPORT`, este recurso de API también describe la cobertura del informe por Regiones de AWS y los marcos.

Tipo: objeto ReportSetting

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

ReportSetting

Servicio: AWS Backup

Contiene información detallada acerca de la configuración de un informe.

Contenido

ReportTemplate

Identifica la plantilla para el informe. Los informes se crean mediante una plantilla. Las plantillas de informes son:

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

Tipo: cadena

Obligatorio: sí

Accounts

Estas son las cuentas que se incluirán en el informe.

Usa el valor de cadena de `ROOT` para incluir todas las unidades organizativas.

Tipo: matriz de cadenas

Obligatorio: no

FrameworkArns

Los nombres de recursos de Amazon (ARN) de los marcos que cubre un informe.

Tipo: matriz de cadenas

Obligatorio: no

NumberOfFrameworks

El número de marcos que cubre un informe.

Tipo: entero

Obligatorio: no

OrganizationUnits

Estas son las unidades organizativas que se incluirán en el informe.

Tipo: matriz de cadenas

Obligatorio: no

Regions

Estas son las regiones que se incluirán en el informe.

Usa el comodín como valor de cadena para incluir todas las regiones.

Tipo: matriz de cadenas

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreJobCreator

Servicio: AWS Backup

Contiene información sobre el plan de prueba de restauración que utilizó AWS Backup para iniciar el trabajo de restauración.

Contenido

RestoreTestingPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un plan de prueba de restauración.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreJobsListMember

Servicio: AWS Backup

Contiene metadatos sobre un trabajo de restauración.

Contenido

AccountId

El ID de la cuenta a la que pertenece el trabajo de restauración.

Tipo: String

Patrón: `^[0-9]{12}$`

Obligatorio: no

BackupSizeInBytes

El tamaño del recurso restaurado, en bytes.

Tipo: largo

Obligatorio: no

CompletionDate

La fecha y la hora en que se completó un trabajo para restaurar un punto de recuperación, en formato Unix y horario universal coordinado (UTC). El valor de `CompletionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

CreatedBy

Contiene información de identificación sobre la creación de un trabajo de restauración.

Tipo: objeto RestoreJobCreator

Obligatorio: no

CreatedResourceArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un recurso. El formato del ARN depende del tipo de recurso.

Tipo: cadena

Requerido: no

CreationDate

La fecha y la hora en que se creó un trabajo de restauración, en formato Unix y horario universal coordinado (UTC). El valor de `CreationDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

DeletionStatus

Indica el estado de los datos generados por la prueba de restauración. El estado puede ser `Deleting`, `Failed` o `Successful`.

Tipo: cadena

Valores válidos: `DELETING | FAILED | SUCCESSFUL`

Obligatorio: no

DeletionStatusMessage

Describe el estado de eliminación del trabajo de restauración.

Tipo: cadena

Requerido: no

ExpectedCompletionTimeMinutes

La cantidad de tiempo en minutos que se espera que tarde un trabajo de restauración de un punto de recuperación.

Tipo: largo

Obligatorio: no

IamRoleArn

Especifica el ARN del rol de IAM utilizado para crear el punto de recuperación de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

PercentDone

Contiene el porcentaje estimado que se ha completado de un trabajo en el momento en que se consultó el estado del trabajo.

Tipo: cadena

Requerido: no

RecoveryPointArn

Un ARN que identifica de forma exclusiva un punto de recuperación; por ejemplo, `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`.

Tipo: cadena

Requerido: no

RecoveryPointCreationDate

La fecha en la que se creó un punto de recuperación.

Tipo: marca temporal

Obligatorio: no

ResourceType

El tipo de recurso de los trabajos de restauración enumerados; por ejemplo, un volumen de Amazon Elastic Block Store (Amazon EBS) o una base de datos de Amazon Relational Database Service (Amazon RDS). Para las copias de seguridad de Windows Volume Shadow Copy Service (VSS), el único tipo de recurso admitido es Amazon EC2.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

RestoreJobId

Identifica de forma exclusiva el trabajo que restaura un punto de recuperación.

Tipo: cadena

Requerido: no

Status

Un código de estado que especifica el estado del trabajo iniciado AWS Backup para restaurar un punto de recuperación.

Tipo: cadena

Valores válidos: `PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

Obligatorio: no

StatusMessage

Un mensaje detallado que explica el estado del trabajo de restauración de un punto de recuperación.

Tipo: cadena

Requerido: no

ValidationStatus

El estado de la validación se ejecuta en el trabajo de restauración indicado.

Tipo: cadena

Valores válidos: `FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

Obligatorio: no

ValidationStatusMessage

Describe el estado de la validación ejecutada en el trabajo de restauración indicado.

Tipo: cadena

Requerido: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreJobSummary

Servicio: AWS Backup

Es un resumen de los trabajos de restauración creados o en ejecución en los 30 últimos días.

El resumen devuelto puede contener lo siguiente: región, cuenta, estado ResourceType, MessageCategory, StartTime EndTime, y recuento de trabajos incluidos.

Contenido

AccountId

El ID de la cuenta propietaria de los trabajos del resumen.

Tipo: String

Patrón: `^[0-9]{12}$`

Obligatorio: no

Count

El valor expresado como número de trabajos en un resumen de trabajos.

Tipo: entero

Obligatorio: no

EndTime

El valor de hora en formato numérico de la hora de finalización de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

Region

Las AWS regiones incluidas en el resumen del trabajo.

Tipo: cadena

Requerido: no

ResourceType

Este valor es el recuento de trabajos para el tipo de recurso especificado. La solicitud `GetSupportedResourceTypes` devuelve cadenas para los tipos de recursos compatibles.

Tipo: String

Patrón: `^[a-zA-Z0-9\-\_\.]{1,50}$`

Obligatorio: no

StartTime

El valor de hora en formato numérico de la hora de inicio de un trabajo.

Este valor es la hora en formato Unix, Hora universal coordinada (UTC) y tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

State

Este valor es el recuento de trabajos con el estado especificado.

Tipo: cadena

Valores válidos: `CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2

- AWS SDK para Ruby V3

RestoreTestingPlanForCreate

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

RecoveryPointSelection

`RecoveryPointSelection`tiene cinco parámetros (tres obligatorios y dos opcionales). Los valores que especifique determinan qué punto de recuperación se incluye en la prueba de restauración. Debe indicar `Algorithm` si desea incluir el último punto de recuperación dentro del suyo `SelectionWindowDays` o si desea un punto de recuperación aleatorio, y debe indicar a través `IncludeVaults` de qué bóvedas se pueden elegir los puntos de recuperación.

`Algorithm`(obligatorio) Valores válidos: "" o `LATEST_WITHIN_WINDOW` "»`RANDOM_WITHIN_WINDOW`.

`Recovery point types`(obligatorio) Valores válidos: "`SNAPSHOT`" y/o "`CONTINUOUS`». Incluir `SNAPSHOT` para restaurar únicamente los puntos de recuperación de instantáneas; incluir `CONTINUOUS` para restaurar puntos de recuperación continua (restauración puntual o PITR); utilizar ambos para restaurar una instantánea o un punto de recuperación continua. El punto de recuperación vendrá determinado por el valor de`Algorithm`.

`IncludeVaults`(obligatorio). Debe incluir uno o más almacenes de respaldo. Utilice el comodín ["*"] o ARN específicos.

`SelectionWindowDays`(opcional) El valor debe ser un número entero (en días) comprendido entre 1 y 365. Si no se incluye, el valor predeterminado es. `30`

`ExcludeVaults`(opcional). Puede optar por introducir uno o más ARN de almacenes de respaldo específicos para impedir que el contenido de esos almacenes pueda restaurarse. O bien, puede incluir una lista de selectores. Si este parámetro y su valor no están incluidos, el valor predeterminado es una lista vacía.

Tipo: objeto RestoreTestingRecoveryPointSelection

Obligatorio: sí

RestoreTestingPlanName

RestoreTestingPlanName Es una cadena única que es el nombre del plan de pruebas de restauración. No se puede cambiar después de la creación y debe constar únicamente de caracteres alfanuméricos y guiones bajos.

Tipo: cadena

Obligatorio: sí

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingPlanForGet

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó un plan de prueba de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

RecoveryPointSelection

Los criterios especificados para asignar un conjunto de recursos, como tipos de punto de recuperación o almacenes de copias de seguridad.

Tipo: objeto RestoreTestingRecoveryPointSelection

Obligatorio: sí

RestoreTestingPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

El nombre del plan de pruebas de restauración.

Tipo: cadena

Obligatorio: sí

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

CreatorRequestId

Identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si la solicitud incluye un `CreatorRequestId` que coincide con un plan de copia de seguridad existente, se devuelve ese plan. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

LastExecutionTime

La última vez que se ejecutó una prueba de restauración con el plan de prueba de restauración especificado. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de `LastExecutionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastUpdateTime

La fecha y hora en que se actualizó el plan de prueba de restauración. Esta actualización está en formato Unix y horario universal coordinado (UTC). El valor de `LastUpdateTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingPlanForList

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó un plan de prueba de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

RestoreTestingPlanArn

Un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva un plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

El nombre del plan de pruebas de restauración.

Tipo: cadena

Obligatorio: sí

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración.

Tipo: cadena

Obligatorio: sí

LastExecutionTime

La última vez que se ejecutó una prueba de restauración con el plan de prueba de restauración especificado. Una fecha y hora, en formato Unix y horario universal coordinado (UTC). El valor de `LastExecutionDate` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

LastUpdateTime

La fecha y hora en que se actualizó el plan de prueba de restauración. Esta actualización está en formato Unix y horario universal coordinado (UTC). El valor de `LastUpdateTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: no

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingPlanForUpdate

Servicio: AWS Backup

Contiene metadatos sobre un plan de prueba de restauración.

Contenido

RecoveryPointSelection

Obligatorio: `Algorithm`; `RecoveryPointTypes`; `IncludeVaults` (uno o varios).

Opcional: SelectionWindowDays('30' si no se especifica); `ExcludeVaults` (por defecto, la lista está vacía si no aparece).

Tipo: objeto RestoreTestingRecoveryPointSelection

Obligatorio: no

ScheduleExpression

Una expresión CRON en la zona horaria especificada cuando se ejecuta un plan de prueba de restauración.

Tipo: cadena

Requerido: no

ScheduleExpressionTimezone

Opcional. La zona horaria en la que se establece la expresión de programación. De forma predeterminada, ScheduleExpressions están en UTC. Puede modificar esto para una zona horaria específica.

Tipo: cadena

Requerido: no

StartWindowHours

El valor predeterminado es 24 horas.

Un valor en horas después de una prueba de restauración programada para que se cancele el trabajo si no se ha iniciado correctamente. Este valor es opcional. Si se incluye este valor, este parámetro tiene un valor máximo de 168 horas (una semana).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingRecoveryPointSelection

Servicio: AWS Backup

`RecoveryPointSelection`tiene cinco parámetros (tres obligatorios y dos opcionales). Los valores que especifique determinan qué punto de recuperación se incluye en la prueba de restauración. Debe indicar `Algorithm` si desea incluir el último punto de recuperación dentro del suyo `SelectionWindowDays` o si desea un punto de recuperación aleatorio, y debe indicar a través `IncludeVaults` de qué bóvedas se pueden elegir los puntos de recuperación.

`Algorithm`(obligatorio) Valores válidos: "" o `LATEST_WITHIN_WINDOW` "»`RANDOM_WITHIN_WINDOW`.

`Recovery point types`(obligatorio) Valores válidos: "`SNAPSHOT`" y/o "`CONTINUOUS`». Incluir `SNAPSHOT` para restaurar únicamente los puntos de recuperación de instantáneas; incluir `CONTINUOUS` para restaurar puntos de recuperación continua (restauración puntual o PITR); utilizar ambos para restaurar una instantánea o un punto de recuperación continua. El punto de recuperación vendrá determinado por el valor de`Algorithm`.

`IncludeVaults`(obligatorio). Debe incluir uno o más almacenes de respaldo. Utilice el comodín ["*"] o ARN específicos.

`SelectionWindowDays`(opcional) El valor debe ser un número entero (en días) comprendido entre 1 y 365. Si no se incluye, el valor predeterminado es. `30`

`ExcludeVaults`(opcional). Puede optar por introducir uno o más ARN de almacenes de respaldo específicos para impedir que el contenido de esos almacenes pueda restaurarse. O bien, puede incluir una lista de selectores. Si este parámetro y su valor no están incluidos, el valor predeterminado es una lista vacía.

Contenido

Algorithm

Los valores aceptables son "LATEST_WITHIN_WINDOW" o "RANDOM_WITHIN_WINDOW"

Tipo: cadena

Valores válidos: `LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW`

Obligatorio: no

ExcludeVaults

Los valores aceptados son ARN específicos o una lista de selectores. Si no se incluye ninguno, aparece una lista vacía de forma predeterminada.

Tipo: matriz de cadenas

Obligatorio: no

IncludeVaults

Los valores aceptados son el comodín ["*"] o ARN específicos o sustitución de comodín ARN ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...]

Tipo: matriz de cadenas

Obligatorio: no

RecoveryPointTypes

Son los tipos de puntos de recuperación.

Incluya `SNAPSHOT` para restaurar únicamente los puntos de recuperación de instantáneas; inclúyala `CONTINUOUS` para restaurar puntos de recuperación continua (restauración puntual o PITR); utilice ambas opciones para restaurar una instantánea o un punto de recuperación continua. El punto de recuperación vendrá determinado por el valor de`Algorithm`.

Tipo: matriz de cadenas

Valores válidos: `CONTINUOUS | SNAPSHOT`

Obligatorio: no

SelectionWindowDays

Los valores aceptados son números enteros de 1 a 365.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForCreate

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración específica.

ProtectedResourceType es obligatorio, como Amazon EBS o Amazon EC2.

Consta de `RestoreTestingSelectionName`, `ProtectedResourceType` y uno de los siguientes elementos:

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

Cada tipo de recurso protegido puede tener un único valor.

Una selección de pruebas de restauración puede incluir un valor comodín ("*") como `ProtectedResourceArns` junto con `ProtectedResourceConditions`. También puede incluir hasta 30 ARN de recursos protegidos específicos en `ProtectedResourceArns`.

`StringEquals` y `StringNotEquals` son ejemplos de `ProtectedResourceConditions`.

Contenido

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

ProtectedResourceType

El tipo de AWS recurso incluido en una selección de pruebas de restauración; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Los tipos de recursos admitidos son:

- `Aurora` para Amazon Aurora
- `DocumentDB` para Amazon DocumentDB (con compatibilidad con MongoDB)

- `DynamoDB` para Amazon DynamoDB
- `EBS` para Amazon Elastic Block Store (EBS)
- `EC2` para Amazon Elastic Compute Cloud
- `EFS` para Amazon Elastic File System
- `FSx` para Amazon FSx
- `Neptune` para Amazon Neptune
- `RDS` para Amazon Relational Database Service
- `S3` para Amazon S3

Tipo: cadena

Obligatorio: sí

RestoreTestingSelectionName

El nombre exclusivo de la selección de pruebas de restauración que pertenece al plan de pruebas de restauración correspondiente.

Tipo: cadena

Obligatorio: sí

ProtectedResourceArns

Cada recurso protegido se puede filtrar por sus ARN específicos, por ejemplo, `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]` o por un comodín :`ProtectedResourceArns: ["*"]`, pero no por ambos.

Tipo: matriz de cadenas

Obligatorio: no

ProtectedResourceConditions

Si ha incluido el comodín ProtectedResourceArns, puede incluir las condiciones de los recursos, por ejemplo. `ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]`

Tipo: objeto ProtectedResourceConditions

Obligatorio: no

RestoreMetadataOverrides

Puede anular determinadas claves de metadatos de restauración incluyendo el parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Los valores de clave no distinguen mayúsculas y minúsculas.

Consulte la lista completa de metadatos inferidos de pruebas de restauración.

Tipo: mapa de cadena a cadena

Obligatorio: no

ValidationWindowHours

Es el número de horas (de 1 a 168) disponibles para ejecutar un script de validación de los datos. Los datos se eliminarán al finalizar el script de validación o al final del periodo de retención especificado, lo que ocurra primero.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForGet

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó una selección de pruebas de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

ProtectedResourceType

El tipo de AWS recurso incluido en una selección de pruebas de recursos; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

RestoreTestingPlanName Es una cadena única que es el nombre del plan de pruebas de restauración.

Tipo: cadena

Obligatorio: sí

RestoreTestingSelectionName

El nombre exclusivo de la selección de pruebas de restauración que pertenece al plan de pruebas de restauración correspondiente.

Tipo: cadena

Obligatorio: sí

CreatorRequestId

Identifica la solicitud y permite que se reintenten las solicitudes que han producido un error sin el riesgo de ejecutar la operación dos veces. Si la solicitud incluye un `CreatorRequestId` que coincide con un plan de copia de seguridad existente, se devuelve ese plan. Este parámetro es opcional.

Si se utiliza, este parámetro debe contener de 1 a 50 caracteres alfanuméricos o “-_”. caracteres.

Tipo: cadena

Requerido: no

ProtectedResourceArns

Puede incluir ARN específicos, por ejemplo, `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, o incluir un comodín: `ProtectedResourceArns: ["*"]`, pero no ambos.

Tipo: matriz de cadenas

Obligatorio: no

ProtectedResourceConditions

En una selección de pruebas de recursos, este parámetro filtra por condiciones específicas, como `StringEquals` o `StringNotEquals`.

Tipo: objeto ProtectedResourceConditions

Obligatorio: no

RestoreMetadataOverrides

Puede anular determinadas claves de metadatos de restauración incluyendo el parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Los valores de clave no distinguen mayúsculas y minúsculas.

Consulte la lista completa de metadatos inferidos de pruebas de restauración.

Tipo: mapa de cadena a cadena

Obligatorio: no

ValidationWindowHours

Es el número de horas (de 1 a 168) disponibles para ejecutar un script de validación de los datos. Los datos se eliminarán al finalizar el script de validación o al final del periodo de retención especificado, lo que ocurra primero.

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForList

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración.

Contenido

CreationTime

La fecha y la hora en que se creó una selección de pruebas de restauración, en formato Unix y Hora universal coordinada (UTC). El valor de `CreationTime` tiene una precisión de milisegundos. Por ejemplo, el valor 1516925490.087 representa el viernes 26 de enero de 2018 a las 12:11:30.087 h.

Tipo: marca temporal

Obligatorio: sí

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Obligatorio: sí

ProtectedResourceType

El tipo de AWS recurso incluido en una selección de pruebas de restauración; por ejemplo, un volumen de Amazon EBS o una base de datos de Amazon RDS.

Tipo: cadena

Obligatorio: sí

RestoreTestingPlanName

Cadena única que es el nombre del plan de prueba de restauración.

El nombre no se puede cambiar después de crear el plan. El nombre consta de únicamente de caracteres alfanuméricos y guiones bajos. La longitud máxima es 50.

Tipo: cadena

Obligatorio: sí

RestoreTestingSelectionName

Nombre único de la selección de pruebas de restauración.

Tipo: cadena

Obligatorio: sí

ValidationWindowHours

Este valor representa el tiempo, en horas, que se retienen los datos después de una prueba de restauración para poder completar la validación opcional.

El valor aceptado es un entero entre 0 y 168 (el equivalente en horas a siete días).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

RestoreTestingSelectionForUpdate

Servicio: AWS Backup

Contiene metadatos sobre una selección de pruebas de restauración.

Contenido

IamRoleArn

El nombre de recurso de Amazon (ARN) del rol de IAM que AWS Backup utiliza para crear el recurso de destino; por ejemplo, `arn:aws:iam::123456789012:role/S3Access`.

Tipo: cadena

Requerido: no

ProtectedResourceArns

Puede incluir una lista de ARN específicos, por ejemplo, `ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."]`, o incluir un comodín: `ProtectedResourceArns: ["*"]`, pero no ambos.

Tipo: matriz de cadenas

Obligatorio: no

ProtectedResourceConditions

Las condiciones que defina para los recursos en su plan de pruebas de restauración mediante etiquetas.

Por ejemplo, `"StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },`. Los operadores de condición distinguen entre mayúsculas y minúsculas.

Tipo: objeto ProtectedResourceConditions

Obligatorio: no

RestoreMetadataOverrides

Puede anular determinadas claves de metadatos de restauración incluyendo el parámetro `RestoreMetadataOverrides` en el cuerpo de `RestoreTestingSelection`. Los valores de clave no distinguen mayúsculas y minúsculas.

Consulte la lista completa de metadatos inferidos de pruebas de restauración.

Tipo: mapa de cadena a cadena

Obligatorio: no

ValidationWindowHours

Este valor representa el tiempo, en horas, que se retienen los datos después de una prueba de restauración para poder completar la validación opcional.

El valor aceptado es un entero entre 0 y 168 (el equivalente en horas a siete días).

Tipo: entero

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

AWS Backup gateway

AWS Backup gateway admite los siguientes tipos de datos:

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine

- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

Servicio: AWS Backup gateway

Describe un intervalo de límite de velocidad de ancho de banda para una puerta de enlace. Un programa de límite de velocidad de ancho de banda consta de uno o más intervalos de límite de velocidad de ancho de banda. Un intervalo de límite de velocidad de ancho de banda define un periodo de tiempo en uno o más días de la semana, durante el cual se especifican los límites de velocidad de ancho de banda para la carga, la descarga o ambas.

Contenido

DaysOfWeek

El componente de días de la semana del intervalo límite de velocidad de ancho de banda, se representa como números ordinales del 0 al 6, donde 0 representa el domingo y 6 representa el sábado.

Tipo: Matriz de números enteros

Miembros de la matriz: número mínimo de 1 artículo. Número máximo de 7 elementos.

Rango válido: valor mínimo de 0. Valor máximo de 6.

Obligatorio: sí

EndHourOfDay

La hora del día en que finaliza el intervalo de límite de velocidad de ancho de banda.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

EndMinuteOfHour

El minuto de la hora en que finaliza el intervalo de límite de velocidad de ancho de banda.

> **Important**
>
> El intervalo de límite de velocidad de ancho de banda finaliza al final del minuto. Para finalizar un intervalo al final de una hora, utilice el valor59.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

StartHourOfDay

La hora del día en que comienza el intervalo de límite de velocidad de ancho de banda.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

StartMinuteOfHour

El minuto de la hora en que comienza el intervalo de límite de velocidad de ancho de banda. El intervalo comienza al principio de ese minuto. Para comenzar un intervalo exactamente al principio de la hora, utilice el valor `0`.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

AverageUploadRateLimitInBitsPerSec

El componente de límite de velocidad de carga promedio del intervalo de límite de velocidad de ancho de banda, en bits por segundo. Este campo no aparece en la respuesta si no se ha establecido el límite de velocidad de carga.

Tipo: largo

Rango válido: valor mínimo de 51 200. Valor máximo de 8 000 000 000 000

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Gateway

Servicio: AWS Backup gateway

Una puerta de enlace es un dispositivo de AWS Backup puerta de enlace que se ejecuta en la red del cliente para proporcionar una conectividad perfecta al almacenamiento de copias de seguridad en la AWS nube.

Contenido

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la `ListGateways` operación para devolver una lista de pasarelas para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: no

GatewayDisplayName

El nombre de visualización de la puerta de enlace.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

GatewayType

El tipo de puerta de enlace.

Tipo: cadena

Valores válidos: `BACKUP_VM`

Obligatorio: no

HypervisorId

El ID de hipervisor de la puerta de enlace.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Obligatorio: no

LastSeenTime

La última vez que la AWS Backup puerta de enlace se comunicó con la puerta de enlace, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

GatewayDetails

Servicio: AWS Backup gateway

Los detalles de la puerta de enlace.

Contenido

GatewayArn

El nombre de recurso de Amazon (ARN) de la puerta de enlace. Utilice la operación `ListGateways` para devolver una lista de puertas de enlace para su cuenta y Región de AWS.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. Longitud máxima de 180

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: no

GatewayDisplayName

El nombre de visualización de la puerta de enlace.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

GatewayType

El tipo de puerta de enlace.

Tipo: cadena

Valores válidos: `BACKUP_VM`

Obligatorio: no

HypervisorId

El ID de hipervisor de la puerta de enlace.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Obligatorio: no

LastSeenTime

Detalles que muestran la última vez que AWS Backup Gateway se comunicó con la nube, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

MaintenanceStartTime

Devuelve la hora de inicio del mantenimiento semanal de la puerta de enlace, incluido el día y la hora de la semana. Tenga en cuenta que los valores están expresados en términos de la zona horaria de la puerta de enlace. Puede ser semanal o mensual.

Tipo: objeto MaintenanceStartTime

Obligatorio: no

NextUpdateAvailabilityTime

Detalles que muestran la hora de disponibilidad de la próxima actualización de la puerta de enlace.

Tipo: marca temporal

Obligatorio: no

VpcEndpoint

El nombre de DNS del punto de conexión de la nube privada virtual (VPC) que utiliza la puerta de enlace para conectarse a la nube como puerta de enlace de copia de seguridad.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Hypervisor

Servicio: AWS Backup gateway

Representa los permisos del hipervisor a los que se conectará la puerta de enlace.

Un hipervisor es un hardware, software o firmware que crea y administra máquinas virtuales y les asigna recursos.

Contenido

Host

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: `^.+$`

Obligatorio: no

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: no

KmsKeyArn

El nombre del recurso de Amazon (ARN) AWS Key Management Service utilizado para cifrar el hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obligatorio: no

Name

El nombre del hipervisor.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

State

El estado del hipervisor.

Tipo: cadena

Valores válidos: `PENDING | ONLINE | OFFLINE | ERROR`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

HypervisorDetails

Servicio: AWS Backup gateway

Estos son los detalles del hipervisor especificado. Un hipervisor es un hardware, software o firmware que crea y administra máquinas virtuales y les asigna recursos.

Contenido

Host

El host del servidor del hipervisor. Puede ser una dirección IP o un nombre de dominio completo (FQDN).

Tipo: cadena

Limitaciones de longitud: longitud mínima de 3. Longitud máxima de 128.

Patrón: `^.+$`

Obligatorio: no

HypervisorArn

El nombre de recurso de Amazon (ARN) del hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: no

KmsKeyArn

El nombre de recurso de Amazon (ARN) de la clave de AWS KMS (KMS) que se utiliza para cifrar el hipervisor.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

Obligatorio: no

LastSuccessfulMetadataSyncTime

Este es el momento en que se produjo la última sincronización correcta de los metadatos.

Tipo: marca temporal

Obligatorio: no

LatestMetadataSyncStatus

Este es el estado más reciente de la sincronización de metadatos indicada.

Tipo: cadena

Valores válidos: `CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED`

Obligatorio: no

LatestMetadataSyncStatusMessage

Este es el estado más reciente de la sincronización de metadatos indicada.

Tipo: cadena

Requerido: no

LogGroupArn

El nombre de recurso de Amazon (ARN) de grupo de puertas de enlace dentro del registro solicitado.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0 caracteres. La longitud máxima es de 2048 caracteres.

Patrón: `^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

Obligatorio: no

Name

Este es el nombre del hipervisor especificado.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

State

Este es el estado actual del hipervisor especificado.

Los estados posibles son `PENDING`, `ONLINE`, `OFFLINE` o `ERROR`.

Tipo: cadena

Valores válidos: `PENDING | ONLINE | OFFLINE | ERROR`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

MaintenanceStartTime

Servicio: AWS Backup gateway

Es la hora de inicio del mantenimiento semanal de la puerta de enlace, incluido el día y la hora de la semana. Tenga en cuenta que los valores están expresados en términos de la zona horaria de la puerta de enlace. Puede ser semanal o mensual.

Contenido

HourOfDay

El componente de horas de la hora de inicio del mantenimiento se representa como hh, donde hh es la hora (de 0 a 23). La hora del día corresponde a la zona horaria de la puerta de enlace.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 23.

Obligatorio: sí

MinuteOfHour

El componente de minutos de la hora de inicio del mantenimiento se representa como mm, donde mm es el minuto (de 0 a 59). El minuto de la hora corresponde a la zona horaria de la puerta de enlace.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 59.

Obligatorio: sí

DayOfMonth

El componente del día del mes de la hora de inicio del mantenimiento representado como un número ordinal de 1 a 28, donde 1 representa el primer día del mes y 28 representa el último día del mes.

Tipo: entero

Rango válido: valor mínimo de 1. Valor máximo de 31.

Obligatorio: no

DayOfWeek

Número ordinal entre 0 y 6 que representa el día de la semana, donde 0 representa el domingo y 6 representa el sábado. El día de la semana corresponde a la zona horaria de la puerta de enlace.

Tipo: entero

Rango válido: valor mínimo de 0. Valor máximo de 6.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Tag

Servicio: AWS Backup gateway

Un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos. Los caracteres permitidos incluyen espacios, números y letras en UTF-8, además de los siguientes caracteres especiales: + - = . _ : /.

Contenido

Key

La parte de clave del par clave-valor de la etiqueta. La clave no pueden comenzar por `aws:`.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatorio: sí

Value

La parte de valor del par clave-valor de la etiqueta.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[^\x00]*$`

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

VirtualMachine

Servicio: AWS Backup gateway

Una máquina virtual que se encuentra en un hipervisor.

Contenido

HostName

El nombre del host de la máquina virtual.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

HypervisorId

El ID del hipervisor de la máquina virtual.

Tipo: cadena

Requerido: no

LastBackupDate

La fecha más reciente en la que se realizó una copia de seguridad de una máquina virtual, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

Name

Nombre de la máquina virtual.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

Path

La ruta de la máquina virtual.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 4096 caracteres.

Patrón: `^[^\x00]+$`

Obligatorio: no

ResourceArn

El nombre de recurso de Amazon (ARN) de la máquina virtual. Por ejemplo, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

VirtualMachineDetails

Servicio: AWS Backup gateway

Sus objetos `VirtualMachine`, ordenados por sus nombres de recurso de Amazon (ARN).

Contenido

HostName

El nombre del host de la máquina virtual.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

HypervisorId

El ID del hipervisor de la máquina virtual.

Tipo: cadena

Requerido: no

LastBackupDate

La fecha más reciente en la que se realizó una copia de seguridad de una máquina virtual, en formato Unix y en hora UTC.

Tipo: marca temporal

Obligatorio: no

Name

Nombre de la máquina virtual.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 100 caracteres.

Patrón: `^[a-zA-Z0-9-]*$`

Obligatorio: no

Path

La ruta de la máquina virtual.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 4096 caracteres.

Patrón: `^[^\x00]+$`

Obligatorio: no

ResourceArn

El nombre de recurso de Amazon (ARN) de la máquina virtual. Por ejemplo, `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 50. La longitud máxima es de 500 caracteres.

Patrón: `^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Obligatorio: no

VmwareTags

Estos son los detalles de las etiquetas de VMware asociadas a la máquina virtual especificada.

Tipo: matriz de objetos VmwareTag

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

VmwareTag

Servicio: AWS Backup gateway

Una etiqueta de VMware es una etiqueta asociada a una máquina virtual específica. Una etiqueta es un par clave-valor que puede utilizar para administrar, filtrar y buscar sus recursos.

El contenido de las etiquetas de VMware se puede hacer coincidir con las AWS etiquetas.

Contenido

VmwareCategory

Esta es la categoría de VMware.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: no

VmwareTagDescription

Es una descripción definida por el usuario de una etiqueta de VMware.

Tipo: cadena

Requerido: no

VmwareTagName

Es el nombre definido por el usuario de una etiqueta de VMware.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: no

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulte lo siguiente:

- AWS SDK para C++

- AWS SDK para Java V2
- AWS SDK para Ruby V3

VmwareToAwsTagMapping

Servicio: AWS Backup gateway

Esto muestra la asignación de las etiquetas de VMware a las AWS etiquetas correspondientes.

Contenido

AwsTagKey

La parte clave del par clave-valor de la AWS etiqueta.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 128.

Patrón: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Obligatorio: sí

AwsTagValue

La parte de valores del par clave-valor de la AWS etiqueta.

Tipo: cadena

Limitaciones de longitud: longitud mínima de 0. La longitud máxima es de 256 caracteres.

Patrón: `^[^\x00]*$`

Obligatorio: sí

VmwareCategory

Esta es la categoría de VMware.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: sí

VmwareTagName

Es el nombre definido por el usuario de una etiqueta de VMware.

Tipo: string

Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 80.

Obligatorio: sí

Véase también

Para obtener más información sobre el uso de esta API en uno de los AWS SDK específicos del idioma, consulta lo siguiente:

- AWS SDK para C++
- AWS SDK para Java V2
- AWS SDK para Ruby V3

Parámetros comunes

La siguiente lista contiene los parámetros que utilizan todas las acciones para firmar solicitudes de Signature Version 4 con una cadena de consulta. Los parámetros específicos de acción se enumeran en el tema correspondiente a la acción. Para obtener más información sobre Signature Version 4, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Action

Las acciones que se van a realizar.

Tipo: cadena

Obligatorio: sí

Version

La versión de la API para la que está escrita la solicitud, expresada en el formato AAAA-MM-DD.

Tipo: String

Obligatorio: sí

X-Amz-Algorithm

El algoritmo de hash que utilizó para crear la solicitud de firma.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: String

Valores válidos: `AWS4-HMAC-SHA256`

Obligatorio: condicional

X-Amz-Credential

El valor del ámbito de la credencial, que es una cadena que incluye la clave de acceso, la fecha, la región a la que se dirige, el servicio que solicita y una cadena de terminación (“aws4_request”). El valor se expresa en el siguiente formato: access_key/AAAAMMDD/region/service/aws4_request.

Para obtener más información, consulte Crear una solicitud API de AWS firmada en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-Date

La fecha utilizada para crear la firma. El formato debe ser ISO 8601 formato básico (AAAAMMDD‘T’HHMMSS‘Z’). Por ejemplo, la siguiente fecha y hora es un valor válido de X-Amz-Date para `20120325T120000Z`.

Condición: X-Amz-Date es opcional en todas las solicitudes; se puede utilizar para anular la fecha empleada a fin de firmar las solicitudes. Si el encabezado Date se especifica en el formato básico ISO 8601, no se requiere X-Amz-Date. Cuando se usa X-Amz-Date, siempre anula el valor del encabezado Date. Para obtener más información, consulte Elementos de una firma de solicitud API de AWS en la Guía del usuario de IAM.

Tipo: cadena

Obligatorio: condicional

X-Amz-Security-Token

El token de seguridad temporal que se obtuvo mediante una llamada a AWS Security Token Service (AWS STS). Para obtener una lista de servicios compatibles con las credenciales de seguridad temporales de AWS STS, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Condición: si utiliza credenciales de seguridad temporales de AWS STS, debe incluir el token de seguridad.

Tipo: cadena

Obligatorio: condicional

X-Amz-Signature

Especifica la firma codificada hexadecimal que se calculó a partir de la cadena que se va a firmar y la clave de firma derivada.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

X-Amz-SignedHeaders

Especifica todos los encabezados HTTP que se incluyeron como parte de la solicitud canónica. Para obtener más información acerca de especificar encabezados firmados, consulte Crear una solicitud API de AWS firmada en la Guía del usuario de IAM.

Condición: especifique este parámetro cuando incluya información de autenticación en una cadena de consulta en lugar de en el encabezado de autorización HTTP.

Tipo: cadena

Obligatorio: condicional

Errores comunes

En esta sección, se enumeran los errores comunes a las acciones de la API de todos los servicios de AWS. En el caso de los errores específicos de una acción de la API de este servicio, consulte el tema de dicha acción de la API.

AccessDeniedException

No tiene acceso suficiente para realizar esta acción.

Código de estado HTTP: 400

IncompleteSignature

La firma de solicitud no se ajusta a los estándares de AWS.

Código de estado HTTP: 400

InternalFailure

El procesamiento de la solicitud ha devuelto un error debido a un error o una excepción desconocidos.

Código de estado HTTP: 500

InvalidAction

La acción u operación solicitada no es válida. Compruebe que la acción se ha escrito correctamente.

Código de estado HTTP: 400

InvalidClientTokenId

El certificado X.509 o el ID de clave de acceso de AWS proporcionado no existen en nuestros registros.

Código de estado HTTP: 403

NotAuthorized

No tiene permiso para realizar esta acción.

Código de estado HTTP: 400

OptInRequired

El ID de clave de acceso de AWS necesita una suscripción al servicio.

Código de estado HTTP: 403

RequestExpired

La solicitud llegó al servicio más de 15 minutos después de la marca de fecha en la solicitud o más de 15 minutos después de la fecha de vencimiento de la solicitud (por ejemplo, para las URL prefirmadas) o la marca de fecha de la solicitud corresponde a una hora futura en más de 15 minutos.

Código de estado HTTP: 400

ServiceUnavailable

La solicitud no se ha ejecutado correctamente debido a un error temporal del servidor.

Código de estado HTTP: 503

ThrottlingException

La solicitud se denegó debido a una limitación controlada.

Código de estado HTTP: 400

ValidationError

La entrada no satisface las limitaciones que especifica un servicio de AWS.

Código de estado HTTP: 400

Historial de documentos para AWS Backup

- Versión de la API: 6 de diciembre de 2023
- Última actualización de la documentación: 3 de junio de 2024

En la siguiente tabla se enumeran todos los AWS Backup lanzamientos desde el lanzamiento del servicio en enero de 2019 hasta la fecha. Para recibir notificaciones sobre las actualizaciones de esta documentación, puede suscribirse al canal RSS que aparece más arriba.

Cambio	Descripción	Fecha
AWS Backup característica: Expansión regional	AWS Backup La compatibilidad con el nivel de archivado de instantáneas de Amazon EBS ya está disponible en las siguientes regiones: • China (Pekín) • China (Ningxia) • AWS GovCloud (EE. UU.-Oeste) • AWS GovCloud (EE. UU.-Este)	3 de junio de 2024
Se actualizaron las políticas administradas de AWS	AWS Backup se agregó permiso `backup:TagResource` a las siguientes políticas administradas: • AWSBackupServiceRolePolicyForBackup • AWSBackupServiceRolePolicyForS3Backup • AWSBackupServiceLinkedRolePolicyForBackup	17 de mayo de 2024

Cambio	Descripción	Fecha
	Para obtener más información, consulte Actualizaciones de políticas.	
AWS Backup ahora disponible en la región de Canadá Oeste (Calgary)	El backup y la restauración para muchos tipos de recursos ya están disponibles en Región de AWS Canada West (Calgary). Para ver las funciones de copia de seguridad compatibles, consulte Disponibilidad de las funciones en. Región de AWS Para ver los tipos de recursos compatibles, consulte Servicios compatibles de Región de AWS.	14 de marzo de 2024
Se agregaron permisos a la política administrada	AWS Backup actualizó la política AWSServiceRolePolicyForBackupRestoreTestingañadiendo permisos para admitir tipos de recursos adicionales dentro de la función de pruebas de restauración. Para obtener más información sobre los permisos específicos agregados, consulte Actualizaciones de políticas.	14 de febrero de 2024

Cambio	Descripción	Fecha
Soporte de backup y restauración de FSx para volúmenes ONTAP FlexGroup	AWS Backup ahora admite la copia de seguridad y la restauración de FSx para los FlexGroup volúmenes ONTAP en la mayoría de los casos. Regiones de AWS Para obtener más información, consulte Restauración de un sistema de archivos de Amazon FSx. .	10 de enero de 2024
Compatibilidad con copia de seguridad y restauración de SAP HANA HA	AWS Backup ahora ofrece soporte para bases de datos de alta disponibilidad de SAP HANA en Amazon EC2 para backup y restore. Para obtener más información, consulte SAP HANA en copias de seguridad de Amazon EC2 y Restauración de un sistema de alta disponibilidad de SAP HANA	21 de diciembre de 2023

Cambio	Descripción	Fecha
AWS Backup Control Audit Manager para pruebas de restauración	AWS Backup Audit Manager ahora ofrece el control del tiempo de restauración para que los recursos cumplan con el objetivo para ayudar a monitorear los tiempos de restauración. Este control comprueba si el tiempo de restauración de un recurso cumple la duración objetivo. Para obtener más información, consulte Controles y corrección y Auditoría de pruebas de restauración.	18 de diciembre de 2023
Compatibilidad con almacenamiento en frío de Amazon EBS	AWS Backup ahora admite la transición de copias de seguridad de EBS del almacenamiento en caliente al almacenamiento en frío. Para obtener más información, consulte • Nivel de archivo de Amazon EBS para almacenamiento en frío • Ciclo de vida y niveles de almacenamiento • Creación de un plan de copia de seguridad	27 de noviembre de 2023

Cambio	Descripción	Fecha
Presentación de las políticas de restauración	AWS Backup introduce las pruebas de restauración, que permiten una evaluación automática y periódica de la viabilidad de la restauración, así como la capacidad de supervisar los tiempos de duración de las tareas de restauración. Para obtener más información, consulte Pruebas de restauración.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Se actualizaron las políticas administradas de AWS	AWS Backup agregó los permisos `ec2:DescribeSnapshotTierStatus` y `ec2:ModifySnapshotTier` a las políticas administradas `AWSBackupServiceRolePolicyForBackups` y `AWSBackupServiceLinkedRolePolicyForBackup`. AWS Backup también agregó los permisos `ec2:DescribeSnapshotTierStatus` y `ec2:RestoreSnapshotTier` a la política administrada `AWSBackupServiceRolePolicyForRestores`. Estos permisos son necesarios para que los usuarios tengan la opción de realizar la transición de los recursos de Amazon EBS almacenados AWS Backup al almacenamiento de archivos y de restaurar los recursos del nivel de almacenamiento de archivos. Para obtener más información, consulte Actualizaciones de políticas.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Se agregó el permiso para transmitir roles para facilitar pruebas de restauración.	AWS Backup agregado `restore-testing.backup.amazonaws.com` a `IamPassRolePermissions` y. `IamCreateServiceLinkedRolePermissions` Esta adición es necesaria para AWS Backup realizar pruebas de restauración en nombre de los clientes.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Se ha agregado una nueva política de roles vinculados a servicios	AWS Backup ha agregado el nuevo rol vinculado al servicio denominado `AWSServiceRoleForBackupRestoreTesting`, que proporciona permisos de respaldo para realizar pruebas de restauración. Esta nueva función vinculada al servicio proporciona los permisos necesarios para realizar AWS Backup las pruebas de restauración. Los permisos incluyen las acciones `list, read, and write` para que los siguientes servicios se incluyan en pruebas de restauración: Aurora, DocumentDB, DynamoDB, Amazon EBS, Amazon EC2, Amazon EFS, FSx para Lustre, FSx para Windows File Server, FSx para ONTAP, FSx para OpenZFS, Amazon Neptune, Amazon RDS y Amazon S3.	27 de noviembre de 2023

Cambio	Descripción	Fecha
Nuevo panel de métricas de tareas en la consola AWS Backup	La AWS Backup consola ahora muestra un panel de tareas, lo que simplifica la supervisión del estado de las copias de seguridad a gran escala con una nueva interfaz visual de usuario y métricas agregadas de respaldo, copia y restauración de los servicios compatibles AWS Backup. El panel de empleos está disponible en todas las regiones en las que está disponible AWS Backup Audit Manager. Las regiones que no figuran en la lista podrán seguir accediendo al CloudWatch panel. Para obtener más información, consulte paneles de la consola de AWS Backup.	15 de noviembre de 2023

Cambio	Descripción	Fecha
Compatibilidad con copias de seguridad de pilas anidadas	AWS Backup ha ampliado su compatibilidad con las copias de seguridad de AWS CloudFormation los recursos. Las pilas de CloudFormation aplicaciones que contienen pilas anidadas se pueden incluir en las copias de seguridad. Para obtener más informaci ón, consulte CloudFormation stack backups.	8 de noviembre de 2023
Compatibilidad con Amazon S3 en China (Pekín) y China (Ningxia).	AWS Backup El soporte para Amazon S3 ya está disponibl e en las regiones de China (Pekín) y China (Ningxia). Para obtener más informaci ón, consulte Disponibilidad de características por región.	26 de octubre de 2023
Support para copias de seguridad continuas y oint-in-time restauración de PC de Amazon Aurora	AWS Backup ahora admite copias de seguridad y point-in-time restauración continuas (PITR) para los recursos de Aurora. Para obtener más información, consulte Copias de seguridad continuas y oint-in-time recuperación de P.	7 de septiembre de 2023

Cambio	Descripción	Fecha
AWS CloudFormation las pilas admiten la exclusión de recursos	AWS Backup ahora admite la opción de excluir los recursos elegidos de la AWS CloudFormation pila. Para obtener más información, consulte AWS CloudFormation stack backups.	6 de septiembre de 2023
Las reglas del plan de copia de seguridad introducen flexibilidad en las zonas horarias	AWS Backup las reglas del plan ahora pueden tener una zona horaria específica para las ventanas de respaldo. Para obtener más informaci ón, consulte Administración de planes de copia de seguridad.	28 de agosto de 2023
AWS Backup ahora disponibl e en la región de Israel (Tel Aviv)	Muchas AWS Backup funciones ya están disponibl es en la nueva región de Israel (Tel Aviv). Para ver qué recursos son compatibles, visite Disponibi lidad de características por Región de AWS.	22 de agosto de 2023

Cambio	Descripción	Fecha
AWS Backup Audit Manager ahora admite cuentas de administrador delegado	AWS Backup Las cuentas de administrador delegado ahora pueden acceder a la generación de informes de Audit Manager. Para obtener más información, consulte • Audite copias de seguridad y cree informes con AWS Backup Audit Manager • Uso de informes de auditoría • Administrador delegado	16 de agosto de 2023
Versión preliminar del almacén de copias de seguridad aislado lógicamente	AWS Backup ahora ofrece una vista previa de un nuevo tipo de bóveda de respaldo para ayudar a complementar las operaciones de protección de datos. Para obtener más información, consulte Almacenes aislados lógicamente (versión preliminar).	8 de agosto de 2023
AWS Backup mejora las copias de seguridad de Amazon S3	AWS Backup ha aumentado las capacidades de rendimiento, tamaño y velocidad para las copias de seguridad en cubos de S3. Para obtener más información, consulte Copias de seguridad Amazon S3.	1 de agosto de 2023

Cambio	Descripción	Fecha
La característica de etiquetar las restauraciones ahora está disponible en regiones de China	Ahora puede copiar las etiquetas que forman parte de una copia de seguridad al crear un trabajo de restauración en las regiones de China (Pekín) o China (Ningxia). Para obtener más información, consulte Copia de etiquetas durante una restauración.	17 de julio de 2023
AWS Backup ahora es compatible con Amazon S3 en regiones adicionales	AWS Backup El soporte para Amazon S3 ya está disponible en las regiones de Europa (España), Europa (Zúrich), Asia Pacífico (Hyderabad) y Asia Pacífico (Melbourne). Para obtener más información, consulte Disponibilidad de características por región.	6 de julio de 2023

Cambio	Descripción	Fecha
La copia entre cuentas se ha ampliado a más regiones	AWS Backup ahora admite copias de seguridad multicuenta de la mayoría de los recursos en las siguientes regiones: Asia Pacífico (Yakarta), Oriente Medio (Bahréin), Asia Pacífico (Hong Kong), África (Ciudad del Cabo), Europa (Milán), Asia Pacífico (Osaka), Oriente Medio (Emiratos Árabes Unidos), Europa (España), Europa (Zúrich), Asia Pacífico (Hyderabad) y Asia Pacífico (Melbourne). Para obtener más información, consulte Disponibilidad de características por región.	5 de julio de 2023
Backup Audit Manager disponible en GovCloud las regiones	AWS Backup ha ampliado AWS Backup Audit Manager a AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste). Para obtener más información, consulte Disponibilidad de características por región.	29 de junio de 2023

Cambio	Descripción	Fecha
La administración de cuentas cruzadas ahora está disponibl e en las regiones GovCloud	AWS Backup ahora es compatible con la gestión multicuenta de los recursos en AWS GovCloud (EE. UU. este) y AWS GovCloud (EE. UU., oeste). Para obtener más informaci ón, consulte Administración de recursos de AWS Backup en varias cuentas de AWS.	29 de junio de 2023
Compatibilidad con copias entre regiones de Amazon Aurora en más regiones	AWS Backup ahora admite copias de seguridad entre regiones para los clústeres de Aurora desde y hacia las siguientes regiones: Asia Pacífico (Yakarta), Oriente Medio (Bahréin), Asia Pacífico (Hong Kong), África (Ciudad del Cabo), Europa (Milán), Oriente Medio (Emiratos Árabes Unidos), Europa (España), Europa (Zúrich), Asia Pacífico (Hyderabad) y Asia Pacífico (Melbourne).	5 de junio de 2023

Cambio	Descripción	Fecha
Copia de etiquetas al restaurar	Las etiquetas que forman parte de una copia de seguridad ahora se pueden copiar al crear un trabajo de restauración. Para obtener más información, consulte Copia de etiquetas durante una restauración.	22 de mayo de 2023
AWS Backup se integra con las notificaciones de usuario AWS	Ahora puede optar por recibir notificaciones relacionadas con los eventos de copia de seguridad, copia y restauración a través de la Consola de AWS User Notifications. Para obtener más información, consulte Introducción a las notificaciones AWS de usuario.	10 de mayo de 2023
Copias de seguridad entre regiones disponibles en cuatro regiones nuevas	AWS Backup ahora admite la copia de seguridad entre regiones en las regiones de Oriente Medio (Emiratos Árabes Unidos), Europa (España), Europa (Zúrich) y Asia Pacífico (Hyderabad).	28 de abril de 2023

Cambio	Descripción	Fecha
Soporte ampliado de copias entre regiones AWS Backup	Las copias de seguridad entre regiones de los recursos de Amazon EFS, VMware y DynamoDB ahora pueden realizarse en las siguiente s regiones: Asia-Pacífico (Yakarta),Medio Oriente (Baréin), Asia-Pacífico (Hong Kong), África (Ciudad del Cabo) y Europa (Milán).	28 de abril de 2023
Copia de seguridad y restauración de Amazon S3 en la región de América del Sur (São Paulo)	AWS Backup El soporte para Amazon S3 (Amazon Simple Storage Service) ya está disponible en la región de Sudamérica (São Paulo). Para obtener más información, consulte Copias de seguridad Amazon S3.	20 de abril de 2023
AWS Backup se expande a la región de Asia Pacífico (Melbourne)	AWS Backup ahora está disponible en la región Asia Pacífico (Melbourne). Para obtener más informaci ón, consulte Disponibilidad de funciones por AWS región.	20 de abril de 2023

Cambio	Descripción	Fecha
Ampliación de la compatibi lidad regional para Amazon S3	AWS Backup La compatibi lidad con Amazon S3 (Amazon Simple Storage Service) ya está disponibl e en las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste) Para obtener más información, consulte Copias de seguridad Amazon S3.	19 de abril de 2023
Copia de seguridad y restauración de bases de datos de SAP HANA en instancias de Amazon EC2	AWS Backup ahora ofrece la posibilidad de realizar copias de seguridad y restaurar las bases de datos de SAP HANA que se ejecutan en instancias de Amazon EC2 en la mayoría de las regiones. Para obtener más información, consulte Copia de seguridad de bases de datos de SAP HANA en instancias de Amazon EC2.	17 de abril de 2023

Cambio	Descripción	Fecha
AWS Backup ahora disponible en las regiones de Europa (España), Europa (Zúrich) y Asia Pacífico (Hyderabad)	AWS Backup El soporte se ha extendido a nuevas regiones, incluidas Europa (España), Europa (Zúrich) y Asia Pacífico (Hyderabad). En estas regiones se pueden realizar copias de seguridad y restauraciones de los recursos compatibles. Para obtener más información, consulte Disponibilidad de funciones por AWS región.	13 de abril de 2023
Política AWS gestionada actualizada `AWSBackupAuditAccess`	Política AWS gestionada actualizada AWSBackupAuditAccess. AWS Backup sustituyó la selección de recursos de la API `config:DescribeCompliancebyConfigRule` por un recurso comodín. Para obtener más información, consulte Actualizaciones de políticas para AWS Backup.	11 de abril de 2023

Cambio	Descripción	Fecha
Hipervisores con Amazon Logs CloudWatch	AWS Backup Los usuarios de gateway ahora pueden integrar los hipervisores con los registros para mantener los CloudWatch registros. Para obtener más información, consulte Edición de la configuración de un hipervisor y de los registros. CloudWatch	29 de marzo de 2023
Compatibilidad regional ampliada para Amazon S3	AWS Backup El soporte para Amazon S3 ya está disponible en las regiones de Asia Pacífico (Yakarta) y Oriente Medio (Emiratos Árabes Unidos).	22 de marzo de 2023
Mejora de la copia de seguridad incremental de máquinas virtuales	Las copias de seguridad de las máquinas virtuales (VM) de VMware que presentan problemas con datos del CBT (Changed Block Tracking) ahora contienen información adicional para ayudar a corregir y solucionar problemas. Para obtener más información, consulte Copias de seguridad incrementales de máquinas virtuales y Solucionar problemas de máquinas virtuales.	15 de marzo de 2023

Cambio	Descripción	Fecha
AWS Backup soporte para varios adaptadores de red	AWS Backup la puerta de enlace ahora admite la configuración de varios adaptadores de red Para obtener más informaci ón sobre la configuración de los adaptadores de red, consulte Configuración de la puerta de enlace para varias NIC en VMware en la Guía para desarrolladores de AWS Backup .	8 de marzo de 2023
AWS Backup compatibilidad con vSphere 8	AWS Backup ahora admite la copia de seguridad y la restauración de máquinas virtuales que se ejecutan en VMware vSphere 8. Para obtener más información sobre las opciones de VMware compatibles, consulte las Máquinas virtuales compatibl es en la Guía para desarroll adores de AWS Backup .	8 de marzo de 2023

Cambio	Descripción	Fecha
AWS Backup Audit Manager es compatible con las copias de seguridad Multi-AZ de Amazon RDS	Backup Audit Manager ofrece ahora compatibilidad con copias de seguridad en varias zonas de disponibilidad de Amazon Relational Database Service Para obtener más informaci ón, consulte cómo auditar copias de seguridad y crear informes con AWS Backup Audit Manager.	1 de febrero de 2023
AWS Backup ofrece copias de seguridad incrementales para las tablas de Amazon Timestream	AWS Backup ahora ofrece capacidades de respaldo ampliadas para las copias de seguridad de Timestream. Los planes de copia de seguridad ahora pueden realizar copias de seguridad increment ales para reducir el tiempo necesario para realizar copias de seguridad de los recursos de Timestream y reducir los costos de almacenamiento. Para obtener más información, consulte Copias de seguridad de Amazon Timestream.	23 de enero de 2023

Cambio	Descripción	Fecha
AWS Backup ahora disponible en Dubái	AWS Backup se ha expandido a la región de Oriente Medio (EAU). En esta región se pueden realizar copias de seguridad y restauraciones de los recursos compatibles.	17 de enero de 2023
Copia entre regiones disponible en más regiones	AWS Backup ahora ofrece copias de seguridad interregionales en la región de Asia Pacífico (Yakarta), la región de Oriente Medio (Bahréin), la región de Asia Pacífico (Hong Kong), la región de África (Ciudad del Cabo) y la región de Europa (Milán) para la mayoría de los recursos. Para obtener más información, consulte Creación de copias de las copias de seguridad entre Regiones de AWS.	21 de diciembre de 2022

Cambio	Descripción	Fecha
Limitación y regulación del ancho de banda de Backup Gateway	AWS Backup La puerta de enlace ahora permite limitar el rendimiento de carga desde las puertas de enlace AWS Backup para controlar la cantidad de ancho de banda de red que utiliza la puerta de enlace. Para respaldar esta función, AWS Backup ha creado y actualizado políticas administradas, que incluyen `AWSBackupFullAccess` y. `AWSBackupOperatorAccess` Para obtener más información, consulte Limitación del ancho de banda de Backup Gateway.	15 de diciembre de 2022

Cambio	Descripción	Fecha
Compatibilidad de etiquetas de VMware para Backup Gateway	AWS Backup Gateway ahora es compatible con las etiquetas de VMware. Los usuarios tienen la flexibilidad adicional de crear AWS etiquetas que coincidan con las etiquetas utilizadas en las máquinas virtuales. Para respaldar esta función, AWS Backup ha creado y actualizado políticas administradas, que incluyen `AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync` `AWSBackupFullAccess` , y `AWSBackupOperatorAccess` . Para obtener más información, consulte Etiquetas de VMware.	15 de diciembre de 2022
AWS Backup soporte para Amazon Timestream	AWS Backup ahora admite la creación de copias de seguridad y la restauración de las tablas de Amazon Timestream. Para obtener más información, consulte Copias de seguridad de Amazon Timestream.	13 de diciembre de 2022

Cambio	Descripción	Fecha
AWS Backup ofrece retención legal	AWS Backup presenta una nueva herramienta para ayudar a proteger los puntos de recuperación en caso de retención legal. Para obtener más información, consulte Retención legal.	27 de noviembre de 2022
AWS Backup Audit Manager Informes entre regiones y cuentas	AWS Backup Audit Manager aporta funciones adicionales a los informes de cumplimie nto y de trabajo. Los usuarios pueden generar informes que incorporen varias regiones y varias cuentas. Para obtener más información, consulte Uso de informes de auditoría.	27 de noviembre de 2022
AWS Backup es compatible con Amazon Redshift	AWS Backup ahora ofrece soporte para realizar copias de seguridad de clústeres de Amazon Redshift y restaurar clústeres y tablas de Amazon Redshift. Para obtener más información, consulte Copias de seguridad Amazon Redshift.	27 de noviembre de 2022

Cambio	Descripción	Fecha
AWS Backup ofrece soporte para hacer copias de seguridad de pilas de aplicaciones AWS CloudFormation	AWS Backup proporciona la capacidad de realizar copias de seguridad CloudFormation y restaurar aplicaciones que contienen varios recursos mediante la creación de copias de seguridad de una pila y la restauración de los recursos que contiene. Para obtener más información, consulte Copias de seguridad de pilas de aplicaciones.	27 de noviembre de 2022
AWS Backup ofrece cuentas de administrador delegadas y delegación de políticas de respaldo	AWS Backup las cuentas inscritas AWS Organizations pueden designar las cuentas de los miembros como cuentas de administrador delegado. Para obtener más información, consulte Administrar varias cuentas con AWS Organizations.	27 de noviembre de 2022

Cambio	Descripción	Fecha
Versión preliminar pública de la copia de seguridad y restauración de SAP HANA en instancias de Amazon EC2	AWS Backup y AWS Backint ofrecen una versión preliminar pública integrada de la funcionalidad para realizar copias de seguridad y restaurar las bases de datos de SAP HANA en instancias EC2. Para obtener más información, consulte nuestra Versión preliminar pública de la copia de seguridad y restauración de SAP HANA en instancias de Amazon EC2. Para respaldar esta versión preliminar, AWS Backup ha proporcionado actualizaciones de políticas y nuevas políticas AWS gestionadas para estas funciones.	20 de noviembre de 2022

Cambio	Descripción	Fecha
Restauración de VMware en instancias de Amazon EC2	AWS Backup ahora ofrece la posibilidad de restaurar máquinas virtuales en instancias de Amazon EC2, además de la capacidad de restaurar máquinas en EBS, VMware, VMware Cloud on AWS y VMware Cloud on. AWS Outposts Para obtener más informaci ón, consulte la documentación sobre cómo utilizar la AWS Backup consola para restaurar los puntos de recuperación de máquinas virtuales.	9 de noviembre de 2022
Funcionalidad ampliada de AWS Backup Vault Lock	AWS Backup Ahora, Vault Lock se puede crear en modo de gobierno para ofrecer protecciones adicionales de IAM o en modo de conformid ad para garantizar la inmutabil idad. Obtenga más información en Bloqueo de almacenes de AWS Backup.	4 de octubre de 2022

Cambio	Descripción	Fecha
AWS Backup Audit Manager ya está disponible en la región de África (Ciudad del Cabo) y en la región de Europa (Milán)	AWS Backup Audit Manager se ha expandido a la región de África (Ciudad del Cabo) y a la región de Europa (Milán). Para obtener más información sobre Backup Audit Manager, consulte Auditar copias de seguridad y crear informes con AWS Backup Audit Manager.	14 de septiembre de 2022
AWS Backup lleva CloudWatch las métricas de Amazon al panel de control de la consola de Backup	AWS Backup mejora el panel de control de la consola Backup para mostrar CloudWatch las métricas integradas de Amazon para las tareas de backup y restauración, con el fin de aumentar la flexibilidad y la capacidad de supervisión.	8 de septiembre de 2022
Compatibilidad con una mayor flexibilidad de cifrado de Amazon EBS durante la restauración	AWS Backup ahora ofrece opciones adicionales de cifrado durante la restauración de las instantáneas de Amazon EBS.	1 de septiembre de 2022

Cambio	Descripción	Fecha
AWS Backup admite copias de seguridad entre cuentas y regiones de Amazon S3	AWS Backup ahora ofrece copias de seguridad entre regiones y cuentas para copias de seguridad de Amazon S3. Para obtener más información, consulte Copias de seguridad Amazon S3.	28 de julio de 2022
AWS Backup Audit Manager ofrece soporte de control adicional para FSx para ONTAP	AWS Backup Audit Manager ahora ofrece controles adicionales para respaldar la supervisión y la auditoría de FSx para los volúmenes de ONTAP, incluidos los recursos de Backup protegidos por un plan de respaldo y la creación del último punto de recuperación. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager.	22 de julio de 2022

Cambio	Descripción	Fecha
AWS Backup añade soporte para realizar copias de seguridad y restaurar clústeres Multi-AZ de Amazon RDS para clústeres PostgreSQL y MySQL	AWS Backup ha agregado una opción de copia de seguridad y restauración de clústeres en zonas de disponibilidad múltiple con una instancia de base de datos principal y dos en espera legibles. Para obtener más información, consulte Copias de seguridad de Amazon RDS Multi-AZ.	20 de julio de 2022
AWS Backup Audit Manager añade un nuevo control para la creación de puntos de recuperación	AWS Backup Audit Manager ofrece un nuevo control de auditoría para aumentar el apoyo al cumplimiento. `Last recovery point created` es un control adicional opcional para garantizar que los puntos de recuperación se creen dentro de los plazos especificados. Para obtener más informaci ón, consulte Último punto de recuperación creado.	29 de junio de 2022

Cambio	Descripción	Fecha
Se agregó un ejemplo AWS Backup de punto final Gateway	AWS Backup Gateway proporcionó un ejemplo de punto final para ayudar a los usuarios a conectarse a las VPN (redes privadas virtuales). Para obtener más informaci ón, consulte Crear un punto final de AWS Backup VPC.	14 de junio de 2022
AWS Backup ahora ofrece puntos de conexión de Amazon VPC para VMware	AWS Backup ahora es compatible con los puntos de enlace de Amazon VPC para VMware, lo que le permite utilizar una red privada virtual entre sus entornos de VMware y utilizar. AWS AWS PrivateLi nk Para obtener más informaci ón, consulte Creación de una puerta de enlace y AWS Backup y AWS PrivateLink.	1 de junio de 2022
AWS Backup Audit Manager ofrece soporte de control adicional para Amazon S3	Backup Audit Manager ahora admite el control de conformid ad Recursos de copias de seguridad protegidos por planes de copia de seguridad para los tipos de recursos de S3. Para obtener más información, consulte Controles y correccio nes de AWS Backup Audit Manager.	25 de mayo de 2022

Cambio	Descripción	Fecha
AWS Backup Audit Manager ofrece soporte de control adicional para Storage Gateway	Backup Audit Manager ahora admite el control de conformidad Recursos de copias de seguridad protegidos por planes de copia de seguridad para los tipos de recursos de Storage Gateway. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager.	25 de mayo de 2022
Compatibilidad con Amazon FSx para OpenZFS	AWS Backup ahora ofrece una administración adicional de la protección de datos para realizar copias de seguridad y restaurar archivos en FSx para sistemas de archivos OpenZFS.	18 de mayo de 2022
AWS Backup Soporte de Audit Manager para VMware	AWS Backup ahora ofrece soporte para máquinas virtuales en los controles y la corrección de Backup Audit Manager. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager.	11 de mayo de 2022

Cambio	Descripción	Fecha
Amazon FSx ahora admite la región de Asia Pacífico (Osaka)	AWS Backup ahora ofrece copias de seguridad de Amazon FSx en la región de Asia Pacífico (Osaka) y copias entre regiones desde y hacia dicha región.	26 de abril de 2022
Compatibilidad con Persisten t_2 de Amazon FSx para Lustre	AWS Backup ahora ofrece compatibilidad general con Amazon FSx for Lustre, que admite niveles de rendimien to más altos por unidad de almacenamiento en comparaci ón con los sistemas de archivos Persistent_1.	5 de abril de 2022
Mejoras de VMware	AWS Backup ahora ofrece restauración a Amazon EBS Volume, restauración a nivel de disco y compatibilidad con VMware on AWS Outposts. Para obtener más información, consulte Restauración de una máquina virtual.	31 de marzo de 2022
AWS Backup Disponibilidad para Asia Pacífico (Yakarta)	AWS Backup ya está disponibl e para los clientes de la región de Asia Pacífico (Yakarta).	17 de marzo de 2022

Cambio	Descripción	Fecha
Nuevos controles para AWS Backup Audit Manager	AWS Backup Audit Manager presenta tres nuevos controles de auditoría: copia entre regiones, copia entre cuentas y Backup Vault Lock. Para obtener más información, consulte Controles y correcciones de AWS Backup Audit Manager.	17 de marzo de 2022
Support para AWS PrivateLink	Con AWS PrivateLink for AWS Backup, puede conectarse directamente AWS Backup mediante un punto final de interfaz en su VPC en lugar de conectarse a través de la Internet pública. Se puede acceder directamente a los puntos finales de la interfaz desde aplicaciones que se encuentran en las instalaciones o en una región diferente AWS . Para obtener más información, consulte AWS Backup y AWS PrivateLink.	28 de febrero de 2022

Cambio	Descripción	Fecha
Compatibilidad con Amazon Simple Storage Service (Amazon S3)	La disponibilidad general AWS Backup de Amazon S3 Regiones de AWS está disponible en todas las regiones, excepto en las regiones de China (Beijing) , China (Ningxia), AWS GovCloud EE. UU. oeste y AWS GovCloud EE. UU. Este. Para obtener más informaci ón, consulte Uso de objetos de Amazon S3.	14 de febrero de 2022
Support para copias de seguridad avanzadas de DynamoDB en las regiones de China AWS	La copia de seguridad avanzada de DynamoDB ya está disponible en las regiones de China (Pekín) y China (Ningxia). Para obtener más información, consulte Copia de seguridad avanzada de DynamoDB.	18 de enero de 2022
Versión preliminar pública de la compatibilidad con Amazon S3	AWS Backup ofrece una vista previa pública de las copias de seguridad de Amazon S3. Para obtener más informaci ón, consulte Uso de datos de Amazon S3.	30 de noviembre de 2021

Cambio	Descripción	Fecha
Compatibilidad con máquinas virtuales (VM) de VMware	Ahora puede utilizarla AWS Backup para hacer copias de seguridad automáticas de las máquinas virtuales de VMware. Para obtener más información, consulte Copias de seguridad de máquinas virtuales.	30 de noviembre de 2021
Compatibilidad con copias de seguridad avanzadas de DynamoDB	Ahora puede utilizar AWS Backup las siguientes funciones para todas las nuevas copias de seguridad de tablas de DynamoDB que cree: almacenamiento en frío por niveles, etiquetado de asignación de costes, copia entre regiones, copia entre cuentas, cifrado independiente y copia de etiquetas de tablas de DynamoDB de origen. Para obtener más información, consulte Copia de seguridad avanzada de DynamoDB la Guía para desarrolladores de Amazon DynamoDB y su uso con AWS Backup DynamoDB.	23 de noviembre de 2021

Cambio	Descripción	Fecha
Support para mejorar la asignación de AWS Backup recursos en las regiones de AWS China	AWS Backup La mejora de la asignación de recursos ya está disponible en las regiones de China (Beijing) y China (Ningxia). Para obtener más información, consulte Asignación de recursos a un plan de copia de seguridad.	16 de noviembre de 2021
Lanzamiento de la mejora de la asignación AWS Backup de recursos	La mejora de la asignació n de recursos de backup le proporciona controles adicionales y detallados y nuevos procesos simplific ados para implementar planes de respaldo que protegen cientos de miles de recursos. AWS Utilice esta característica para aumentar la velocidad, la flexibilidad y la precisión a la hora de proteger los datos que AWS Backup utiliza. Para obtener más informaci ón, consulte Asignación de recursos a un plan de copia de seguridad.	10 de noviembre de 2021
Compatibilidad con Amazon Neptune	Ahora puede utilizarla AWS Backup para hacer copias de seguridad de los clústeres de Amazon Neptune. Para obtener más información, consulte ¿Qué es AWS Backup?	5 de noviembre de 2021

Cambio	Descripción	Fecha
Compatibilidad con Amazon DocumentDB	Ahora puede utilizarla AWS Backup para hacer copias de seguridad de los clústeres de Amazon DocumentDB. Para obtener más informaci ón, consulte ¿Qué es AWS Backup?	5 de noviembre de 2021
Support para AWS Backup Vault Lock en las regiones de AWS China	AWS Backup Vault Lock ya está disponible en las regiones de China (Pekín) y China (Ningxia). Para obtener más información, consulte Bloqueo de almacenes de AWS Backup.	3 de noviembre de 2021
Lanzamiento de AWS Backup Vault Lock	Con AWS Backup Vault Lock, puede evitar que se eliminen las copias de seguridad almacenadas en una bóveda AWS Backup de copias de seguridad. Para obtener más información, consulte Bloqueo de almacenes de AWS Backup.	7 de octubre de 2021

Cambio	Descripción	Fecha
Lanzamiento de los informes de conformidad de AWS Backup Audit Manager	Con los informes de conformidad, puede generar informes diarios sobre la conformidad de su actividad y sus recursos de backup con respecto a los controles que definió en sus marcos de trabajo de AWS Backup Audit Manager. Para obtener más información, consulte Plantillas de informes de conformidad.	5 de octubre de 2021
AWS CloudFormation soporte para AWS Backup Audit Manager	Con AWS CloudFormation, ahora puede implementar marcos, controles y planes de informes de AWS Backup Audit Manager de manera segura y repetible a escala. Para obtener más información, consulte Auditoría e informes de Backup con AWS Backup Audit Manager.	4 de octubre de 2021

Cambio	Descripción	Fecha
Lanzamiento de AWS Backup Audit Manager	Con AWS Backup Audit Manager, ahora puede definir los controles para la actividad y los recursos de backup e identificar las actividad es y los recursos que no cumplen con sus controles . También puede usar AWS Backup Audit Manager para generar informes diarios y bajo demanda que sirvan como evidencia del cumplimie nto de los controles definidos a lo largo del tiempo. Para obtener más información, consulte Auditoría e informes de Backup con AWS Backup Audit Manager.	24 de agosto de 2021
Compatibilidad con nuevas operaciones asíncronas de puntos de recuperación	AWS Backup ahora asume una función vinculada al servicio para administrar las reglas del ciclo de vida de las copias de seguridad en caso de que modifique o elimine su función de IAM original. Para obtener más información, consulte Eliminación de copias de seguridad.	23 de agosto de 2021

Cambio	Descripción	Fecha
Compatibilidad con copias de seguridad de varios volúmenes y coherentes ante bloqueos de Amazon EBS	Ahora, cuando lo utiliza AWS Backup para proteger sus instancias de Amazon EC2, AWS Backup realiza copias de seguridad de varios volúmenes y coherentes con los bloqueos de todos los volúmenes de Amazon EBS adjuntos a cada instancia de Amazon EC2 de forma predeterminada. Para obtener más información, consulte Creación de copias de seguridad de varios volúmenes y coherentes ante bloqueos de Amazon EBS.	14 de junio de 2021
Support para Amazon FSx de forma adicional Regiones de AWS	Ahora puede utilizarlos AWS Backup para proteger sus sistemas de archivos Amazon FSx en las siguiente s regiones: AWS GovCloud (US) región de Europa (Milán), región de África (Ciudad del Cabo) y región de Oriente Medio (Bahréin). Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	15 de abril de 2021

Cambio	Descripción	Fecha
Compatibilidad con copias de seguridad entre regiones y cuentas para Amazon FSx	Ahora puede utilizarlo AWS Backup para copiar copias de seguridad de Amazon FSx entre cuentas Regiones de AWS y cuentas. Para obtener más información, consulte Creación de una copia de la copia de seguridad. Si utiliza políticas administr adas por el cliente, debe agregar el nuevo permiso `fsx:CopyBackup` para evitar que se produzcan errores en los trabajos de copia de seguridad existente s. Para obtener ese permiso, consulte la última instrucci ón de la política de copia de seguridad de Amazon FSx en las Políticas administradas por el cliente.	12 de abril de 2021
Compatibilidad con etiquetas de asignación de costos para copias de seguridad de Amazon EFS	Ahora puede utilizar etiquetas de asignación de costes para realizar un seguimien to detallado de los costes de sus copias de seguridad de Amazon EFS, así como ver y filtrar esas etiquetas mediante ellas AWS Cost Explorer. Para obtener más información, consulte Uso de etiquetas de asignación de costes.	7 de abril de 2021

Cambio	Descripción	Fecha
Autorización FedRAMP High	AWS Backup ahora está autorizado para soportar cargas de trabajo de FedRAMP High. Para obtener más información, consulte Servicios de AWS en el ámbito del programa de conformidad.	25 de marzo de 2021
¿Nuevo? Región de AWS	AWS Backup ya está disponible en la región de Asia Pacífico (Osaka). En esta región, AWS Backup actualmente no admite Storage Gateway, Amazon FSx ni copias de seguridad entre cuentas en la región. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	25 de marzo de 2021
Compatibilidad con operaciones por lotes en puntos de recuperación	Ahora puede usar la AWS Backup consola para automatizar las operaciones por lotes y limpiar los puntos de recuperación de sus almacenes de respaldo. Para obtener más información, consulte Eliminación de copias de seguridad.	23 de marzo de 2021

Cambio	Descripción	Fecha
Compatibilidad con restauraciones a la clase de almacenamiento Amazon EFS One Zone	Ahora puede restaurar sus copias de seguridad de Amazon EFS en la clase de almacenamiento Amazon EFS One Zone. Para obtener más información, consulte Restauración de un sistema de archivos de Amazon EFS.	12 de marzo de 2021
Support para la restauración y el backup continuo de Amazon Relational Database point-in-time Service	Ahora puede utilizarlos AWS Backup para automatizar las copias de seguridad continuas y realizar point-in-time restauraciones (PITR) de Amazon RDS, además de organizar las copias de seguridad de las instantáneas. Para obtener más informaci ón, consulte Restaurar a un tiempo específico mediante la recuperación. point-in-time	10 de marzo de 2021
Support para Amazon CloudWatch	Ahora puedes usarlo CloudWatch para monitorea r AWS Backup las métricas. Para obtener más informaci ón, consulta Monitorización de eventos y métricas con Amazon CloudWatch y Amazon EventBridge.	3 de febrero de 2021

Cambio	Descripción	Fecha
Support para Amazon EventBridge	Ahora puede usarlo EventBridge para monitorear AWS Backup eventos. Para obtener más información, consulta Monitorización de eventos y métricas con Amazon CloudWatch y Amazon EventBridge.	3 de febrero de 2021
Compatibilidad con copias de seguridad entre cuentas	Ahora puede utilizarlos AWS Backup para hacer copias de seguridad de sus recursos en varios Cuentas de AWS. Para obtener más información, consulta Cómo crear copias de seguridad en todas AWS las cuentas.	18 de noviembre de 2020
Compatibilidad con copias de seguridad y restauración de sistemas de archivos de Amazon FSx	Ahora puede utilizarla AWS Backup para hacer copias de seguridad de los sistemas de archivos Amazon FSx. Para obtener más información, consulte Uso de sistemas de archivos de Amazon FSx.	9 de noviembre de 2020
¿Nuevo Regiones de AWS	AWS Backup ya está disponible en África (Ciudad del Cabo) y Europa (Milán) Regiones de AWS. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	21 de octubre de 2020

Cambio	Descripción	Fecha
Compatibilidad con copias de seguridad de Windows habilitadas para VSS	Ahora puede realizar copias de seguridad y restaurar aplicaciones de Windows habilitadas para VSS (Volume Shadow Copy Service) que se ejecuten en instancia s de Amazon EC2. Para obtener más información, consulte Creación de copias de seguridad de Windows VSS.	22 de septiembre de 2020
Compatibilidad con copias de seguridad automáticas de Amazon EFS	Ahora puede utilizarla AWS Backup para realizar copias de seguridad automáticas de los sistemas de archivos de Amazon EFS. Para obtener más información, consulte Primeros pasos 4: creación de copias de seguridad automátic as de Amazon EFS.	16 de julio de 2020
¿Nuevo Región de AWS	AWS Backup ya está disponibl e en AWS GovCloud (US) Region. Para obtener más información, consulte Puntos de conexión y cuotas de AWS Backup en la Referencia general de AWS .	24 de junio de 2020

Cambio	Descripción	Fecha
Support para administrar copias de seguridad en múltiples Cuentas de AWS	Ahora puede administrar las copias de seguridad en varias Cuentas de AWS mediante AWS Organizations. Para obtener más información, consulte Cómo funciona la administración entre cuentas.	24 de junio de 2020
Support para Amazon Aurora se agregó a AWS Backup	Ahora puede configurarlo AWS Backup para hacer copias de seguridad de los recursos de Amazon Aurora. Para obtener información, consulte Información general de copias de seguridad y restauración de un clúster de base de datos Aurora en la Guía del usuario de Amazon Aurora.	10 de junio de 2020
Support para configurar los servicios con los que trabajar AWS Backup	Ahora puede configurarlo AWS Backup para hacer copias de seguridad de los recursos de AWS servicios específicos. Para obtener más información, consulte Aceptar la administración de servicios con AWS Backup.	20 de mayo de 2020

Cambio	Descripción	Fecha
Compatibilidad con la realización de copias de seguridad de instancias de Amazon EC2 y copias de seguridad entre regiones	Ahora puede realizar copias de seguridad de instancias de Amazon EC2 completas y puede copiar recursos en todas las Regiones de AWS. Para obtener más información, consulte Creación de copias de las copias de seguridad entre Regiones de AWS.	13 de enero de 2020
Nueva guía	AWS lanzamientos AWS Backup y la Guía para AWS Backup desarrolladores.	15 de enero de 2019

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.